최종연구보고서	KISA-WP-2010-0003

해외 무선랜 보안 법제도 연구

A Study on Overseas Legal Policy of Wireless Lan Security

수 탁 기 관 : 연 세 대 학 교 산 학 협 력 단

2010. 7.

한국인터넷진흥원
Korea Internet & Security Agency

제 출 문

한국인터넷진흥원 원장 귀하

본 보고서를 “해외 무선랜 보안 법제도 연구”의 최종 연구 결과보고서로 제출합니다.

2010 년 7 월 22 일

수탁 기관 : 연세대학교 산학협력단
연구책임자 : 교 수 오 병 철 (연세대학교 법학전문대학원)
참여연구원 : 연 구 원 정 필 운 (연세대학교 법학연구원)
연 구 원 정 기 봉 (연세대학교 법학전문대학원)
연 구 원 윤 종 인 (연세대학교 법학연구원)
연 구 원 최 수 연 (연세대학교 법학전문대학원)
연 구 원 이 현 섭 (연세대학교 법학전문대학원)

요 약 문

1. 제목

해외 무선랜 보안 법제도 연구

2. 연구개발의 목적 및 중요성

무선랜 관련 법제도 및 정책 연구는 무선랜의 확산에 비하여 미흡한 실정이다. 예를 들어, 무선랜 공유기 개방에 따른 법적 권리·의무의 관계는 어떻게 되는지, 그리고 권한없는 무선랜 접속과 권한없이 무선랜에 접속하여 발생하는 2차적 침해는 어떻게 해결하여야 할 것인지 등 관련 문제에 대한 연구는 찾아보기 힘든 실정이다.

현재 해외의 몇몇 국가들은 무선랜을 활발히 이용하고 있으며, 한편으로는 다양한 형태의 법적 분쟁 사례를 겪어왔다. 이를 해결하기 위하여 법제도 정비 및 정책 수립을 추진하고 있다. 따라서, 해외의 분쟁사례와 법제도 및 정책들은 향후 발생할 수 있는 분쟁의 방지 및 해결에 도움을 줄 수 있을 것이며, 법제도 및 정책을 수립하는데 참고가 될 것이어서 이에 대한 연구가 필요하다고 할 것이다.

3. 연구개발의 내용 및 범위

무선랜에 대한 공학적 관점에서의 기술 동향과 보안 적용 현황을 파악하여 법제도적으로 고려하여야 할 기술적 사항을 검토한다. 다음으로, 해

외 무선랜 보안 관련 법·제도에 대한 자료를 입수하여 이에 대한 분석을 통해 시사점을 도출한다. 그리고 미국, 영국, 독일 등 해외의 무선인터넷 침해관련 처벌 및 그 근거를 조사하여 각 국가별 특징과 처벌 추이 및 효과를 분석한다.

그리고 무선랜 보안강화가 주는 긍정적 영향과 부정적 영향을 종합적으로 검토하고 다양한 보안이슈의 특성을 무선랜 운영주체를 세분화하여 법적 관점에서 고찰하도록 한다. 이를 바탕으로 무선랜 보안과 관련하여 법·제도의 규율 방안 및 정책 방향을 고민하도록 한다.

4. 연구결과

연구결과 전세계적으로 무선랜의 이용이 증가하고 있으며, 보안의 위험성을 인식하고 이에 대한 기술적 대응에 노력하고 있음을 알 수 있다. 그러나 무선랜 보안에 특화되어 이를 직접적인 규율 대상으로 하고 있는 법률은 어느 나라에서도 찾아보기 어렵다. 이는 보안의 문제를 인터넷 전반에 걸친 일반적인 이슈로 인식하고, 특정 디바이스나 서비스 마다 특화시켜 다루지 않는 것이 세계적인 법적 규제의 추세라고 할 수 있을 것이다.

다만 영국의 디지털경제법 제정과정에서 카페나 레스토랑과 같은 불특정 다수에게 무선랜을 접속시켜주는 주체에 대해서 보안설정을 의무화하여야 하는가가 큰 사회적인 논란을 가져왔다. 그러나 결과적으로는 40만 명이상의 가입자를 가진 ISP에게만 보안설정을 의무화하는 쪽으로 타협점을 찾음으로써 중요한 의미는 퇴색되었다. 이론적으로는 기존의 해킹을 처벌하기 위한 규정을 개방된 무선랜에 임의로 접속하는 것에도 적용가능한가가 이론적으로 논란의 대상이 되고 있음은 세계 공통이다.

무선랜 보안을 침해한 실제 사건도 세계적으로 흔하지는 않다. 다만 영국, 미국, 싱가포르에서 개방된 무선랜에 접속한 그 자체에 대해 재산권침해로 처벌한 극히 소수의 사소한 사건을 발견할 수 있었다. 최근 AP보유자에게 접속인증 보안설정의무를 일반적으로 인정한 독일 연방대

법원의 판결은 무선랜 보안에 대해 엄청난 반향을 가져올 것으로 예상된다. 그러나 이에 대해서는 전세계적으로 비판의 견해도 상당히 제기되고 있으므로 좀 더 논의의 추이를 지켜볼 필요가 있을 것이다.

이러한 해외 동향은 우리나라의 무선랜 보안정책을 수립하는데 기대했던 것 만큼의 시사점을 주지는 못한다는 점에서, 우리나라가 선도적으로 무선랜 보안정책을 독자적으로 수립하는 것이 불가피하다고 생각된다. 그리하여 민간부문의 무선랜은 자율적으로 보안을 확보하도록 유도하고, 공공부문의 무선랜은 공공성을 고려하여 접속인증과 데이터 암호화 모두 구비하는 것을 정책의 기본원칙으로 설정하여야 할 것이다.

5. 활용에 대한 건의

무선랜을 비롯한 IT분야에서는 기술적인 측면 뿐 아니라 정책적인 측면에서도 우리나라가 전세계적으로 선도적인 지위를 차지하고 있음을 본 연구를 통해서 알 수 있다. 따라서 무선랜 보안 뿐만 아니라 IT전반에 대한 정책수립 과정에서 해외동향에 대한 관심보다는 우리나라의 기술적, 사회적, 정치적 상황에 적합한 고유한 정책을 개발하는 것이 더 의미있다는 점을 고려하여야 할 것이다. 즉 IT기술에서의 자부심을 IT정책에 대한 자신감으로 연결시켜야 할 시점이라 생각된다.

6. 기대효과

본 연구의 결과를 통해 무선랜 보안의 중요성에 대해 사회 전반적으로 관심을 높이는 동시에 향후 관련 정책을 수립할 때 중요한 비교법적 참고자료 및 정책방향 설정의 자료로 이용할 수 있을 것이다.

SUMMARY

1. Title

A Study on Overseas Legal Policy of Wireless LAN Security

2. Purpose of the study

Research of legislation and policy on Wireless LAN security lags behind the proliferation of Wireless LAN technology. We could hardly find research, for example, on such issues as to what rights and obligations exist with regard to open wireless LAN access points and how to deal with an unauthorized access to wireless LAN and ensuing secondary breach of other's right.

At present a few countries have deployed wireless LAN actively, facing a variety of legal problems arising from it. In order to resolve those disputes they are actively putting their legislative and policy-making efforts. Thus, necessary is a study on legal disputes, legislation, and policies regarding wireless LAN in other countries since the result of the study will help us avoid or resolve disputes and guide us in making laws and policies.

3. Contents and scope

This report first examines trends in wireless LAN technology and current security status of wireless LAN and addresses technological issues that are to be considered from the legal and policy-making perspectives. Next the report analyzes legislation and policies regarding Wireless LAN Security in other countries and draws insights. Then it compares the laws and its enforcement related to illegal access of wireless LAN of a number of countries including US, UK, and Germany, and analyzes trend and effect of punishment for each country.

Also the report examines both positive and negative impacts of strengthening wireless LAN security requirement on our society, and investigates those security issues from the legal standpoint categorizing wireless access points according to its operator/owner. Based on these examinations the report provides advice on legislating and policy-making strategies for wireless LAN security.

4. Results of the study

With the number of wireless LAN locations continuing to increase worldwide, every country recognizes its security risks and tries to provide technical solutions. However few country has a law directly dictating wireless security obligations. In U.K., though, the legislation of the Digital Economy Act generated significant controversy as to whether the obligation of enabling security mechanisms has to be levied upon those who provide wireless access to general public like cafe or restaurant owners, ending up with a compromise that the code will only apply to ISPs with over 400,000 subscribers. It is a

common theoretical question worldwide whether it is legitimate to apply the existing provisions originally intended to punish hacking into computers to piggybacking open wireless networks.

There are not that many reported cases worldwide where the breach of wireless LAN security is actually brought to the court except a few trivial criminal cases in UK, US, and Singapore where unauthorized access itself was punished for breaching property rights. Recent ruling of the Federal Court of Justice of Germany that acknowledged the owner's obligation of enabling security on wireless access points is expected to invite considerable controversies. But we may well wait and see how the debate will evolve since the ruling is facing a barrage of worldwide criticism.

5. Expected effects and applications

The result of this study will be able to serve as reference and background information for those who plan to call for public attention to the importance of wireless LAN security and make relevant policies in the future.

목 차

제 1 장 연구의 배경 및 목적 ····· 1
제 1 절 연구의 배경 ····· 1
제 2 절 연구의 목적 ····· 2

제 2 장 무선랜 활용 및 보안 동향 ····· 4
제 1 절 무선랜 개요 ····· 4
제 2 절 무선랜 이용 현황 ····· 6
1. 해외 무선랜 이용 현황 ····· 6
2. 국내 무선랜 이용 현황 ····· 9
제 3 절 무선랜 보안 동향 ····· 12
1. 무선랜 보안상 취약점 ····· 12
2. 무선랜 보안 기술 ····· 13
3. 해외 무선랜 보안 적용 실태 ····· 18
4. 국내 무선랜 보안 적용 실태 ····· 21
5. 취약한 무선랜 보안 적용 실태에 대한 대책 ····· 23

제 3 장 해외 무선랜 보안 법규와 정책 ····· 28
제 1 절 관련자에 대하여 의무를 부과하는 법규 ····· 28
1. 영국의 '디지털경제법'(Digital Economy Act 2010) ····· 28
2. 미국 캘리포니아 주 사업 및 직업법 22948.6조 ····· 44
3. 미국 뉴욕 주 Westchester County ····· 49

4. 미국 유타 주 ····· 49
5. 인도 ····· 50
6. 나이지리아 ····· 51
7. 독일 ····· 53
제 2 절 사용자의 권한없는 접근을 금지, 처벌하는 법규 ····· 56
1. 미국 2009 House Bill 1011 ····· 56
2. 미국 컴퓨터 사기와 남용에 관한 법률(CFAA) ····· 58
3. 미연방 전자통신프라이버시법(ECPA) ····· 61
4. 미국 플로리다 주 ····· 62
5. 미국 미시건 주 ····· 62
6. 호주 Cybercrime Act 2001 ····· 63
7. 영국 '경찰 및 사법절차에 관한 법률'
(Police and Justice Act 2006) ····· 64
8. 일본 '부정액세스행위 금지 등에 관한 법률' ····· 65
9. 싱가포르 '컴퓨터 오용에 관한 법률'
(Computer Misuse Act)' ····· 66
10. 캐나다 형법 ····· 67
제 3 절 통신요금의 회피를 목적으로 타인의
서비스를 이용하는 것을 금지하는 법규 ····· 68
1. 미국 알래스카 주 ····· 68
2. 영국 '통신법'(Communications Act 2003) ····· 68
3. 싱가포르 전기통신법(Telecommunications Act) ····· 69
4. 캐나다 형법 ····· 69
제 4 절 허가제도 ····· 70
1. 러시아 ····· 70
2. 남아프리카 공화국 ····· 71
3. 필리핀 ····· 71
4. 사우디아라비아 ····· 72
5. 호주 통신법(Telecommunications Act 1997) ····· 74

제 5 절 기타 ····· 74
1. 중국 ····· 74
2. 호주 전파통신법(Radiocommunications Act 1992) ····· 75

제 4 장 무선랜 보안 침해 사례 ····· 77
제 1 절 해외 무선랜 침해 사례 ····· 77
1. 인증이 필요한 WiFi 침해 사례 ····· 77
2. 개방된 무선 네트워크(오픈 WiFi) 침해 사례 ····· 78
3. 오픈 WiFi 제공자의 책임 ····· 94
제 2 절 무선랜 취약성 보고 사례 ····· 105
1. 해외 무선랜 취약성 보고 사례 ····· 105
2. 국내 무선랜 취약성 보고 사례 ····· 109

제 5 장 무선랜 보안 정책 방향 ····· 111
제 1 절 서론 ····· 111
1. 무선랜 활용의 장애요인 분석 ····· 111
2. 무선랜 보안의 필요성 ····· 114
3. 무선랜 보안과 활성화와의 상관관계 ····· 115
4. 무선랜 공급주체의 구분 ····· 117
제 2 절 민간 부문의 무선랜 보안 정책 방향 ····· 119
1. 기본원칙 ····· 119
2. 접속인증 ····· 120
3. 데이터 암호화 ····· 132
제 3 절 공공부문의 무선랜 보안 정책 방향 ····· 133
1. 원칙 ····· 133
2. 접속인증 ····· 137
3. 데이터 암호화 ····· 143
제 4 절 구체적인 법제도 정비 방안 ····· 144
1. 입법론적 정비 방안 ····· 144

2. 법해석학적 정비 방안 ····· 150

제 6 장 결 론 ····· 154

참고문헌 ····· 157

Contents

Chapter 1 Introduction ····· 1

Section 1 Background ····· 1

Section 2 Objectives ····· 2

Chapter 2 Wireless LAN Deployment and Security ··· 4

Section 1 Overview ····· 4

Section 2 Deployment ····· 6

1. Worldwide Deployment Status ····· 6

2. Domestic Deployment Status ····· 9

Section 3 Security Status ····· 12

1. Security Weakness ····· 12

2. Security Technology ····· 13

3. Worldwide Security Status ····· 18

4. Domestic Security Status ····· 21

5. Measures for Enhancing Security ····· 23

Chapter 3 Overseas Legal Policy of Wireless LAN Security ·· 28

Section 1 Rules Imposing Obligations ····· 28

1. UK Digital Economy Act ····· 28

2. California Bus.&Prof. Code ····· 44
3. Westchester WiFi Legislation ····· 49
4. Utah Code ····· 49
5. India ····· 50
6. Nigerian Communications Act 2003 ····· 51
7. Germany ····· 53
Section 2 Rules Forbidding Unauthorized Access ····· 56
1. US 2009 House Bill 1011 ····· 56
2. US Computer Fraud and Abuse Act ····· 58
3. US Electronic Communications Privacy Act ····· 61
4. US Florida State ····· 62
5. US Michigan State ····· 62
6. Australia Cybercrime Act 2001 ····· 63
7. UK Police and Justice Act 2006 ····· 64
8. Japan Illegal Access Prohibition Law ····· 65
9. Singapore Computer Misuse Act ····· 66
10. Canada Penal Code ····· 67
Section 3 Rules Forbidding Using Other's Network ····· 68
1. US Alaska ····· 68
2. UK Communications Act 2003 ····· 68
3. Singapore Telecommunications Act ····· 69
4. Canada Penal Code ····· 69
Section 4 Permit System ····· 70
1. Russia ····· 70
2. South Africa ····· 71
3. The Philippines ····· 71

4. Saudi Arabia ····· 72
5. Australia Telecommunications Act 1997 ····· 74
Section 5 Others ····· 74
1. China ····· 74
2. Australia Radiocommunications Act 1992 ····· 75

Chapter 4 Cases of Wireless LAN Security Breach ·· 77
Section 1 Overseas breach Cases ····· 77
1. WiFi Authentication Breach ····· 77
2. Open WiFi Breach ····· 78
3. Open WiFi Provider's Liabilities ····· 94
Section 2 Wireless LAN Security Weaknesses ····· 105
1. Overseas Cases ····· 105
2. Domestic Cases ····· 109

Chapter 5 Directions of Wireless LAN Security Policy ·· 111
Section 1 Introduction ····· 111
1. Barriers to WiFi Proliferation ····· 111
2. Necessity of Security ····· 114
3. Correlation between Security and Proliferation ····· 115
4. Categorization of WiFi Service Providers ····· 117
Section 2 Private Sector ····· 119
1. Principles ····· 119
2. Authentication ····· 120
3. Data Encryption ····· 132
Section 3 Public Sector ····· 133

1. Principles ····· 133
2. Authentication ····· 137
3. Data Encryption ····· 143
Section 4 Proposals and Advices ····· 144
1. Legislative Issues ····· 144
2. Legal Interpretative Issues ····· 150

Chapter 6 Conclusions ····· 154

References ····· 157

그림 목차

(그림 2-1) 미국 AT&T 무선랜 접속건수 증가 ····· 5
(그림 2-2) 무선랜 접속 가능 장소의 증가 ····· 7
(그림 2-3) 미국에서 무선랜 접속에 1차적으로 사용되는 기기의 비율 (Primary Device Usage) ····· 9
(그림 2-4) 국내 와이파이존의 증가 ····· 11
(그림 2-5) WEP 데이터 암호화 방식 ····· 16
(그림 2-6) 조사대상 공항내 무선랜 AP의 보안 상태 ····· 19
(그림 2-7) 바이러스 SSID의 예 ····· 21
(그림 2-8) 무선 AP에서 사용하고 있는 무선랜 보안 기술 ····· 22
(그림 2-9) 무선 AP의 보안설정 화면 ····· 23
(그림 4-1) 구글 스트리트 뷰 관련 사진 ····· 88
(그림 4-2) 구글의 "gslite" ····· 89
(그림 5-1) 무선랜 공급주체의 구분 ····· 119

표 목차

[표 2-1] IEEE 무선랜 표준의 구성 ····· 4
[표 2-2] 무선인터넷 기술의 비교 ····· 5
[표 2-3] 주요 국가의 무선랜 접속 장소의 비교 ····· 8
[표 2-4] 행정청의 무선랜 보안 점검의 법적 근거 검토 ····· 25

제 1 장 연구의 배경 및 목적

제 1 절 연구의 배경

오늘날 우리는 집이나 직장 등 실내에서 무선랜 공유기를 설치하여 무선랜에 접속할 뿐만 아니라, 밖에서도 노트북이나 스마트폰을 들고 다니며 와이파이존 또는 핫스팟 지역에서 무선랜에 접속하는 경우가 일상화 되었다.

그러나, 무선랜에 접속하는 일반 사용자들은 무선랜 공유기에 암호를 설정하여 보안을 확보하려는 인식이 부족하고, 암호를 설정하고자 하여도 그 방법을 모르거나 그 방법이 복잡하여 귀찮게 여기는 경우가 많다. 예를 들면, 집에서 무선랜 공유기를 설치하고 접속하는 경우 무선랜 공유기에 암호화를 하여 보안을 확보하려는 노력은 거의 찾아볼 수 없으며, 오히려, 컴퓨터가 자동으로 무선랜에 접속하는 경우에는 자신의 무선랜 공유기에 접속하는지 아니면, 집 주변 타인의 무선랜 공유기에 접속하는지도 알지 못하는 경우가 많다. 실제로 무선랜 사용료를 지불하면서 1년 내내 타인의 무선랜 공유기에 접속하여 사용하는 경우도 발생하며, 마찬가지로 타인이 자신의 무선랜에 접속하여도 그 사실조차 인식하지 못하는 경우도 발생한다.

최근 무선랜 사용이 급격히 늘면서 무선랜 보안의 문제도 사회적으로 대두되게 되었다. 무선랜의 보안이 특히 취약한 이유 중 하나는 허가나 신고가 필요없는 ISM대역을 사용하고 있기 때문에 허가주의나 신고주의가 적용되는 다른 주파수 대역을 이용한 통신보다 상대적으로 보안이 취약하다는 점이다.

무선랜의 보안 문제는 실제로 다양한 법적인 문제를 발생시킬 수 있다. 일차적으로는 개방되어 있는 타인의 무선랜에 권한없이 접속하거나 해킹하여 접속함으로써 불법적으로 개인정보를 취득하는 경우도 있을 수 있

으며, 타인의 IP를 도용하여 명예훼손, 저작권 침해, 해킹, 바이러스 및 음란물을 유포하는 등 이차적 문제의 발생 가능성이 높다.

그러나 그동안 무선랜 관련 법제도 및 정책 연구는 무선랜의 확산에 비하여 극히 미흡한 실정이어서, 무선랜 공유기에서 발생하는 신호가 공유기 보유자의 법률상 소유권에 속하는 것인지, 무선랜 공유기 개방에 따른 법적 권리·의무의 관계는 어떻게 되는지, 그리고 권한없는 무선랜 접속과 권한없이 무선랜에 접속하여 발생하는 2차적 침해는 어떻게 해결하여야 할 것인지 등 관련 문제에 대한 연구는 찾아보기 힘든 실정이다.

해외의 몇몇 국가들은 무선랜과 관련한 다양한 형태의 법적 분쟁 사례를 경험함으로써, 이를 해결하기 위하여 법제도를 정비하고 관련 정책을 수립하는 등 여러 노력을 기울이고 있다. 따라서 해외의 분쟁사례와 법제도 및 정책들을 조사하고 연구하는 것은 앞으로 발생할 수 있는 무선랜 관련 법적분쟁의 방지 및 해결에 도움을 줄 수 있을 것이며, 우리나라의 무선랜 보안에 관한 법제도 및 정책을 수립하는데 도움이 될 것이어서 이에 대한 연구가 필요하다고 할 것이다.

제 2 절 연구의 목적

이 연구는 국민들의 무선랜에 대한 욕구를 충족하는 동시에 안심하고 사용할 수 있는 무선랜 환경을 조성하기 위한 국가적 차원의 무선랜 보안에 대한 법제도 및 정책 방향을 정립하는데 도움이 될 수 있도록 하는데 그 목적이 있다.

이를 위하여 본 연구는 다음과 같은 방법으로 진행한다. 우선, 무선랜에 대한 공학적 관점에서의 기술 동향과 보안 적용 현황을 파악하여 법제도적으로 고려하여야 할 기술적 사항을 검토한다. 특히, 보안위협 유형별로 모바일 바이러스, 해킹 등으로 구분하여, 최신 피해 사례 및 공격 유형을 분석하고, 국내외 최신 기술적 대응방안 및 WiFi 연합(Wireless-Fidelity

Alliance) 등에서 무선랜 해킹을 방지하기 위한 자체노력 및 기술적, 제도적 수단 등의 대표적 사례를 조사하고 이를 분석하도록 한다.

다음으로, 해외 무선랜 보안 관련 법·제도에 대한 자료를 입수하여 이에 대한 분석을 통해 시사점을 도출하며, 미국, 영국, 프랑스, 일본 등 해외의 무선인터넷 침해관련 처벌방법 및 근거를 조사하고, 각 국가별 특징과 처벌 추이 및 효과를 분석하고, 민사상 손해배상 사례 여부를 파악하는 등 현재까지의 해외 무선랜 관련 사례 등을 수집·분석하여 법적 문제를 검토하고 우리에게 적용될 수 있는지 고민하여 본다.

또한, 각 부분별로 무선랜 보안강화가 주는 긍정적 영향과 부정적 영향을 다양한 보안이슈의 특성을 고려하여 종합적으로 법적 관점에서 검토하며, 검토한 내용을 바탕으로 무선랜 보안에 대한 법·제도의 규율 방안 및 정책 방향을 제시하도록 한다.

따라서, 이 연구보고서는 다음과 같이 서술한다. 제2장에서는 국내외 무선랜 구축 동향과 무선랜 보안 적용 현황을, 제3장에서는 해외 무선랜 보안 법규와 정책에 대하여 기술하고, 제4장에서는 무선랜 보안 침해 사례를 조사·검토하며, 마지막으로 제5장에서는 무선랜 보안 정책 방향에 대하여 기술하도록 한다.

제 2 장 무선랜 활용 및 보안 동향

제 1 절 무선랜 개요

현재 사용되고 있는 무선랜은 국제표준기구인 IEEE[1]에서 제정한 802.11 계열의 기술 표준을 따르고 있다. 무선랜 장비는 무선랜 시장의 활성화를 위해 업계에 의해 설립된 비영리 단체인 와이파이연합(WiFi Alliance)[2]의 기술 인증을 통과하여야만 WiFi 인증마크를 부착할 수 있다.

[표 2-1] IEEE 무선랜 표준의 구성

표준명	제정시기	주파수 대역	최대전송속도
802.11	1997	2.4 GHz	2Mbps
802.11a	1999	5 GHz	54Mbps
802.11b	1999	2.4 GHz	11Mbps
802.11g	2003	2.4 GHz	54Mbps
802.11n	2009	2.4~2.5 GHz	300Mbps

무선랜은 사용의 편리함과 낮은 설치 및 유지 비용 덕분에 점차 많은 분야에 걸쳐 활용되고 있다. LTE[3]와 같은 제4세대(4G) 이동통신 기술이 보급되면 무선랜의 사용이 감소될 것이라는 견해도 있으나 무선랜의

1) IEEE (Institute of Electrical and Electronics Engineers) : 국제 전기전자 기술자 협회로 무선랜 관련 표준개발 전문기구

2) http://www.WiFi.org/ (2010. 7. 10 방문) 무선랜 와이파이소개, 인증프로그램, 인증제품목록, 행사일정, 보도자료 수록

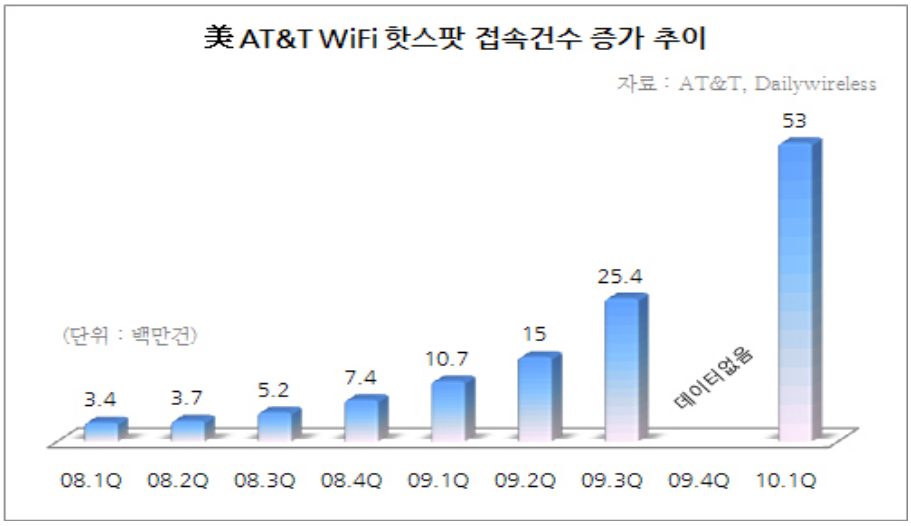
3) 롱텀에볼루션(long term evolution)의 머리글자를 딴 것으로, 3세대 이동통신(3G)을 '장기적으로 진화'시킨 기술이라는 뜻에서 붙여진 명칭이다. 와이브로 에볼루션과 더불어 4세대 이동통신 기술의 유력한 후보 가운데 하나로 꼽힌다.

이러한 원가경쟁력으로 인하여 무선랜의 활용도는 계속 증가하리라는 견해가 지배적이다.

[표 2-2] 무선인터넷 기술의 비교

구 분	3G(WCDMA)	WiBro	무선랜(WiFi)
커버리지	전국	수도권	Hot-Spot
이동성	이동형	이동형	고정형
설치 및 유지비용	높음	보통	낮음
보안성	높음	높음	낮음
전송속도	중, 저속	고속	초고속

미국 스마트폰 이용자의 약 81%는 각종 서비스 이용시 3G보다 무선랜을 더 선호한다는 설문조사도 보고되었다. AT&T는 올 1분기 무선랜 접속건수가 전년 동기 대비 5배 이상 증가한 5,300만건을 넘어섰다고 발표했다.



(그림 2-1) 미국 AT&T 무선랜 접속건수 증가

하지만 무선랜은 동시에 무선 통신의 특성상 직면하게 되는 다수의 보안 취약점을 가지고 있으며 이런 문제점을 해결하기 위해 다양한 보안관련 기술이 개발 및 적용되고 있다 하지만 그에 반해 무선랜 사용자의 보안 인식은 여전히 부족한 상태로 매년 개인정보 유출 등의 보안사고가 반복적으로 발생하고 있는 상황이다.

이미 개인정보 유출이나 저작권 침해 등의 법적 분쟁이 증가하고 있고 앞으로 지하철, 할인마트, 카페 등 일상 생활의 여러 분야에서 무선랜 사용이 증가할 것으로 예상되는 만큼 무선랜 보안은 더욱 중요한 이슈로 다루어지게 될 것으로 예상되고 있다.

본 장에서는 국내외의 무선랜 이용 현황과 보안 적용 현황에 대한 조사 결과를 서술한다.

제 2 절 무선랜 이용 현황

근래 활성화 되고 있는 무선랜은 크게 민간 부문 무선랜과 공공 부문 무선랜으로 나눌 수 있으며, 민간 부문 무선랜은 다시 정보통신서비스 제공자의 무선랜(ISP 무선랜[4])과 정보통신서비스 제공자에 해당되지 않는 사설 무선랜으로 다시 구분할 수 있다. 또 ISP 무선랜은 다시 이용주체와 영업특성의 차원에서 Hot Spot 무선랜[5]과 FMC 무선랜[6]으로 세분화 할 수 있다.

1. 해외 무선랜 이용 현황

---

4) ISP(Internet Service Provider)는 국내에서는 「전기통신사업법」 제2조제1항제1호에 따른 전기통신사업자와 영리를 목적으로 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자(정보통신서비스 제공자)로 정의된다.

5) 국내 통신업계에서는 와이파이존으로 불리운다.

6) FMC(Fixed Mobile Convergence)는 유무선융합기술을 가리키고, 특히 무선랜기반 인터넷전화 기술을 말한다.

가. 와이파이존의 수 조사

미국 지와이어(Jiwire)의 '10년 1/4분기 조사자료[7]에 따르면 지난 4월 현재 전세계 140개국에서 무선랜 접속이 가능한 와이파이존 내지 Hot Spot은 약 295,481곳이고, 전세계적으로 무선랜 접속이 가능한 장소의 숫자는 IEEE802.11g 표준이 도입된 2004년 이후 5년간 439% 증가하였고 특히 '08년과 '09년 사이에는 21.9% 증가하였다.

(그림 2-2) 무선랜 접속 가능 장소의 증가

그 중 와이파이존 내지 Hot Spot이 가장 많은 나라는 미국으로 76,425곳에 달했고, 중국이 39,357곳으로 그 뒤를 이었다. 이어 영국, 프랑스, 독일, 러시아 등도 우리나라보다 와이파이존 수가 더 많았다.

---

7) http://www.jiwire.com/downloads/pdf/JiWire_MobileAudienceInsightsReport_Q12010.pdf (2010. 7. 24 방문) 미국 무선인터넷 기업 'Jiwire'의 '10년 1/4분기 조사자료. 전 세계 140개국의 주요 협력사로부터 제공받은 자료를 근거로 하였다.

[표 2-3] 주요 국가의 무선랜 접속 장소의 비교

순위	주요 국가	무선랜 접속 장소(개수)
1	미국	76,425
2	중국	39,357
3	프랑스	29,800
4	영국	27,966
5	독일	15,028
6	러시아	14,705
7	대한민국	12,817
8	일본	12,056
9	스웨덴	7,221
10	스위스	5,514

나. 무선랜 사용 장소의 빈도 조사

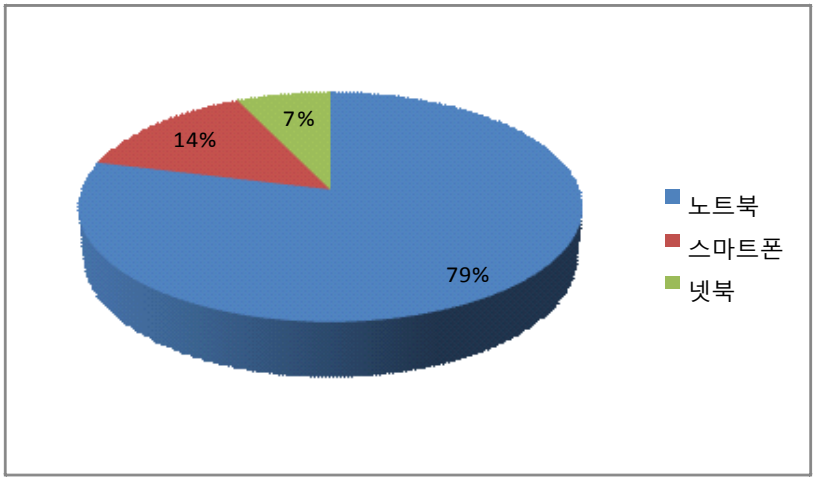
미국의 경우 사용자들이 무선랜을 사용하는 장소가 어디인지 조사한 결과 무선랜 사용 장소는 호텔 내지 리조트(60.0%), 카페(18.1%), 공항(14.7%) 순으로 많았고, 그 중 무료 서비스가 42.5%였으며 이 비율은 지난 분기 대비 약 5%가 증가한 수치였다[8]. 전세계 평균 무료 서비스 비율은 미국보다 낮은 21.4%였다.

다. 사용자들이 무선랜 접속에 사용하는 기기와 무선랜 접속의 목적

노트북을 사용하여 무선랜에 접속하는 사용자가 79%로 비율이 높으나, 스마트폰을 사용하여 무선랜에 접속하는 사용자의 비율이 빠른 속도로

8) 종전에 유료로 무선랜 서비스를 제공하였던 반즈앤노블(Barnes and Noble's), 보더즈(Borders), 맥도널드 등의 소매점이 무료 서비스로 전환하였다.

증가하고 있으며, 특히 모바일 무선랜 사용자들(on-the-go users)의 56%는 스마트폰을 사용하여 무선랜에 접속하고 있다. 미국의 경우 모바일 무선랜 사용자들이 무선랜을 통해 실행시키는 응용프로그램은 페이스북(Facebook)이나 트위터(Twitter)와 같은 소셜네트워킹이 가장 많았다[9]. 그 다음으로 날씨정보, 뉴스, 여행정보, 음악 등 엔터테인먼트, 게임 순이었다.



(그림 2-3) 미국에서 무선랜 접속에 1차적으로 사용되는 기기의 비율(Primary Device Usage)

2. 국내 무선랜 이용 현황

스마트폰 시대가 열리면서 이동통신사들이 와이파이존 구축 확대에 나서는 가운데 2010. 4. 기준 우리나라의 와이파이존은 모두 12,817곳으로 집계됐다[10][11]. 무선인터넷 수요가 크고 유동인구가 많은 곳 위주로 집중

9) 미국에서 스마트폰 사용자의 약 63%가 소셜네트워킹 애플리케이션 목적으로 무선랜에 접속하고 있었다.
10) 2010. 6. 11. 정보통신산업진흥원 자료
11) 여기에서의 '와이파이존'이란 대부분이 ISP들이 제공하는 무선랜을 말하는 것이고, 개인이 가정이나 사무실에서 임의로 설치하는 사설 무선공유기는 포함되지 않는 것

구축하며, Hot Spot 개념보다 이동성 등을 감안한 Zone개념으로 구축하고 있다.

이를 지역별로 살펴보면 전체의 5분의 1가량인 2,750곳이 서울에 위치한 것으로 나타났고, 경기도가 1,969곳으로 그 뒤를 이었다. 이어 경상북도에 1,030곳의 와이파이존이 설치된 것으로 조사됐고, 대구(989곳), 인천(924곳), 부산(902곳) 등 주로 대도시나 광역시에 와이파이존이 상대적으로 많았다. 경상남도는 713곳, 강원도는 607곳, 전라북도는 596곳의 와이파이존을 보유했고, 충청북도(529곳), 충청남도(509곳), 대전(441곳), 전라남도(430곳) 등이 뒤를 이었다. 제주도에는 모두 246곳의 와이파이존이 있는 것으로 집계됐고, 울산은 전국에서 가장 적은 179곳의 와이파이존이 있는 것으로 나타났다.

국내 와이파이존의 대부분은 KT가 구축한 쿡앤쇼존으로 KT는 올해 9월까지 전국 3만여곳, 연말까지 4만여곳으로 확대할 계획이다[12]. KT의 분석에 따르면 전체의 절반 이상이 대학교와 도서관에 설치되어 있고, 카페 내지 레스토랑, 관공서, 백화점 내지 할인마트, 금융기관 등에서도 이용 가능하다.

SK텔레콤도 개방형 와이파이존인 'T스팟'(T spot)을 전국 1만5천여곳에 구축키로 하고 지난 3월부터 구축을 진행하고 있다. 구축 지역은 극장, 대형 쇼핑몰, 공항, 터미널, 철도역사, 주요 번화가, 레저시설, 패밀리 레스토랑, 카페, 백화점, 할인점, 병원 등이다. 특히 SK텔레콤은 최근 부산 도시철도 4개 노선 108개 역사에 대한 개방형 와이파이존 구축 계획을 발표했다[13].

LG유플러스도 연내 1만1천곳, 2012년까지 5만곳의 와이파이존을 구축

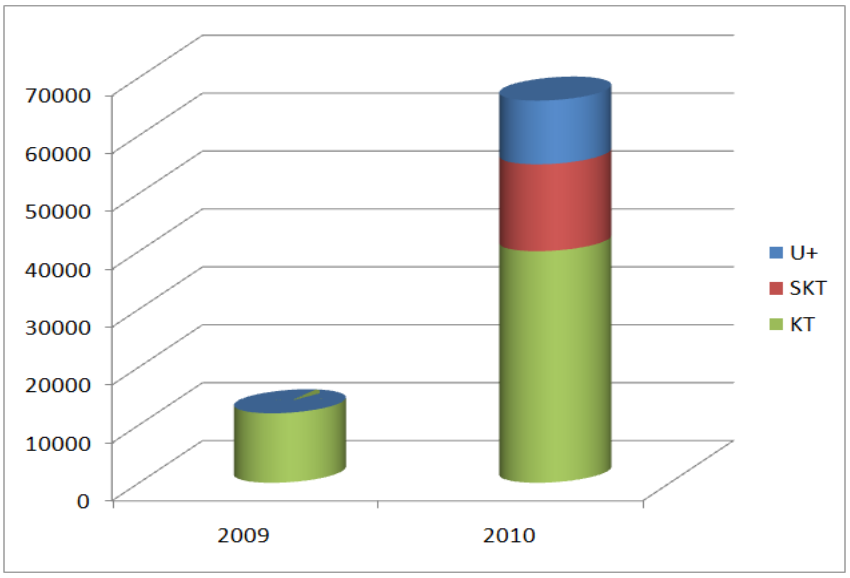
이므로 실제로 접속이 가능한 와이파이존은 훨씬 더 많을 것으로 추산된다.

12) http://news.mk.co.kr/outside/view.php?year=2010&no=383443(2010. 7. 24. 방문).

13) SK텔레콤은 타사 가입자의 접속도 무료로 허용하는 개방형 무선랜 정책을 취하여 KT의 무선랜 인프라를 공용자산화하라는 압력을 가하고 있다. 무료의 개방형 무선랜 정책을 취한 이유는 유무선 결합상품 경쟁이 이미 시작된 상황에서 무선랜만 떼어내어 망이용대가를 산정하는 것이 어려울 뿐만 아니라 포털 등 인터넷 서비스 사업자와의 공평성 시비도 우려가 되기 때문이다. 이는 궁극적으로 망중립성 이슈로 귀결될 것이다.

할 계획이라고 발표하였다. LG유플러스는 현재 전국 180만개에 달하는 인터넷전화용 무선 AP의 활용 방안으로서 희망 고객에 한해 공유하는 방안을 적극 검토 중이다[14].

KT, SK텔레콤, LG유플러스 통신3사가 연말까지 구축하기로 한 와이파이존을 더하면 모두 6만6천곳에 달하게 돼 우리나라의 와이파이망은 세계 2위, 면적대비 세계 최고 수준으로 올라갈 것으로 예상된다.



(그림 2-4) 국내 와이파이존의 증가

방송통신위원회가 2009년 발표한 제2차 무선인터넷 활성화 추진계획에 의하면 무선인터넷 트래픽 증가로 인한 기간망 혼잡을 피하기 위하여 이동통신사의 네트워크와 무선랜 간 결합서비스를 제공하도록 유도하게 된다[15]. 즉, 이동 중에는 휴대폰으로 이동통신망을 이용하고, 고정된 곳

14) http://economy.hankooki.com/lpage/industry/201007/e2010072014235147580.htm (2010. 7. 24. 방문).

15) SK텔레콤은 KT의 무선랜 인프라에 대항하기 위하여 T스팟의 확충과 더불어 데이터 무제한 서비스를 제공할 계획이다. 데이터무제한 서비스는 와이파이와 같이 지정된 장소에서만 접속할 수 있는 것이 아니라 3G 망을 통하여 이동 중에도 사용할 수 있는 장점이 있다. 그러나 무선데이터 활성화를 위해 3G 망의 성능 향상 및 차세

에서는 스마트폰으로 무선랜을 통하여 유선 초고속인터넷을 무료로 이용하게 되면, 이용자 측면에서도 요금에 대한 부담도 줄게 된다.

제 3 절 무선랜 보안 동향

1. 무선랜 보안상 취약점

무선랜은 공기를 전송 매체로 사용하는 기술의 특성상 많은 취약점이 존재한다. 또한 불특정 다수의 신호 수신이 가능함으로 인해 도청이 가능하고 무선 전파를 전송하는 무선 장비에 대한 공격이 가능하다.

무선랜, 특히 사설 무선랜은 가정 또는 일반 사무실 환경에서 기존 유선 인터넷망을 확장하여 사용되는 경우가 많기 때문에 대부분이 기존의 유선 네트워크에 무선 AP를 연결한 후 무선랜 기능이 있는 노트북 PC 또는 스마트폰을 사용하여 접속하고 있다. 따라서 유선 네트워크와 무선랜의 보안상 무단접속 차단은 전혀 고려되지 않는 경우가 많으며 이로 인하여 보안상 취약점이 문제된다. 무선랜의 보안상 취약점은 크게 물리적, 기술적, 관리적 취약점으로 나눌 수 있다.

가. 물리적 취약점

무선 AP가 외부인에 노출되는 경우에는 외부인에 의한 장비의 파손, 전원 케이블의 분리 등 전원 리사이클링, 이더넷 케이블의 분리, 장비 리셋을 통한 설정값 초기화 등의 문제가 발생할 수 있다. 특히 장비 리셋의 경우에는 정당한 권리를 가진 관리자라 할지라도 그의 실수로 또는 정전사고로 인하여 무선 AP가 리셋됨으로써 보안 설정값이 초기화

대 네트워크인 LTE(Long Term Evolution) 구축 등 통신망 확충 비용이 크다; http://www.betanews.net/article/500089(2010. 7. 14. 방문).

되어 보안상 문제가 발생하는 사례가 존재한다.

나. 기술적 취약점

무선랜의 기술상 특성을 악용하는 도청, 서비스거부[16], 불법 AP[17] (Rogue AP) 등의 보안 공격이 존재한다. 특히 무선 데이터가 암호화 되어 있지 않은 경우 모든 전송 데이터를 도청할 수 있어 심각한 문제를 일으킬 수 있다.

다. 관리상 취약점

장비가 파손되거나 도난당하여도 이를 파악하지 못하는 경우, 무관심으로 인해 무선랜 장비에 보안기능을 미설정하고 장비가 제공하는 기본값 혹은 초기값을 사용하는 경우, 무선 AP의 전파 출력 조정을 하지 않아 외부로 무선랜 전파가 유출되는 경우 공격자의 표적이 될 수 있다

2. 무선랜 보안 기술

무선랜 보안 기술은 사용자로 하여금 접속허용을 나타내는 일정 형태의 징표를 제시하도록 하고, 미리 등록된 사용자 데이터베이스에 존재함을 확인한 후 접속을 허가하는 '접속인증기술'과 무선으로 전송되는 데이터의 실제 내용을 허가받지 않은 사람이 볼 수 없도록 은폐하기 위해 데이터를 암호로 바꾸는 '데이터암호화기술'로 구분할 수 있다. 다만 실제 로는 두 가지 기술이 혼합되어 구현되는 경우도 많다.

---

16) 서비스 거부(DoS)란 해킹수법의 하나로 한명 또는 그 이상의 사용자가 대량의 무선 패킷을 전송함으로써 시스템이 더 이상 정상적인 서비스를 할 수 없도록 만드는 공격 방법이다. Distribute Denial of Service attack(DDoS)는 여러 대의 컴퓨터를 일제히 동작하게 하여 특정 사이트를 공격하는 DOS 해킹 방식의 하나이다.

17) 공격자가 불법적으로 무선 AP를 설치하여 무선랜 사용자들의 전송 데이터를 수집하는 행위를 말한다.

가. 무선랜 접속인증기술

무선랜 표준이 제공하는 사용자 인증은 네트워크ID(SSID), MAC 주소 인증, WEP 공유키 인증, IEEE 802.1x 프로토콜 등이 있고, USIM 카드가 장착된 단말기의 경우 이동통신망을 이용한 인증 등 무선랜 표준 외의 방법으로 사용자 인증을 할 수도 있다[18]. WEP 방식은 데이터 암호화 기술 부분에서 설명하기로 하고 우선 SSID 인증, MAC 주소 인증, IEEE 802.1x 인증에 대하여 설명한다.

(1) SSID 설정을 통한 접속제한

접속하려고 하는 무선 AP의 SSID[19]를 모르는 사용자는 무선랜에 접속을 시도할 수 없게 된다. 무선랜 관리자가 SSID를 브로드캐스트하지 않도록 설정하고 정당한 권한을 가진 사용자에게만 미리 SSID를 알려 주고 그 사용자로 하여금 알려준 SSID로 연결을 시도하도록 한다면 SSID를 모르는 공격자의 연결 시도에 방어할 수 있다. 그러나 이러한 단순한 접근 제한 방법에는 무선랜 분석 도구를 이용하여 SSID를 알아낼 수 있는 취약점이 있다. 또한 사용자가 SSID를 직접 입력하지 않더라도 무선랜 단말기가 알아서 수신되는 AP들의 신호를 비교하여 가장 좋은 품질의 신호를 보내오는 AP에 자동으로 접속을 시도하는 방식도 존재하여 SSID 접속제한

18) SK텔레콤은 7월 이후 출시되는 휴대폰은 단말부터 암호화가 구현된 가입자식별모듈(USIM) 인증을 적용하고 올해 3월 이후 출시된 단말기는 이동통신망을 통해 자동 인증 처리하고 있다. 타사 가입자는 주민번호를 이용한 실명인증을 도입했다. KT는 USIM 기반 사용자 인증과 WPA 데이타암호화기술을 적용해 기존 MAC 인증방식의 취약점이었던 ID 패스워드나 MAC 주소 도용의 위험성을 없애겠다고 발표하였다. LG유플러스는 7월부터 기존 대비 보안이 강화된 802.1x 인증체제를 도입할 계획"이라고 발표하였다; http://www.dt.co.kr/contents.html?article_no=2010071402010151742002 (2010.7.14. 방문).

19) Subsystem Identification의 약자로 AP가 제공하는 무선랜 서비스 영역을 식별하기 위해 사용하는 ID를 말한다.

방식은 가장 취약한 접속제한 방식에 불과하다.[20]

많은 사용자들은 운영상의 편의를 위해서 사용자들끼리 서로의 자료에 접근할 수 있도록 공유폴더를 만들어 네트워크상에 개방하고 있어서 공격내지 정보유출의 대상이 되고 있다. 정보보안의 관점에서는 공유폴더를 만들지 않는 것이 가장 좋으나 꼭 사용해야 할 경우에는 공유폴더에 접속이 허용된 사용자 리스트와 접속에 필요한 암호를 설정하여 사용해야 한다

(2) MAC 주소 인증

MAC 주소[21] 필터링은 공격의 위험을 줄이는 간단한 방법이면서 네트워크규모에 상관 없이 적용할 수 있는 보안기술로 알려져 있다. 설정방법 또한 간단하고 기본적인 공격을 방어하는데 효과적이다. 현재 시중에 판매되는 대부분의 무선 AP에서 지원되는 보안기능이다. 그러나 무선랜 장비가 많은 대규모 기관에서는 사용자의 MAC 주소를 관리하기 위한 업무가 과도해지고, 장비에 저장되어 있는 MAC 주소 정보가 외부로 노출될 수 있다는 문제가 있다.

(3) IEEE 802.1x 인증

고정된 공유키 값을 사용하는 WEP 인증의 취약점을 보완하고자 802.1x 표준은 인증서버를 이용하는 동적 WEP을 규정하였다. 인증서버가 사용자가 접속을 시도할 경우에 인증을 수행하고, 기관에서 사용하는 WEP 키의 설정과 갱신 등의 관리를 수행한다. 하나의 연결마다 새로운 WEP 키값을 부여하면, WEP 키값의 외부 유출시 피해가 적어지게 된다.

---

20) HotSpot 서비스를 원활하게 제공하기 위해서 발전한 기술적 방식이다.

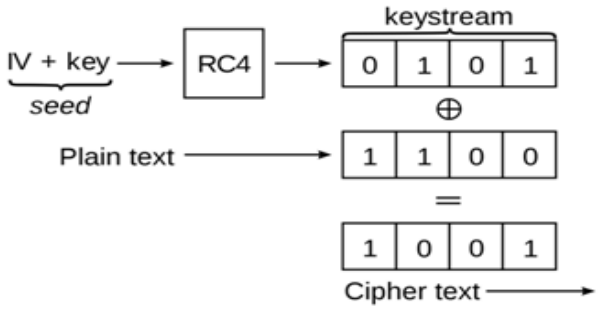
21) MAC 주소는 네트워크 접속장비인 랜카드에 부여되는 48bit의 주소 값으로 랜카드 제조회사가 완성된 랜카드 제품을 출시할 때 하드웨어에 부여하는 값을 말한다. 하나의 랜카드에 부여되는 MAC 주소값은 유일한 값으로 네트워크기기를 식별하는데 사용된다.

하지만, 동적 WEP의 적용도 WEP이 갖던 단방향 인증으로 인한 한계가 존재하였고, 이를 해결하고자 802.1x 표준에서는 EAP 인증 기능을 제공하고 있다. EAP(Extensible Authentication Protocol)란 그 위에 MD5, TLS, TTLS, PEAP[22] 등 다양한 종류의 인증 방식의 패킷을 캡슐화 하여 전송하는 프로토콜이다[23]. 그 사용자 인증 방식에 따라 각각 EAP-MD5, EAP-TLS, EAP-TTLS, PEAP 등으로 불리운다.

나. 무선전송 데이터 암호화 기술

(1) WEP(Wired Equivalency Protocol)

IEEE 802.11b에서 처음으로 무선 전송 데이터의 암호화에 대한 내용이 포함되었는데 802.11b에서 정의된 WEP는 40비트의 WEP 공유비밀키와 임의로 선택되는 24비트의 Initialization Vector(IV)로 조합된 총64비트의 키를 이용한 RC4 스트림 암호화 방식으로 MAC 프레임들을 보호한다.



(그림 2-5) WEP 데이터 암호화 방식

22) TLS(Transport Layer Security), TTLS(Tunneled Transport Layer Security), PEAP(Protected Extensible Authentication Protocol).

23) 사용자와 AP 사이에는 EAPOL(EAP over LAN)프로토콜을 통해서 패킷을 전송하고, AP와 인증서버 사이에는 RADIUS(Remote Authentication Dial-in User Services) 프로토콜을 통해서 패킷을 전송한다. 일부에서는 AP와 인증서버 사이의 프로토콜을 RADIUS over LAN이라고 설명하기도 한다.

WEP 암호화 방식의 문제점은 초기벡터 값의 짧아서 재사용 가능성이 높다는 점, 불완전한 RC4 암호화 알고리즘 사용으로 인하여 암호키 노출 가능성이 높다는 점, 짧은 길이의 암호키 사용으로 인하여 공격 가능성이 높다는 점 등이다. 간단한 도구를 이용해 암호화 key 값을 알아내는 것이 가능한 상황이다. WEP 암호는 카페라테 공격방법[24]으로 6분 이내 해독 가능하다고 알려져 있다.

(2) WPA/WPA2(WiFi Protected Access)

2004년에 제정된 IEEE 802.11i 표준[25]에는 WPA1과 WPA2[26] 규격이 포함되어 있다. 또한 무선랜 인증방식에 사용되는 모드[27]에 따라 WPA-개인과 WPA-엔터프라이즈로 구분되어 진다.

WPA/WPA2의 경우에는 WEP과 달리 무선 데이터 전송시 고정된 키 값을 이용해 무선 전송 데이터를 암호화하지 않으므로 단순히 무선 전송 데이터 패킷의 수집을 통해서는 무선 전송 데이터의 암호화 키값을 유추해낼 수는 없다. 현재의 무선랜 표준으로서는 IEEE 802.11i가 가장 보안에 안전한 방식으로서 WPA 인증방식은 별도의 무선 인증서버를 사용하지 않는 일반 가정이나 소규모 사무실 환경에서 가장 효율적인 보안 강화 방안으로 인정받고 있다.

그러나 무선랜의 가장 우수한 보안기술로 인정받아온 WPA2마저도

---

24) http://www.airtightnetworks.com/home/resources/knowledge-center/caffe-latte.html (2010. 7. 10. 방문).

25) 무선 장비와 단말기간의 가상 인증 기능을 제공하는 EAP(Extensible Authentication Protocol)의 도입 등 검증된 보안기술들이 포함되어 보다 강화된 인증과 데이터 암호화 기능을 제공한다.

26) WPA1은 TKIP(Temporal Key Integrity Protocol)을 WPA2는 CCMP 암호화 방식을 사용한다.

27) WPA-개인은 PSK 모드를 사용하는 경우를 WPA-엔터프라이즈는 Radius 인증서버를 사용하는 경우를 말한다. PSK 인증방식은 별도의 인증서버가 설치되어 있지 않은 소규모망에서 사용된다.

보안상 취약점이 발견되었다는 보도가 등장하고 있는 상황이다.[28] 물론 이에 대해 전문가의 추측일 뿐 그 위험에 현실적으로 직면해 있는 것은 아니라는 반론도 존재하지만, 무선랜 보안의 기술의 한계를 보여주는 실례로 평가할 수 있다.

3. 해외 무선랜 보안 적용 실태

가. 세계 공항 대상 무선랜 스캔 보고서[29]

(1) 조사 방법

2008년 1월부터 3.까지 27개 공항(미국 20, 유럽 2, 아시아 5)의 796개 무선 AP를 조사대상으로 삼아 공항내의 무작위로 선택한 장소들에서 5분간 무선랜 신호를 스캔하고 데이터 수집장치에 신호내용을 기록하였다.

(2) 무선전송 데이터의 암호화 현황

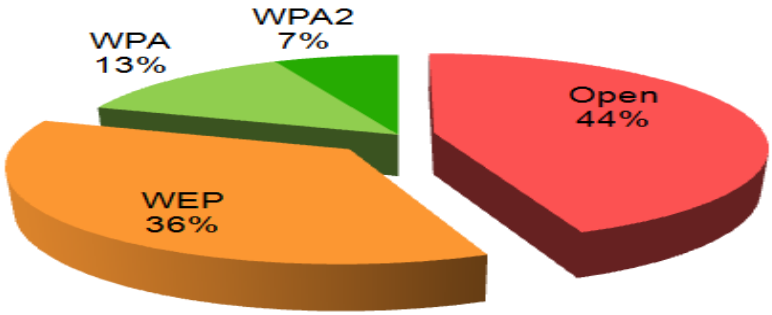
조사 대상 중 59% 이상이 보안 설정 없이 운영하고 있었고, 21% 이상이 보안이 취약한 WEP 암호화 방식을 사용하고 있는 결과 총 80% 이상의 무선 AP가 보안이 취약한 상태에서 동작하고 있었다. 특히 사설 AP의 경우 ISP 무선랜[30]이 아닌데도 OPEN(보안 미설정)되어 있는 AP가 44%에 이르렀다.

---

28)http://www.idg.co.kr/newscenter/common/newCommonView.do?newsId=622092010. 6. 11.(2010. 7. 26. 방문).

29) 'Air Tight Networks사'(美 보안솔루션 업체)의 세계 27개 공항 대상 무선랜 취약성 조사 결과; http://www.airtightnetworks.com/home/resources/knowledge-center.html (2010. 7. 10. 방문).

30) 77%의 AP가 사설 무선랜 AP였고 23%가 ISP 무선랜 AP였다. ISP 무선랜 AP는 OPEN되어 있고 SSID를 공개적으로 방송(tmobile, concourse, attwifi 등)하고 있었다.



(그림 2-6) 조사대상 공항내 무선랜 AP의 보안 상태

(3) 무선랜 접속시 인증보안 현황

무선랜 사용자들은 그들의 의사와 상관없이 네트워크 정보(이전에 접속했던 SSID, 보안셋팅 등)를 전송하고 있어서 이러한 SSID를 모용하여 접속자 정보를 빼내는 Honeypot 공격에 노출 위험에 처해 있었다.

무선랜 접속자의 10% 이상에 해당하는 무선랜 단말기가 그의 의사와 상관없이 무선랜 바이러스(Viral WiFi[31])에 감염된 SSID를 전송하고 있었고, 해커는 공유 폴더 내의 자료 접근 가능한 상태였다.

나. 세계 금융가 대상 무선랜 스캔 보고서

(1) 조사 방법

2009년 1월부터 3월까지 7개 금융기관 밀집지역(미국 6, 영국 1)의 3,632개 무선 AP와 547명의 무선랜 사용자를 조사대상으로 삼아 각 밀집지역 내에서 무작위로 선택한 30개의 장소에서 5분간 무선랜 신호를 스캔하고 데이터 수집장치에 신호내용을 기록하였다[32].

---

31) 무선랜 바이러스는 애드혹(ad hoc) 모드의 바이러스 SSID를 말한다. 무선랜 바이러스는 감염된 무선랜 단말기로부터 다른 단말기로 전파된다; http://www.airtightnetworks.com/home/resources/knowledge-center/viral-ssid.html(2010. 7. 10. 방문).

32) 'Air Tight Networks사'의 세계 7개 금융가 대상 무선랜 취약성 조사 결과. Financial

(2) 무선전송 데이터의 암호화 현황

조사 대상 중 24% 이상이 보안 설정 없이 운영하고 있었고, 33% 이상이 보안이 취약한 WEP 암호화 방식을 사용하고 있는 결과 총 57% 이상의 무선 AP가 보안이 취약한 상태에서 동작하고 있었다[33].

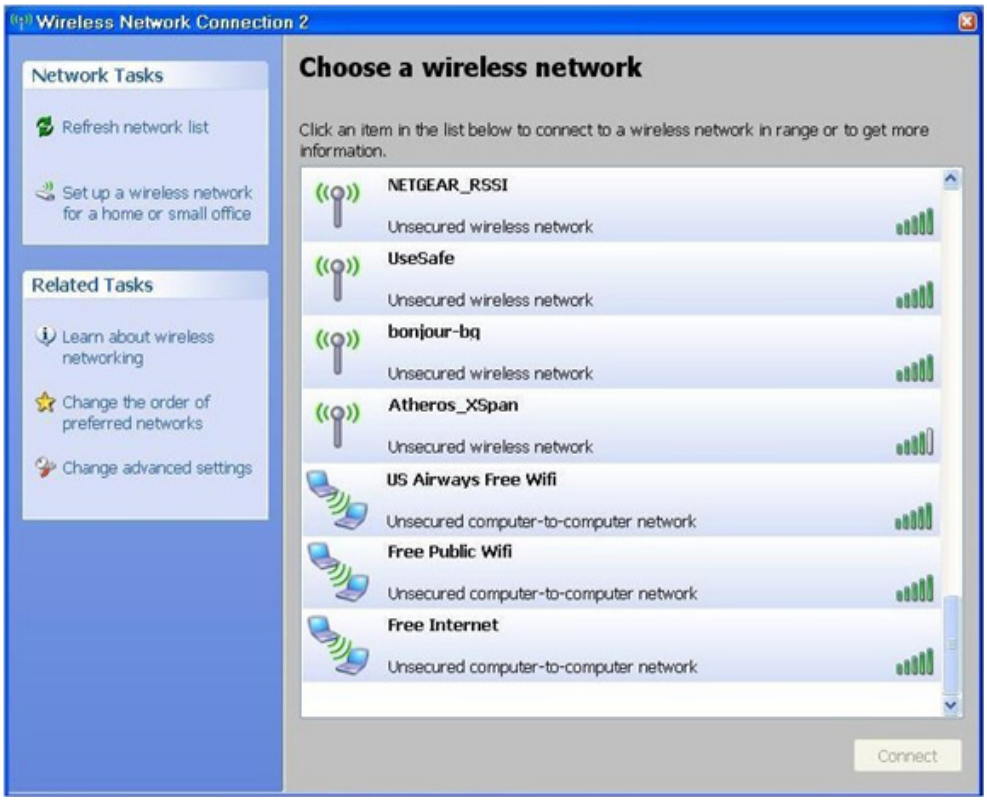
(3) 무선랜 접속시 인증보안 현황

무선랜 사용자 중 56%가 그들의 의사와 상관없이 네트워크 정보(이전에 접속했던 SSID, 보안셋팅 등)를 전송하고 있어서 이러한 SSID를 모용하여 접속자 정보를 빼내는 Honeypot 공격에 노출 위험에 처해 있었다.

무선랜 접속자의 13% 이상에 해당하는 무선랜 단말기가 그의 의사와 상관없이 무선랜 바이러스(Viral WiFi)에 감염되어 애드혹(ad hoc) 모드에서 동작하며 바이러스 SSID를 전송하고 있었다. 공유폴더에 저장된 펀드매니저의 개인정보가 유출 가능한 상태였다. "Free Public WiFi", "Free Internet Access" 등의 바이러스 SSID가 널리 퍼져 있었다.

Districts Wireless Vulnerability Study(2009). http://www.airtightnetworks.com/home/resources/knowledge-center/ financial-districts-scanning-report.html(2010. 7. 10. 방문).

33) Enterprise 무선랜 AP가 39%이고 개인용 무선랜 AP가 61%.



(그림 2-7) 바이러스 SSID의 예

4. 국내 무선랜 보안 적용 실태

가. 서울시내 사설 무선랜 보안 운영 조사 결과

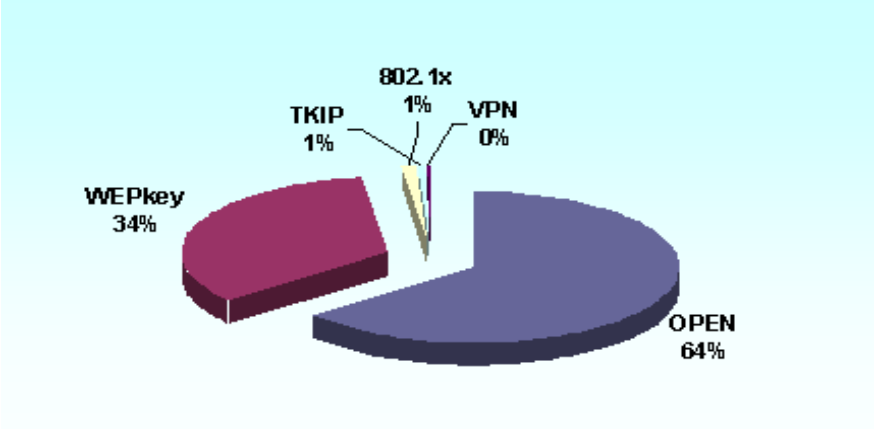
(1) 조사 방법

2006년 서울시 강북, 강남 12개 지점에서 수집된 무선랜 사용자 단말기 4,008대와 무선랜 AP 총 830대를 대상으로 조사하였다[34].

34) 정현철, "무선랜 보안 실태 조사 및 분석을 통한 보안 강화 방안 연구", 제25회 한국정보처리학회 춘계학술발표대회 논문집 제13권 제1호, 2006. 5.

(2) 무선전송 데이터의 암호화 현황

무보안 AP는 조사대상 AP의 64%에 달하였고 WEP 방식을 적용한 경우는 34%였다[35].



(그림 2-8) 무선 AP에서 사용하고 있는 무선랜 보안 기술

나. 강남역 무선랜 보안 운영 조사 결과

(1) 조사 방법

2009년 강남역 8개 구역에서 수집된 무선랜 AP 총 119대를 대상으로 조사하였다[36].

(2) 무선전송 데이터의 암호화 현황

사설 AP의 28%가 무보안 상태였고, 72%가 WEP/WPA 인증방식

35) '06. 9. 성균관대학교 인터넷보안연구실(최형기 교수)에서 서울시내 주요 백화점 10곳을 대상으로 조사한 결과 무보안 상태인 곳이 2곳, WEP을 적용한 곳은 8곳으로 나타났다.
36) 2009년 KT의 조사자료; 무선 인터넷 2.0 시대의 WiFi 활용 방향, 2010. 3.

적용하고 있었다. LGD AP의 경우 WEP Key(123456789a)로 접속 가능한 상태였다.

5. 취약한 무선랜 보안 적용 실태에 대한 대책

가. 보안설정의 간편화

기존에는 무선을 안전하게 사용하고 연결하기 위해서는 다음의 절차를 취하여야 했다.

1) 무선 AP에 연결된 PC에서 http://192.168.0.1/ 에 접속하여 아래 그림과 같이 SSID, 채널, 모드, 암호화 변수, 무선보안키 등을 입력한다.
2) 단말기에서 주변 무선을 검색한 후 해당 SSID를 설정한다.
3) 무선 AP에 입력한 무선보안키 값을 단말기에 입력해 주어야 한다.

이러한 보안설정 과정은 기술지식이 부족한 일반 사용자에게 지나치게 복잡한 절차라는 점이 보안성이 취약한 무선 AP가 많은 실태의 원인으로 지적되어 왔다.

(그림 2-9) 무선 AP의 보안설정 화면

가정과 소규모사무실의 경우 이러한 보안설정을 간편하게 하기 위하여 와이파이연합(WiFi Alliance)은 2007년 WiFi Protected Setup(WPS)이라는 표준 및 인증프로그램을 제정하였다[37]. 이 기능을 통하여 일반 사용자들도 간편하게 보안설정을 하고 신규 단말기를 무선랜에 연결할 수 있는 방법이 제공되었다.

이러한 WPS 기능[38] 특히 PBC 방식(버튼 방식)[39]을 사용하면 다음과 같이 보안설정 및 연결 과정이 간편하게 된다.

1) 노트북에서 무선관리 프로그램을 역고 WPS 버튼을 클릭한다.
2) 120초 간의 대기시간이 진행되는 동안 무선 AP에 달려있는 WPS 버튼을 누른다.
3) 잠시후 자동으로 무선이 연결될 뿐만 아니라 무선보안키값도 자동으로 생성되어 적용된다.

와이파이연합에서 일반 사용자들의 보안설정절차를 간편하게 함으로써 취약한 보안실태 문제를 완화시키기 위하여 2007년 WPS 표준을 제정하였으나 아직 널리 보급이 되지 않았다.

나. 보안 현황 점검

무선 AP의 취약한 보안 실태 문제를 완화하기 위해 사업자나 이용자에게 보안설정 등 정보보호조치 의무를 부과하거나 행정청에게 보안현황을 점검할 권한을 구체적으로 규정한 현행법은 없다. 다만 안전 진단 기준, 개인정보 보호 조치 기준, 가이드라인 등의 개정을 통해서 용이하게 적용할 수 있는 조항은 일부 존재하고 있다. 무선 AP의 보안 강화를 위하여 주체별 적용을 고려해 볼 만한 현행법은 다음과 같다.

---

37) http://www.WiFi.org/wifi-protected-setup(2010. 7. 10. 방문).
38) 그러나, 이 기능이 Windows Vista 이상에서만 지원되기 때문에 Windows XP 가 설치된 노트북을 사용할 경우 문제가 발생할 수 있다.
39) WPS 에는 PIN 방식도 제공된다.

[표 2-4] 행정청의 무선랜 보안 점검의 법적 근거 검토

의무 주체	현행법
o 무선AP를 제공하는 사업자 (ISP)	정보통신망법
o 사설 무선 AP 사용자 (개인, 기업 등)	법적 근거 없음
o 공공무선랜(Municipal Wireless network)을 운영하는 지방자치단체 등 공공기관	전자정부법
o 무선AP를 수입・제조하여 판매하는 자	전파법
o 호텔, 공항 등 무선AP를 설치하여 고객에 대한 무선랜서비스 제공자	정보통신망법

(1) 정보통신망 이용촉진 및 정보보호 등에 관한 법률

방송통신위원회는 정보통신망 이용촉진 및 정보보호 등에 관한 법률(이하 정보통신망법) 제46조의3 제1항[40] 을 정보보호 안전진단의 일부로서 안전진단 수행기관을 통하여 해당 ISP를 대상으로 무선랜 보안 현황을 점검할 수 있는 법적 근거로 삼을 수도 있을 것이다. 그러나 이 규정의 적용을 받을 주체는 극히 제한적이므로, 정보통신서비스 제공자에 해당되지 않는 사설 AP의 경우에는 이러한 안전진단을 받아야 할 법적 의무가 없다. 따라서 무선랜 공급의 상당한 비율을 차지하는 동시에 보안에

40) 제46조의3 (정보보호 안전진단) ① 다음 각 호의 어느 하나에 해당하는 자는 방송통신위원회가 안전진단을 수행할 수 있다고 인정한 자(이하 "안전진단 수행기관"이라 한다)로부터 자신의 정보통신망 또는 집적정보통신시설에 대하여 매년 정보보호지침에 따른 정보보호 안전진단을 받아야 한다. 이 경우 안전진단 수행기관은 15명 이상의 정보보호 기술인력을 보유하고 최근 3년 이내에 정보보호컨설팅을 수행한 실적이 있는 법인이어야 한다.
1.「전기통신사업법」 제2조제1항제1호에 따른 전기통신사업자로서 전국적으로 정보통신망서비스를 제공하는 자(이하 "주요정보통신서비스 제공자"라 한다)
2. 집적정보통신시설 사업자
3. 정보통신서비스 제공자로서 매출액, 이용자 수 등이 대통령령으로 정하는 기준에 해당하는 자

가장 취약한 사설 AP의 경우에는 행정기관의 무선랜 보안 점검을 실시할 법적 근거가 현행법상으로는 전혀 존재하지 않는다.

(2) 전파법

전파법 제53조 제1항[41]은 방송통신위원회에게 무선설비규칙을 위반한 자에 대하여 소속 공무원에게 조사 또는 시험할 수 있는 권한을 부여하고 있다.

무선설비규칙(제98조)에 무선랜 보안 관련 규정을 신설하게 되는 경우에는, 방송통신위원회는 동법 제53조 제1항을 해당 ISP나 사설AP 소유자 등을 대상으로 무선랜 보안 현황을 점검할 수 있는 법적 근거로 삼을 수 있는 여지가 있다. 그러나 현행 무선설비규칙을 그대로 적용하는 한 전파법에 따라 AP가 무선설비규칙을 위반하였는가를 점검할 법적 근거는 미비하다고 할 것이다.

(3) 전기통신사업법

전기통신사업법 제38조의2제2항[42]의 "전기통신역무의 품질"의 개념을 "무선랜 보안수준"을 포함하도록 포괄적으로 해석할 수 있다면, 방송통신위원회는 전기통신역무 품질평가의 일부로서 무선랜 역무를 제공하는 ISP를 대상으로 무선랜 보안 현황을 점검할 수 있는 법적 근거로 삼을

41) 제45조 (기술기준) 무선설비는 주파수 허용편차와 공중선전력 등 방송통신위원회 고시로 정하는 기술기준에 적합하여야 한다.
제53조 (조사 및 조치) ① 방송통신위원회는 제19조, 제25조, 제26조, 제29조, 제45조, 제46조, 제52조, 제57조 또는 제58조를 위반한 자가 있다고 인정되면 방송통신위원회 고시로 정하는 바에 따라 소속 공무원에게 조사 또는 시험하도록 할 수 있다.

42) 제38조의2(전기통신역무의 품질개선 등) ①전기통신사업자는 그가 제공하는 전기통신역무의 품질을 개선하기 위하여 노력하여야 한다.
② 방송통신위원회는 전기통신역무의 품질을 개선하고 이용자의 편익을 증진하기 위하여 전기통신역무의 품질평가등 필요한 시책을 강구하여야 한다.
③ 방송통신위원회는 전기통신사업자에게 제2항의 규정에 의한 전기통신역무의 품질평가 등에 필요한 자료의 제출을 명할 수 있다.

수 있다. 그러나 이는 Hot-spot이나 FMC에나 적용할 수 있을 것이다.

(4) 통신비밀보호법

통신비밀보호법은 범죄수사 또는 국가안보를 위한 통신제한조치와 긴급통신제한조치를 규정하고 있다. ISP나 사설AP 소유자 등을 대상으로 무선랜 보안 현황을 점검할 수 있는 법적 근거로 삼기에는 적절치 않다.

제 3 장 해외 무선랜 보안 법규와 정책

제 1 절 관련자에 대하여 의무를 부과하는 법규

1. 영국의 '디지털경제법'(Digital Economy Act 2010)

가. 개요

영국은 인터넷 규제를 강화한 '디지털경제법'에 근거하여 불법 파일 공유자의 인터넷 계정을 차단하고 공공장소에서의 일정 규모이상의 ISP에 대하여 무선랜 공급을 차단할 의무를 부과하는 등 다양한 정책들이 시행되었다.

구체적으로 인터넷서비스 제공자가 반복적으로 불법 파일공유를 시도하는 지식재산권 침해자의 인터넷 속도를 늦추거나 차단할 수 있으며, 대법원이 저작권 침해 자료를 다수 다루는 웹사이트를 폐쇄할 수 있는 근거 조항이 마련되었다.

나. 관련 법조문 (국문)

9 인터넷 접근을 제한할 의무: 평가와 준비[43)]

---

43) 9 Obligations to limit internet access: assessment and preparation
After section 124F of the Communications Act 2003 insert－
"124G Obligations to limit internet access: assessment and preparation
(1) The Secretary of State may direct OFCOM to－ .
(a) assess whether one or more technical obligations should be imposed on internet service providers;
(b) take steps to prepare for the obligations;
(c) provide a report on the assessment or steps to the Secretary of State.
(2) A "technical obligation", in relation to an internet service provider, is an obligation for the provider to take a technical measure against some or all

통신법(2003) 124F 뒤에 추가한다-

"124G 인터넷 접근을 제한할 의무: 평가와 준비

(1) 주무장관[44]은 OFCOM[45]에게 다음을 지시할 수 있다.

(a) 하나 또는 그 이상의 기술적 의무가 ISP에게 부과되었는지 평가할 것;

(b) 의무 준수를 준비하기 위한 절차로 나아갈 것

(c) 주무장관에게 평가와 절차 진행에 관한 보고서를 제공할 것

---

relevant subscribers to its service for the purpose of preventing or reducing infringement of copyright by means of the internet.

(3) A "technical measure" is a measure that−

(a) limits the speed or other capacity of the service provided to a subscriber;

(b) prevents a subscriber from using the service to gain access to particular material, or limits such use;

(c) suspends the service provided to a subscriber; or

(d) limits the service provided to a subscriber in another way.

(4) A subscriber to an internet access service is "relevant" if the subscriber is a relevant subscriber, within the meaning of section 124B(3), in relation to the provider of the service and one or more copyright owners.

(5) The assessment and steps that the Secretary of State may direct OFCOM to carry out or take under subsection (1) include, in particular−

(a) consultation of copyright owners, internet service providers, subscribers or any other person;

(b) an assessment of the likely efficacy of a technical measure in relation to a particular type of internet access service; and

(c) steps to prepare a proposed technical obligations code.

(6) Internet service providers and copyright owners must give OFCOM any assistance that OFCOM reasonably require for the purposes of complying with any direction under this section.

(7) The Secretary of State must lay before Parliament any direction under this section.

(8) OFCOM must publish every report under this section−

(a) as soon as practicable after they send it to the Secretary of State, and

(b) in such manner as they consider appropriate for bringing it to the attention of persons who, in their opinion, are likely to have an interest in it.

(9) OFCOM may exclude information from a report when it is published under subsection (8) if they consider that it is information that they could refuse to disclose in response to a request under the Freedom of Information Act 2000."

44) 영국에서 The Secretary of State는 미국에서의 국무장관과 달리 장관을 지칭하는 일반적인 표현이다. 이 법의 주무부서는 비즈니스혁신기술부이므로 이 법에서의 주무장관은 비즈니스혁신기술부 장관을 의미한다.

45) The Office of Communications

(2) ISP와 관련된 기술적 의무는 인터넷을 통한 저작권의 침해를 막거나 감소시키기 위한 목적으로 제공자가 일부 또는 전부의 관련 있는 이용자에 대하여 기술적 수단을 이용하도록 하는 의무이다.

(3) 기술적 수단이란 이하의 수단을 의미한다.

(a) 이용자에게 제공되는 속도 또는 다른 서비스의 용량을 제한하는 것;

(b) 이용자가 그 서비스를 특정 자료에 대하여 접근을 얻는 데 사용하는 것을 막는 것 또는 그러한 사용을 제한하는 것;

(c) 이용자에게 제공되는 서비스를 유예하는 것;

(d) 이용자에게 제공되는 서비스를 다른 방법으로 제한하는 것;

(4) 이용자가 서비스의 제공자와 하나 또는 그 이상의 저작권 소유자와 관련이 있는 124B(3)가 의미하는 관련된 이용자인 경우 인터넷 접근 서비스에 대하여 이용자는 관련성이 있다.

(5) 주무장관이 OFCOM에게 (1)항 아래서 수행하고 부담하도록 명령할 수 있는 평가와 절차는 특히 다음을 포함한다

(a) 저작권 소유자, ISP, 이용자 또는 다른 사람과의 상담;

(b) 인터넷 접속 서비스의 특정 유형과 관련된 기술적 수단의 효과성의 평가;

(c) 제안된 기술적 의무 규정을 준비하기 위한 절차

(6) ISP와 저작권 소유자는 OFCOM이 이 조항에 근거한 명령을 준수하기 위한 목적에서 요구하는 도움을 제공해야 한다.

(7) 주무장관은 국회에 이 조항에 근거한 명령을 제출해야 한다.

(8) OFCOM은 이 조항에 근거하여 보고서를 출판해야 한다.

(a) 그들이 보고서를 장관에게 제출한 후 가능한 빨리 출판해야 한다

(b) 보고서상 이해관계인에게 보고서를 전달할 수 있도록 적절한 고려를 하여 절차를 취해야 한다.

(9) 정보자유법에 근거한 요구에 대한 응답으로 공개를 거부할 수 있는 정보라고 여겨질 경우에는 OFCOM은 만약 보고서가 세부항목 (8)에 근거하여 출판되었을 때 보고서에서 그 정보를 배제해야 한다.

10 인터넷 접근을 제한할 의무[46)]

---

46) 10 Obligations to limit internet access
After section 124G of the Communications Act 2003 insert－
"124H Obligations to limit internet access
(1) The Secretary of State may by order impose a technical obligation on internet service providers if－
(a) OFCOM have assessed whether one or more technical obligations should be imposed on internet service providers; and
(b) taking into account that assessment, reports prepared by OFCOM under section 124F, and any other matter that appears to the Secretary of State to be relevant, the Secretary of State considers it appropriate to make the order.
(2) No order may be made under this section within the period of 12 months beginning with the first day on which there is an initial obligations code in force.
(3) An order under this section must specify the date from which the technical obligation is to have effect, or provide for it to be specified.
(4) The order may also specify－
(a) the criteria for taking the technical measure concerned against a subscriber;
(b) the steps to be taken as part of the measure and when they are to be taken.
(5) No order is to be made under this section unless－
(a) the Secretary of State has complied with subsections (6) to (10), and
(b) a draft of the order has been laid before Parliament and approved by a resolution of each House.
(6) If the Secretary of State proposes to make an order under this section, the Secretary of State must lay before Parliament a document that－
(a) explains the proposal, and
(b) sets it out in the form of a draft order.
(7) During the period of 60 days beginning with the day on which the document was laid under subsection (6) ("the 60-day period"), the Secretary of State may not lay before Parliament a draft order to give effect to the proposal (with or without modifications)
(8) In preparing a draft order under this section to give effect to the proposal, the Secretary of State must have regard to any of the following that are made with regard to the draft order during the 60-day period－
(a) any representations, and
(b) any recommendations of a committee of either House of Parliament charged with reporting on the draft order.
(9) When laying before Parliament a draft order to give effect to the proposal (with or without modifications), the Secretary of State must also lay a document that explains any changes made to the proposal contained in the document laid before Parliament under subsection (6).
(10) In calculating the 60-day period, no account is to be taken of any time

통신법(2003)의 section 124G에 다음을 추가한다.

“124H 인터넷 접근을 제한할 의무

(1) 주무장관은 다음의 경우에 ISP에 대하여 기술적 의무를 부과할 것을 요구해야 한다

(a) 하나 또는 그 이상의 기술적 의무가 ISP에게 부과되어야 한다고 평가될 때

(b) 부과의무의 평가, 124F조에 근거하여 OFCOM에 의하여 준비된 보고서, 주무장관에게 관련이 있는 것으로 나타난 다른 요소 등을 주무장관은 적절하게 고려해야 한다.

(2) 최초의 법률 시행일로부터 12개월 내의 기간동안에는 이 조항에 근거한 어떠한 명령도 발해질 수 없다.

(3) 이 조항에 근거한 명령은 기술적 의무가 효력을 발생하는 날짜를 특정하고 그 특정된 날짜에 이루어져야 한다.

(4) 그 명령은 또한 다음을 구체화해야 한다.

(a) 이용자에 대하여 기술적 수단을 부담하는 것의 기준;

(b) 그 수단의 일부로서 부담하는 절차 및 부담의 시기

(5) 다음의 경우가 아닌 한 이 조항에 근거한 어떠한 명령도 발해질 수 없다.

(a) 주무장관이 세부조항 (6)에서 (10)을 따를 것

(b) 명령의 초안이 국회에 제출되고 양원의 결의안에 의하여 찬성될 것

(6) 주무장관이 이 조항에 근거하여 명령을 발할 것을 제안한다면, 주무장관은 국회에 다음의 문서를 제출해야 한다.

(a) 제안의 설명

(b) 초안 명령의 형식으로 구성할 것

(7) 세부조항 (6)에 근거한 문서의 제출된 후 60일 동안(이하 “60일 기간”이라 한다.), 주무장관은 국회에 제안의 효과를 발생시키는 초안을 제출할 수 없다. (변경 여부에 관계없이)

---

during which Parliament is dissolved or prorogued or during which either House is adjourned for more than 4 days.

(8) 제안의 효과를 발생시키는 이 조항에 근거한 초안을 준비함에 있어 주무장관은 "60일 기간" 동안 초안을 구성함에 있어 다음을 고려해야 한다.

(a) 초안에 대한 진정

(b) 초안을 보고받은 국회 위원회의 권고사항

(9) 제안의 효과를 발생시키기 위하여 초안을 국회에 제출할 때(변경 여부에 관계없이), 주무장관은 세부조항 (6)에 근거하여 국회에 제출한 문서가 포함하는 제안에 대한 변경사항을 설명하는 문서 역시 제출해야 한다.

(10) "60일 기간"을 계산함에 있어, 국회가 해산하거나 휴회하거나 양원 중 한 곳이 4일 이상 휴회한 동안의 기간은 포함하지 않는다.

17 특정 장소에 대하여 인터넷 접속을 금지하는 명령에 대한 조항을 만들 수 있는 권한[47)]

---

47) 17 Power to make provision about injunctions preventing access to locations on the internet

(1) The Secretary of State may by regulations make provision about the granting by a court of a blocking injunction in respect of a location on the internet which the court is satisfied has been, is being or is likely to be used for or in connection with an activity that infringes copyright.

(2) "Blocking injunction" means an injunction that requires a service provider to prevent its service being used to gain access to the location.

(3) The Secretary of State may not make regulations under this section unless satisfied that—

(a) the use of the internet for activities that infringe copyright is having a serious adverse effect on businesses or consumers,

(b) making the regulations is a proportionate way to address that effect, and .

(c) making the regulations would not prejudice national security or the prevention or detection of crime.

(4) The regulations must provide that a court may not grant an injunction unless satisfied that the location is—

(a) a location from which a substantial amount of material has been, is being or is likely to be obtained in infringement of copyright,

(b) a location at which a substantial amount of material has been, is being or is likely to be made available in infringement of copyright, or

(c) a location which has been, is being or is likely to be used to facilitate access

(1) 법원의 저작권을 침해하는 활동이 발생하였거나 발생할 수 있는 또는 이와 연관된 장소에 대한 인터넷의 접속차단 명령에 의하여 주무장관은 규제조항을 만들 수 있다.

(2) "접속차단 명령"은 서비스 제공자에게 그 장소에서 서비스에 접속하는 것을 막도록 요구하는 명령을 의미한다.

(3) 주무장관은 다음이 만족되지 않는 한 규제를 하면 안된다.

(a) 저작권 침해 활동을 위한 인터넷의 사용이 사업자 또는 소비자들에게 심각하게 부정적인 영향을 줄 것

(b) 규제를 하는 것이 규제대상 행위의 영향에 비례할 것

(c) 규제를 하는 것이 국가안보나 범죄탐지에 해를 끼치지 않을 것

---

to a location within paragraph (a) or (b).

(5) The regulations must provide that, in determining whether to grant an injunction, the court must take account of—

(a) any evidence presented of steps taken by the service provider, or by an operator of the location, to prevent infringement of copyright in the qualifying material,

(b) any evidence presented of steps taken by the copyright owner, or by a licensee of copyright in the qualifying material, to facilitate lawful access to the qualifying material,

(c) any representations made by a Minister of the Crown,

(d) whether the injunction would be likely to have a disproportionate effect on any person's legitimate interests, and

(e) the importance of freedom of expression.

(6) The regulations must provide that a court may not grant an injunction unless notice of the application for the injunction has been given, in such form and by such means as is specified in the regulations, to—

(a) the service provider, and .

(b) operators of the location.

(7) The regulations may, in particular—

(a) make provision about when a location is, or is not, to be treated as being used to facilitate access to another location,

(b) provide that notice of an application for an injunction may be given to operators of a location by being published in accordance with the regulations, .

(c) provide that a court may not make an order for costs against the service provider,

(d) make different provision for different purposes, and

(e) make incidental, supplementary, consequential, transitional, transitory or saving provision.

(4) 다음을 만족하지 않는 한 법원이 접속차단 명령을 승인할 수 없다.
  (a) 상당한 양의 자료들에 대한 저작권침해가 존재해왔거나 존재하고 있는 또는 존재할 것 같은 장소
  (b) 상당한 양의 자료들에 대한 저작권침해가 가능하거나 가능할 것 같은 장소
  (c) (a),(b)정에 해당하는 장소에 접근을 가능하게 하거나 가능할 것 같은 장소
(5) 접속차단 명령을 승인할지를 결정함에 있어 법원은 다음의 사항을 고려하여야 한다.
  (a) 자료의 저작권 위반을 막기 위하여 서비스 제공자 또는 장소의 운영자의 조치의 증거
  (b) 자료에 대한 합법적 접근을 가능하게 하기 위한 저작권자 또는 저작권 승인자의 행위의 증거
  (c) 각료들의 진정
  (d) 그 명령이 사람의 정당한 이익에 불합리한 영향을 줄 것 같은지의 여부
  (e) 표현의 자유의 중요성
(6) 법원은 규제규정에 의하여 구체화된 형식과 수단에 의하여 접속차단 명령이 이하에게 통지되지 않는 한 그 명령을 승인하여서는 안된다.
  (a) 서비스 제공자
  (b) 장소의 운영자
(7) 규제는 특히 다음과 같을 수 있다.
  (a) 특정 장소가 언제 규제대상이고 아닌지에 대해서 조항이 규정하고 이는 다른 장소에 접근을 가능하게 하는 경우에도 마찬가지로 다루지는 것
  (b) 접속차단 명령에 대한 적용의 공고는 그 장소의 운영자에게 그 규제에 부합되도록 이루어져야 한다는 것
  (c) 법원이 서비스 제공자에 대하여 비용을 청구하여서는 안된다는 것
  (d) 별도의 목적으로 별도의 조항을 만드는 것

(e) 이에 부수적인, 보충적인, 그 결과로 발생하는, 일시적인 조항을 만들 수 있는 것

다. 그 밖의 구체적 내용

(1) ISP의 이용자에 대한 저작권 침해 통지 의무

ISP는 저작권 소유자가 작성한 저작권 침해 보고서를 받아 이를 법이 정하는 바에 따라 이용자에게 통보하여야 한다[48].

48) 3 Obligation to notify subscribers of reported infringements
After section 124 of the Communications Act 2003 insert－
"Online infringement of copyright: obligations of internet service providers
124A Obligation to notify subscribers of copyright infringement reports
(1) This section applies if it appears to a copyright owner that－
(a) a subscriber to an internet access service has infringed the owner's copyright by means of the service; or
(b) a subscriber to an internet access service has allowed another person to use the service, and that other person has infringed the owner's copyright by means of the service.
(2) The owner may make a copyright infringement report to the internet service provider who provided the internet access service if a code in force under section 124C or 124D (an "initial obligations code") allows the owner to do so.
(3) A "copyright infringement report" is a report that－
(a) states that there appears to have been an infringement of the owner's copyright;
(b) includes a description of the apparent infringement;
(c) includes evidence of the apparent infringement that shows the subscriber's IP address and the time at which the evidence was gathered;
(d) is sent to the internet service provider within the period of 1 month beginning with the day on which the evidence was gathered; and
(e) complies with any other requirement of the initial obligations code.
(4) An internet service provider who receives a copyright infringement report must notify the subscriber of the report if the initial obligations code requires the provider to do so.
(5) A notification under subsection (4) must be sent to the subscriber within the period of 1 month beginning with the day on which the provider receives the report.
(6) A notification under subsection (4) must include－

(2) ISP의 저작권 침해 리스트 제공 의무

저작권 소유자가 정기적으로 요구하나 법이 정한 경우에 ISP들은 관련한

(a) a statement that the notification is sent under this section in response to a copyright infringement report;
(b) the name of the copyright owner who made the report;
(c) a description of the apparent infringement; .
(d) evidence of the apparent infringement that shows the subscriber's IP address and the time at which the evidence was gathered;
(e) information about subscriber appeals and the grounds on which they may be made;
(f) information about copyright and its purpose;
(g) advice, or information enabling the subscriber to obtain advice, about how to obtain lawful access to copyright works;
(h) advice, or information enabling the subscriber to obtain advice, about steps that a subscriber can take to protect an internet access service from unauthorised use; and
(i) anything else that the initial obligations code requires the notification to include.
(7) For the purposes of subsection (6)(h) the internet service provider must take into account the suitability of different protection for subscribers in different circumstances.
(8) The things that may be required under subsection (6)(i), whether in general or in a particular case, include in particular－
(a) a statement that information about the apparent infringement may be kept by the internet service provider;
(b) a statement that the copyright owner may require the provider to disclose which copyright infringement reports made by the owner to the provider relate to the subscriber;
(c) a statement that, following such a disclosure, the copyright owner may apply to a court to learn the subscriber's identity and may bring proceedings against the subscriber for copyright infringement; and
(d) where the requirement for the provider to send the notification arises partly because of a report that has already been the subject of a notification under subsection (4), a statement that the number of copyright infringement reports relating to the subscriber may be taken into account for the purposes of any technical measures.
(9) In this section "notify", in relation to a subscriber, means send a notification to the electronic or postal address held by the internet service provider for the subscriber (and sections 394 to 396 do not apply)."

리스트를 제공해야 한다.[49]

(3) 의무 불이행시 벌금 부과

이를 이행하지 않을 경우 법에 대한 불복으로 간주해 누락된 보고 건당 최대 25만 파운드의 벌금을 물도록 하였다[50].

라. 분석 및 평가

(1) 문제점

WiFi와 관련하여 제기되는 문제점은 카페나 레스토랑 또는 개인과 같이 사설 무선랜 제공자가 제공한 공개 WiFi 네트워크에 누군가가 접속하여 저작권 침해 행위를 하였을 때, 그 사설 무선랜 제공자의 법적 지위의 문제이다.

---

49) 124B Obligation to provide copyright infringement lists to copyright owners
(1) An internet service provider must provide a copyright owner with a copyright infringement list for a period if－
(a) the owner requests the list for that period; and
(b) an initial obligations code requires the internet service provider to provide it.
2) A "copyright infringement list" is a list that－
(a) sets out, in relation to each relevant subscriber, which of the copyright infringement reports made by the owner to the provider relate to the subscriber, but
(b) does not enable any subscriber to be identified.
(3) A subscriber is a "relevant subscriber" in relation to a copyright owner and an internet service provider if copyright infringement reports made by the owner to the provider in relation to the subscriber have reached the threshold set in the initial obligations code."

50) 124L Enforcement of obligations
(2) The amount of the penalty imposed under section 96 as applied by this section is to be such amount not exceeding £250,000 as OFCOM determine to be－
(a) appropriate; and
(b) proportionate to the contravention in respect of which it is imposed.

디지털경제법상 저작권 침해 통지의 대상은 이용자들로서 혐의가 있는 침해자, 그들에게 인터넷을 사용할 수 있도록 승낙한 타인 등을 포함한다. 여기에 사설 무선랜 제공자들이 포함되는가도 논란이 된다.

그러나 "이용자"란 동법에서 (a) 서비스의 제공자와의 합의 하에서 서비스를 제공받는 자이고 (b) 통신사업자로서 서비스를 제공받지 않는 자로 정의된다. 따라서 사설 무선랜 제공자로서는 당해 사안에서 현실적으로 소규모 WiFi일지라도 통신 서비스를 제공한 자라는 점에서 "이용자"에 해당하지 않는다고 주장할 여지가 있다.

만약 "이용자"가 아니라면, ISP에 해당하는지 여부가 문제된다. 영국법상의 정의에 따르면 ISP는 "인터넷 접근 서비스"를 제공하는 자로서 이는 다시 "(a) 이용자에게 제공되는; (b) 전반적으로 또는 주로 인터넷으로의 접근 공급으로 구성되는 (c) 이용자의 접근을 가능하도록 IP주소(들)의 배정을 포함하는 전기통신서비스"와 같이 정의된다. 이러한 규정을 고려할 때, 사설 무선랜 제공자가 ISP에 해당하는 것으로 보기에도 무리가 있다.

일반 개인이 운영하는 WiFi 네트워크에 있어 또다른 문제는, 사설 무선랜 제공자와 piggybacking을 통한 저작권 침해자 간에 의사의 공동이 있었다고 인정할 수 있는가 하는 문제이다. "의사의 공동"에 대해서는 법상 어디에도 정의된 바가 없다. 예를 들면 이용자가 외부에서 가장 가까운 공개 WiFi 네트워크에 접속하는 방식으로 인터넷을 사용하였을 때, 그 사설 무선랜 제공자와 이용자간에 진정한 "의사의 공동"이 있었다고 볼 수 있는지 의심스럽다.

일부에서는 사설 무선랜 제공자가 이를 공개함으로서 접근을 가능하게 한 이상 묵시적인 합의를 한 것으로 볼 수 있다는 견해가 있다. 그러나 이렇게 본다면 그는 이용자가 아닌 ISP로 여겨져야 할 것이고 이러할 경우 동법상 ISP로서의 책임을 부담하게 되어 최대 250,000파운드의 벌금을 부담해야 한다. 그러나 일반인에게 있어 벌금의 액수가 지나치게 과도하고, 자신도 알지 못하는 사이에 WiFi를 통해 인터넷에 접근한 자가 누구인지 인식할 수도 없고, 법적 책임에 따른 경고를 전달한 방법도 마땅치

않아 이러한 규정의 적용은 부당하다.

한편 도서관 등의 공공시설, 카페, 맥도날드 등의 상업시설에 있어 WiFi 공급자는 이용자보다는 통신 제공자로서 볼 가망이 더 크다. 또한 이러한 경우 WiFi 서비스 제공자와 이용자 간의 합의 역시 명백하게 존재한다고 쉽게 판단할 수 있다. 따라서 저작권 침해 사용자를 식별하여 통지하는 등의 법적 의무를 지게 되는데 이는 무료로 서비스를 제공하는 자의 입장에서 매우 큰 부담이 되어 WiFi 서비스의 제공을 감소시키는 커다란 요인이 될 수 있다.

(2) 대응방안 - 구체적 상황에 따른 법적 지위의 설정

카페, 맥도날드와 같은 곳에서는 무료 네트워크 서비스는 이메일과 웹브라우징이 가능한 정도의 기본적인 서비스이다. 이러한 무료 광대역 서비스가 파일 공유 또는 심각한 저작권 침해에 이용될 수 있을 만큼 충분한 능력이 있다고 하기는 어렵다. 이러한 면을 볼 때, 그 WiFi 운영자는 ISP보다는 이용자로서 취급되어야 할 것이다. 그러나 유무선 통신사업자와 경쟁하는 수준의 WiFi 제공자는 파일 공유 등을 지원하기에 충분하므로 다른 ISP와 같이 초기 의무를 준수해야 한다.

호텔, 회의장 등은 일반적으로 저작권 침해가 심각한 문제가 될 수 있는 수준의 서비스를 제공하는 경우가 있다. 이때 각 시설은 그들이 제공하는 서비스의 수준에 따라 법이 규정하는 이용자, ISP, 통신 제공자 중 어디에 해당하는지를 결정해야 한다. 이에 따라 시설에 대하여 적절하고 비례에 맞추어 규제가 이루어져야 한다.

마. 입법에 의한 해결 - 적용대상이 되는 ISP의 범위 설정

(1) 의의

영국은 위와 같은 이유로 디지털경제법의 주적용 대상인 ISP의 범위를

어디까지로 설정할 지에 대하여 OFCOM의 Regulatory Codes를 통해 구체화 하였다. 온라인 저작권 침해와 디지털경제법에 대한 Draft Initial Obligations Code에서는 40만 이상의 가입자를 가진 고정형 ISP만을 저작권보호규정의 규범대상으로 정하고 있다.

(2) 관련 규정 (국문)

ISP에 대한 규정의 적용[51]

3.6 디지털경제법에 대한 주석 51은 다음과 같이 서술한다:

"정부의 의도는 매우 낮은 수준의 온라인 저작권 침해가 입증된 자를 제외한 모든 ISP들에게 그 의무를 부과하는 것이다. 그들의 네트워크 상에 상당한 정도로 존재하지 않는 문제에 대응하여 상당한 비용을 ISP에게 지출하도록 요구하는 것은 비례에 어긋난다는 것이 이러한 의도의 기초이다. 따라서 규정에 적용을 제한하는 한계 기준을 설정하는 것에 대하여 그 제안은 ISP가 단위시간당 받는 저작권 침해 보고서의 수에 근거하고자 한다. 정부는 대부분의 중소규모 ISP들과 이동형 네트워크 운영자 들이 이러한 한계 기준에

---

51) Application of the Code to Internet Service Providers

3.6 Paragraph 51 of the explanatory notes to the DEA states that:

"The government's intention is for the obligations to fall on all ISPs except those who are demonstrated to have a very low level of online infringement. This is on the basis that it would be disproportionate (in cost terms) to require an ISP to incur significant costs to counter a problem that does not exist to any significant degree on its network. The proposal is therefore for the code to set out qualifying threshold criteria, based on the number of CIRs an ISP receives in a set period of time. The government anticipates that most small and medium-sized ISPs and, possibly, the mobile networks would fall under the threshold. However, this exemption would not be a one-off exercise and the qualifying period would be a rolling one (for example, "x" number of CIRs received in a rolling 3 month period). ISPs would need to ensure online infringement of copyright remained at a low level or else face the prospect of passing the qualifying threshold. Once in scope, ISPs would have to comply with the obligations and to continue to do so even if the number of CIRs later fell below the threshold."

도달하지 못할 것이라고 예측한다. 그러나 이러한 면제는 한번의 결정으로 끝나는 것이 아니라, 일정한 주기로 기준 도달 여부에 따라 달라질 수 있다. (예를 들면, 3개월마다 CIR의 수를 기준으로 할 수 있다.) ISP들은 온라인 저작권 침해를 낮은 수준으로 유지할 필요가 있다. 그렇지 않을 경우 제한의 한계점을 넘어 규제 대상이 될 것이다. ISP들은 의무를 준수하고 비록 CIR의 숫자가 한계점 밑으로 떨어지더라도 의무 준수를 계속해야 한다. 그 규정(디지털 경제법)은 처음에 400,000명 이상의 이용자를 보유한 고정형 ISP들만을 대상으로 적용할 것을 제안한다[52].

---

52) We propose that the Code should initially apply only to those fixed ISPs with more than 400,000 subscribers

3.14 On the second question, relating to the potential coverage threshold for ISPs, we propose that, for the first notification period, Qualifying ISPs should be those which provide a fixed internet access service to more than 400,000 subscribers. Currently there are seven fixed ISPs that meet this criterion: BT, O2 (taking into account its fixed internet access subscribers only), Orange (taking into account its fixed internet access subscribers only), Post Office, Sky, TalkTalk Group and Virgin Media.

3.15 Whilst it may be unusual for Ofcom to make a code the application of which is limited according to the size of an operator, the guidance on how we are to interpret these provisions in the DEA is very clear (see paragraph 3.6 above). We believe, therefore, that the approach set out represents a proportionate means of delivering the objectives of the DEA. In particular, we consider that our approach is proportionate in this case for the following reasons:

3.15.1 The seven ISPs with more than 400,000 subscribers together account for 96.5% of the residential and SME business broadband market;

3.15.2 There is a natural breakpoint in that the smallest of the seven ISPs is more than twice the size of the next smallest;

3.15.3 According to information we have obtained from Copyright Owners on the distribution of alleged online copyright infringement activity by ISP, we consider there is a broad correlation between the number of subscribers an ISP has and the level of alleged copyright infringement activity on their service;

3.15.4 Having considered alternative approaches, we believe that our proposed approach provides the clarity and certainty required by stakeholders as they plan for the Code to come into force; and

3.15.5 It is consistent with the government's anticipation that most small and medium-sized ISPs and, possibly, the mobile networks would initially fall outside the threshold.

3.14 두 번째 질문에서, ISP의 잠재적인 범위의 한계점과 관련하여, 첫 번째 통지 기간 동안, 제한적 ISP는 400,000명 이상의 이용자에게 고정형 인터넷 접근을 제공하는 자로 할 것을 제안한다. 현재 이 기준을 만족하는 7개의 고정형 ISP 사업자가 있다: BT, O2 (고정형 인터넷 접속을 통한 이용자만을 고려한 경우), Orange (고정형 인터넷 접속을 통한 이용자만을 고려한 경우), Post Office, Sky, TalkTalk Group and Virgin Media.

3.15 운영자의 규모에 따라 OFCOM이 법규의 적용을 제한하는 것은 흔치 않지만, 디지털경제법 상의 조항들을 해석하는 기준은 매우 명백하다 (위의 3.6 참조). 그러므로 이러한 접근이 디지털경제법의 목적에 부합하는 비례한 수단이라 확신한다. 특히, 다음과 같은 이유로 이 경우 이러한 접근이 비례한다고 생각한다:

3.15.1 400,000명 이상의 이용자를 가진 7개의 ISP 사업자들이 가정용, 사업용 광대역 시장의96.5%를 차지한다는 점.

3.15.2 7개의 ISP중 가장 작은 사업자가 8번째 ISP보다 2배 이상 규모가 크다는 점에서 구분점이 된다는 점.

3.15.3 ISP에 의한 온라인 저작권 침해 혐의의 분배에 대한 저작권 소유자 협회의 정보에 따르면, ISP가 보유하는 이용자의 수와 저작권 침해 혐의가 있는 활동의 수준간에 폭넓은 상관관계가 존재하는 점.

3.15.4 다른 대안을 고려할 때, 이 접근법이 법안을 입안토록 한 이해관계인이 요구하는 명백성과 확실성을 갖춘 점

3.15.5 이는 대부분의 중소규모 ISP와 이동형 네트워크에 대하여 처음에는 적용대상에서 제외하도록 한 정부의 기대에 부응한다는 점.

(3) 평가 및 적용

디지털경제법의 제정과정에서 영국 내부에 커다란 논란이 발생하였다. 왜냐하면 지금까지는 카페나 레스토랑 그리고 도서관 등 대중을 상대로 무상으로 무선랜을 제공해온 주체들이 디지털경제법상의 ISP에 해당되는

가가 모호하므로, 만약 ISP라고 한다면 앞으로는 상당히 무거운 의무와 책임을 부담해야 하고 따라서 더 이상 현재와 같은 자유로운 무선랜의 공급은 현실적으로 불가하기 때문이다. 개인들이 지금까지 자유롭게 무상으로 무선랜을 향유해왔지만 앞으로는 더 이상 그런 무상의 자유로운 무선랜 접속은 기대할 수 없게 된다는 우려와 불만 때문이었다.

이를 해결하고자 나온 절충적 대안이 400,000명 이상의 사용자를 보유한 ISP를 우선적인 적용대상으로 하는 것이었다. 이 법안이 과거의 규정과 비교할 때, 책임의 정도를 현저하게 상승시킨 점에서 경과기간을 두어 통신 사업자들로 하여금 규정 준수를 위한 준비를 할 수 있도록 여유를 주는 것이 불가피했고 따라서 즉시 법안을 준수할 능력을 가진 대형 ISP 사업자들로 적용대상을 제한한 것은 그 정당성이 인정된다고 볼 수 있다. 차후에 사업자들의 규정 준수 현황과 여론을 보아 소형 ISP들에게도 법안을 적용해야 할지 판단해야 할 것이다.

이러한 법안 해석의 세부 규정을 적용할 경우, 카페나 맥도날드 점포 같은 WiFi 운영자의 경우 400,000명 이상의 이용자를 가진 ISP라 할 수 없으므로 동법에서 규정하는 ISP로서의 의무를 부담하지 않을 것이다. 따라서 이용자로서의 권리의무 관계를 부담할 것이고, ISP의 범위에 포함되었다면 부담하였을 이용자에 대한 통지의무 및 위반시 벌금부담과 같은 과도한 의무를 부담하지 않을 것이다. 결국 현재와 같은 개인의 자유로운 무선랜 접속은 큰 변화없이 유지될 수 있게 되어서 심각한 사회적 논란은 수그러 들게 되었다.[53]

2. 미국 캘리포니아 주 사업 및 직업법 22948.6조[54]

가. 의의

---

53) 이러한 영국의 논란은 무선랜 보안의 중요성에도 불구하고 무상의 자유로운 무선랜 접속을 갈망하는 일반 대중의 기대에 정면으로 충돌하는 갈등상황을 정치적으로 감당할 수 있는 능력이 우리 사회에는 과연 있는가 하는 의문을 던져주는 것이다.

54) West's Ann.Cal.Bus. & Prof.Code § 22948.6.

캘리포니아 주는 이 법률에서 무선 Access Point 상품의 생산자에게 무선랜 보안을 위하여 일정한 의무를 부과하고 있다. 이는 통신 기기 등 제품 생산자에 대한 법적 책임을 명문으로 규정한 이례적인 법규이다.

나. 법조문 (국문)

§ 22948.6. 소규모 사무실, 재택 사무실, 주거지에서의 사용을 위한 무선AP가 포함된 장치; 경고 및 다른 보호 정보의 요구[55]

(A) 구내기반 무선 네트워크 라우터 또는 액세스 브리지와 같이, 소규모 사무실, 재택 사무실 또는 주거 내에서의 사용을 목적으로 하여 주내에서 새로 출시되는 무선 AP를 포함하는 장치는 다음과 같은 규칙에 따라 생산되어야 한다[56].

(1) 소프트웨어에 그 장치의 환경설정 과정 중에 발생할 수 있는 보안 경고를 포함시켜야 한다. 경고는 소비자에게 승인되지 않은 접근으로부터 자신의 무선 네트워크 연결을 보호하는 방법을 알려야 한다. 이 요건은 소비자에게 상품 설명서, 생산자의 인터넷 웹사이트 또는 정확한 정보를 제공하는 소비자 보호 인터넷 웹사이트 등의 참조를 통한 위와 같은 내용의 경고에 의해 충족될 수 있다[57].

---

55) § 22948.6. Devices including an integrated and enabled wireless access point for use in a small office, home office, or residential setting; required warnings and other protection information.

56) (A) A device that includes an integrated and enabled wireless access point, such as a premises-based wireless network router or wireless access bridge, that is for use in a small office, home office, or residential setting and that is sold as new in this state for use in a small office, home office, or residential setting shall be manufactured to comply with one of the following:

57) (1) Include in its software a security warning that comes up as part of the configuration process of the device. The warning shall advise the consumer how to protect his or her wireless network connection from unauthorized access. This requirement may be met by providing the consumer with instructions to protect

(2) 사용을 하기 위해 소비자가 반드시 제거해야 하는 임시 경고 스티커를 장치에 부착하여야 한다. 경고는 소비자에게 승인되지 않은 접근으로부터 자신의 무선 네트워크 연결을 보호하는 방법을 알려야 한다. 이 요건은 소비자에게 그들의 무선 네트워크 연결은 승인되지 않은 사용자가 접근할 수 있음을 알리거나 그러한 내용을 알리는 상품 설명서, 생산자의 인터넷 웹사이트 또는 정확한 정보를 제공하는 소비자 보호 인터넷 웹사이트 등의 참조를 통하여 충족될 수 있다[58].

(3) 장치는 다음의 보호를 제공해야 한다[59]:

(a) 소비자에게 그들의 무선 네트워크 연결이 승인되지 않은 사용자가 접근할 수 있음을 알려야 한다[60].

(b) 소비자에게 그들의 무선 네트워크 연결을 승인되지 않은 접근으로부터 보호하는 방법을 알려야 한다[61].

(c) 해당 제품의 사용을 허가하기 전에 소비자로부터 동의를 요구하도록 하는 보호방법을 장치 상에서 제공하여야 한다. 상품 설명서 또는 생산자의 인터넷 웹 사이트 등을 통해 부가적인 정보를 제공

---

his or her wireless network connection from unauthorized access, which may refer to a product manual, the manufacturer's Internet Web site, or a consumer protection Internet Web site that contains accurate information advising the consumer on how to protect his or her wireless network connection from unauthorized access.

58) (2) Have attached to the device a temporary warning sticker that must be removed by the consumer in order to allow its use. The warning shall advise the consumer how to protect his or her wireless network connection from unauthorized access. This requirement may be met by advising the consumer that his or her wireless network connection may be accessible by an unauthorized user and referring the consumer to a product manual, the manufacturer's Internet Web site, or a consumer protection Internet Web site that contains accurate information advising the consumer on how to protect his or her wireless network connection from unauthorized access.

59) (3) Provide other protection on the device that does all of the following:

60) (a) Advises the consumer that his or her wireless network connection may be accessible by an unauthorized user.

61) (b) Advises the consumer how to protect his or her wireless network connection from unauthorized access.

할 수 있다[62].

(4) 소비자의 동의 없이 활성화된 기기(장치)의 경우 그 장치의 사용을 허가하기 전에 소비자의 무선 네트워크 연결을 승인되지 않은 접근으로부터 보호하기 위한 다른 보호방법을 제공해야 한다[63].

(b) 본 조는 무선 AP를 포함하며 연방정부의 비면허대역에서 사용되는 장치들에만 적용된다[64].

(c) 본 조는 2007년 10월 1일 이후 생산된 상품에만 적용된다[65].

§ 22948.5. 정의규정[66]

본 장에서의 용어의 정의는 다음과 같다.:[67]

(a) "연방정부의 비면허대역"은 연방 통신 위원회가 사용자에게 특정 면허를 발급하지 않고, 대신 공유목적으로 지정된 스펙트럼의 일부에서 사용될 수 있는 장비를 승인한 경우 그 스펙트럼을 의미한다[68].

(b) "소규모 사무실"은 고용인이 50명 이하인 사업을 의미한다[69].

(c) "스펙트럼"은 전자기 신호가 전송될 수 있는 주파수 대역을 의미한다. 이는 라디오, 텔레비전, 무선 인터넷 연결, 그 밖의 전파로

---

62) (c) Requires an affirmative action by the consumer prior to allowing use of the product. Additional information may also be available in the product manual or on the manufacturer's Internet Web site.

63) (4) Provide other protection prior to allowing use of the device, that is enabled without an affirmative act by the consumer, to protect the consumer's wireless network connection from unauthorized access.

64) (b) This section shall only apply to devices that include an integrated and enabled wireless access point and that are used in a federally unlicensed spectrum.

65) (c) This section shall only apply to products that are manufactured on or after October 1, 2007.

66) § 22948.5. Definitions

67) For purposes of this chapter, the following terms have the following meanings:

68) (a) "Federally unlicensed spectrum" means a spectrum for which the Federal Communications Commission does not issue a specific license to a user, but instead certifies equipment that may be used in a segment of spectrum designated for shared use.

69) (b) "Small office" means a business with 50 or fewer employees within the company.

가능한 다른 모든 통신수단을 포함한다[70].

(d) "무선 AP"는 구내기반 무선 네트워크 라우터 또는 무선 네트워크 브리지와 같이, 인터넷 서비스 제공자에 대한 연결을 목적으로 하는 무선 네트워크를 생성하고 무선 클라이언트들이 이에 접속할 수 있도록 하는 장치를 의미한다[71].

(e) "무선 클라이언트"는 인터넷 서비스 제공자에 대한 연결을 목적으로 하는 무선 네트워크에 접속을 가능하게 하는 무선 장치를 의미한다[72].

다. 분석 및 평가

일반적으로 무선랜과 관련한 법적 분쟁에서 직접 관련된 자는 ISP, 무선랜 네트워크 운영자, 무선랜 네트워크 접속 및 이용자일 것이다. 따라서 대부분의 법률규정은 이들간의 권리의무관계를 규정하고 있다. 그러나 미국 캘리포니아 주 사업 및 직업법 22948.6조는 무선 AP(Access Point) 기기 생산자에게 일정한 의무를 부담시키고 있다. 엄밀한 의미에서 기기 생산자는 제3자로서 법률상 책임을 부담시키는 것이 부당하다는 견해가 있다. 그러나 1) AP 생산자 역시 무선랜 네트워크를 통하여 경제적 이익을 얻는다는 점에서 이해관계자라고 보는 것이 가능하고, 2) 이들이 부담하는 의무가 과도한 비용이나 노력이 들지 않는다는 점에서 무리한 요구라고 할 수 없다. 3) 또한 무선 AP 이용자들의 보안에 대한 인식이라는 정책 목적 달성에 상당한 수단이라는 점에서 그 정당성이 인정된다.

---

70) (c) "Spectrum" means the range of frequencies over which electromagnetic signals can be sent, including radio, television, wireless Internet connectivity, and every other communication enabled by radio waves.

71) (d) "Wireless access point" means a device, such as a premises-based wireless network router or a wireless network bridge, that allows wireless clients to connect to it in order to create a wireless network for the purpose of connecting to an Internet service provider.

72) (e) "Wireless client" means a wireless device that connects to a wireless network for the purpose of connecting to an Internet service provider.

3. 미국 뉴욕 주 Westchester County

'공공인터넷보호법[73]'(Public Internet Protection Act)을 제정하여 무선 인터넷에 대한 보안조치를 강화하였다. 이는 1) 고객 개인정보를 수집하는 사업자(기업이용자)가 무선인터넷을 이용할 경우 최소한의 보안 조치를 하도록 의무화하였고, 2) 인터넷카페 등 무료 무선인터넷서비스를 고객에게 제공하는 자는 이용자의 보안조치를 위해 안내표지문을 부착할 것을 의무화 하였다[74].

4. 미국 유타 주

Utah Code Section §76-10-1231(1)[75]는 Internet Service Provider가 이용자에게 유해한 컨텐츠 등이 제공될 것으로 우려되는 경우 이를 거르는 것을 의무화하도록 하고 있으며, § 76-10-1231(5)[76]를 통하여 이를 위반

73) Westchester's WiFi Legislation ARTICLE XXV. PUBLIC INTERNET PROTECTION ACT.

74) Sec. 863.1202. Security of Personal Information
1. Any commercial business that stores, utilizes or otherwise maintains personal information electronically shall be required to take minimum security measures as defined herein to secure and prevent unauthorized access to all such information.
2. Commercial businesses that additionally provide or offer public Internet access shall conspicuously post a sign in the area where such Internet access is located stating:
FOR YOUR OWN PROTECTION AND PRIVACY, YOU ARE ADVISED TO INSTALL A FIREWALL OR OTHER COMPUTER SECURITY MEASURE WHEN ACCESSING THE INTERNET. FOR INFORMATION ON INTERNET SAFETY PLEASE VISIT www.westchestergov.com.
Such sign shall be designed, produced and distributed by the department of weights and measures at no cost and shall, at a minimum, be printed in 14 point bold type on a placard measuring 8.5 inches in height by 11 inches in width.

75) (1)(a) Upon request by a consumer, a service provider shall filter content to prevent the transmission of material harmful to minors to the consumer.
(b) A service provider complies with Subsection (1)(a) if it uses a generally accepted and commercially reasonable method of filtering.

76) (5) A service provider that intentionally or knowingly violates Subsection (1) or

할 경우 1만 달러의 벌금을 부과할 수 있도록 규정하고 있다.

5. 인도

가. 규제법안 제정의 계기

2008년 9월, 인도의 뭄바이에 있는 해군 기지 내의 American national Kenneth Haywood의 무선랜이 무단 접속에 의하여 테러 이메일에 이용된 사건이 있었다. 당시 해당 무선랜은 공개로 설정되어 있어서 아무나 접속해서 외부로 통신할 수 있었고 테러 추적 결과 범죄에 이용된 것이 확인되었다. 이에 따라 WiFi의 보안에 대한 정부규제가 필요하다는 인식이 높아졌다.

나. 규제내용

WiFi 서비스를 제공하는 ISP들에게 compliance requirements를 요구하여 반드시 WiFi의 access point를 안전하게 하도록 해야 할 의무를 부여하였고, 모든 접속자들이 안전하고 권한 있게 접속하였는지 확인할 수 있는 WiFi end point에 중앙인증 및 트래킹 시스템을 제공하고 그 기록을 1년 이상 보관하도록 하였다. 또한 모든 회원 인증의 방법은 정해진 방법을 통해서만 하도록 강제하였다.

2009년 2월 23일 WiFi의 안전한 이용을 위한 규제를 발표하여 ISP들에게 4개월의 유예기간을 주고 사용자 정보의 등록제 및 로그인 시스템을 마련하도록 강제하였다[77].

---

(2) is subject to a civil fine of $2,500 for each separate violation of Subsection (1) or (2), up to $10,000 per day.

77) 2009년 5월 11일자 economictimes.indiatimes.com 기사 참조
ISPs seek more customer awareness for safe WiFi play
The ministry of communications & IT in February had set a June deadline for the Internet Service Providers (ISPs) to register their wireless customers. However,

6. 나이지리아

가. Nigerian Communications Act 2003

나이지리아에서 사용하고자 하는 통신기기들은 허가를 받아야 한다[78].

---

the wireless players, including service and hardware providers to research analyst firms tracking the sector, are worried not because they may miss the deadline, but the regulation will not achieve its target.

That target was to make wireless, or WiFi, world more secure. While they accept that regulation is necessary for this environment, they also claim that not enough customer-education has been done.

"The department of telecommunications' (DoT) regulation aims to prevent misuse of WiFi internet access and to be able to track the perpetrator in case of abuse. So, it has instructed ISPs to enforce centralised authentication using login ID and password for each user. But this is not enough," said Kaustubh Phanse, wireless architect, AirTight Networks, a wireless security products provider. The regulation by the government was triggered by the cyber terrorist attacks, which hit India late last year, exposing how easy it is to misuse unsecured WiFi networks.

Accepting that regulation was the first step, the equivalent of shutting the front door, AirTight networks' chief technology officer Pravin Bhagwat said: "End-users or organisations need to implement safety measures. The key is to make people aware about safety measures. The regulation is looking only at unauthorised access to the internet. The problem won't go away with just that information. Education and self-regulation by users is just as important."

Citing several ways a determined hacker can get around the regulation, Mr Bhagwat said that a malicious user in the vicinity of an unsecured WiFi network can eavesdrop on in-flight data and spoof the identity of the genuine user to gain internet access and wreak damage. Or, if a user is already logged into an unsecured WiFi network, a hacker can hijack the session to gain unauthorised internet access by spoofing the authenticated user's device. The hacker does not then require a login ID or password.

"There are several ways that a hacker can circumvent the centralised authentication that the government regulation mandates and malicious users are unlikely to register their identity with ISPs using a photo identity. They will resort to fake photo IDs or even simply resort to using any of several means to achieve their goals without leaving a trace. ISPs and subscribers may thus find themselves on the wrong side of the law inspite of having followed all steps that have been mandated," he said.

78) 31. (1) No person shall operate a communications system or facility nor provide a communications service in Nigeria unless authorised to do so under a

WiFi Hotspot 설치를 장려하기 위해 이를 위한 가이드라인도 제공하나 이에 대해서도 역시 허가제가 적용된다.

나. 상업적 통신 서비스를 위한 2.4.GHz 대역 사용의 규제 가이드라인[79)]

(1) 목적

서비스의 질을 보장하여 간섭 없는 사용을 위한 규제를 제공하는 것을 그 목적으로 한다[80)].

(2) 내용

모든 장비는 나이지리아 통신법(NCA2003) 제132조를 따르도록 하고[81)], 상업적 WiFi hotspot에 대하여 등록 의무를 부담하도록 한다[82)]. 기술적

---

communications licence or exempted under regulations made by the Commission under this Act.
(2) Any person who acts in breach of sub-section (1) of this section commits an offence and is liable on conviction to -
(a) a fine not less than the initial fee for the relevant licence;
(b) a fine not exceeding 10 (ten) times the initial fee for the relevant licence;
(c) imprisonment for a term not exceeding 1 (one) year; or
(d) both such fine and imprisonment; Provided that upon conviction, the person shall also forfeit to the Commission the property, facilities, installations and equipment used by him for the provision and operation of the unlicensed service.

79) REGULATORY GUIDELINES FOR THE USE OF 2.4 GHz ISM BAND FOR COMMERCIAL TELECOM SERVICES.

80) Purpose of Regulation
The main objectives of this set of guidelines is to ensure interference- free operation by all users of the band and to ensure that a guaranteed grade of service is available to the 이용자s through established quality of service benchmarks, and consumer code of practice.

81) 1(c) All equipment to be deployed must be type approved by the Commission prior to importation and deployment in compliance with Section 132 of NCA 2003. Existing ISM band operators who wish to adapt their present equipment for WiFi deployment must seek approval from the Commission.

82) (d) All sites in which commercial WiFi hotspots are to be provided must be

사양에 대하여 상세하게 명시하는 한편[83], 보안과 관련하여 공급자는 데이터 보안 및 사용자 개인정보 보안을 위해 적정한 조치를 취해야 하며, 최소한 WEP/WPA 기준을 충족시켜야 할 것을 의무화하고 있다[84].

7. 독일

(1) 사건의 개요

어떤 음악가가 공개 Wi-Fi를 운영하는 자를 고소하였다. 그의 무선 인터넷 연결을 통하여 온라인 파일 공유 네트워크를 이용하여 제공된 음악 파일이 불법적으로 다운로드 되었기 때문이다.

그의 무선 인터넷 연결은 설치 당시부터 비밀번호가 설정되지 않은 상태로 허가받지 않은 자들도 접속이 가능한 상태였다. 이에 대하여 그 무선랜 운영자는 음악 파일이 다운로드 되던 당시 휴가 중임을 증명하여서 자신이 그 파일을 다운로드 받은 것이 아니라 제3자가 자신의 무선 인터넷 연결을 통하여 음악 파일을 다운로드 받은 것이라고 하여 자신의 책임이 없음을 항변하였다.

(2) 법원의 판단

---

registered with the Commission.

83) 3장 TECHNICAL SPECIFICATIONS에서 Basic Specifications으로 IEEE802.11b를 제시하고, 그밖에 Operational Features, Automatic Transmit Power Control (ATPC), Dynamic Frequency Selection/Adaptive Frequency Hopping Technique, Bandwidth and Carrier Separation, Modulation, Adaptive Frequency Hopping/Adaptive Dynamic Polling, Spectrum Mask, Spurious emissions, Unwanted emissions, Coverage Diameter, Media Access Protocol, Data Rate, Frequency stability 등에 대해서 구체적으로 규정한다.

84) 4.3 Security
The provider should take adequate measure to protect the data traffic to uphold the 이용자's right to privacy, as entrenched in the constitution of the Federal Republic of Nigeria. Minimum Standard specified by Wired Equivalent Privacy (WEP)/WPA benchmarks must be met.

그러나 독일 연방대법원은 운영자에 대하여 제3자가 그의 인터넷 네트워크를 통하여 저작권 침해 등의 남용행위를 하는 것을 막지 못한 것에 대하여 일정 정도의 책임이 있다고 인정하였다.

법원은 "사설 무선랜의 운영자는 권한없는 제3자가 그를 통하여 저작권 위반을 저지르는데 남용될 지도 모르는 위험으로부터 그들의 무선 인터넷 연결이 충분히 보호되고 있는지 검사할 의무가 있다"고 판시하였다. 만약 이러한 의무를 준수하지 않아 제3자가 보호되지 않은 무선랜 연결을 불법적으로 음악 또는 다른 파일을 다운로드 받는데 이용한 경우, 그 무선랜의 운영자는 최대 100유로(약 14만원)의 벌금을 부과할 수 있도록 하였다.

그러나 법원은 제3자가 다운로드 받은 불법적 저작물에 대한 저작권 위반에 대한 책임을 무선랜 운영자에게 부담시키지는 않았고 무선랜 운영자로서의 주의의무 위반에 대하여 책임을 지도록 하였다.

한편 무선랜 운영자에게 과도한 네트워크 보호 의무를 부담시키지 않도록 운영자가 부담하는 보호의무의 범위를 제한적으로 결정하였다. 무선랜 운영자들이 끊임없이 그들의 무선 연결의 보안을 업데이트할 것을 기대하는 것은 아니고, 단지 처음 인터넷 접속을 위해 네트워크를 설치할 때 비밀번호를 설정하여 권한없는 자들이 접근하는 것을 막도록 하는 보호활동만이 요구된다고 판시하였다.

(3) 판결에 대한 평가

이 사건 판결은 공개 WiFi 자체를 금지하는 것은 아니지만, 이를 통하여 저작권 침해 등의 문제가 발생하였을 때 무선랜 운영자에게 주의의무 위반에 대한 책임을 부담한다는 것을 명시적으로 밝힌 사건이다.

이에 관하여 독일 The national consumer protection agency의 대변인인 Carola Elbrecht는 무선랜 운영자들이 무선 연결에 대하여 보호 수단을 설치해야 한다는 것은 타당한 의무이고, 이와 동시에 법원이 계속적인 기술적 업데이트를 사설 Wi-Fi 운영자에게 요구하지 않은 것은 과도한

의무를 부담시키지 않은 점에서 공정하다고 평가하였다[85].

살피건대, 공개 Wi-Fi를 개설함으로서 임의의 제3자가 인터넷에 접속하는 것을 허용하는 행위는 자신이 ISP로부터 사용을 인정받은 인터넷 접속 자체를 타인과 자발적으로 나누어 갖는 것으로서 그 자체는 권리의 적법한 행사 내지는 사회부조적 관점에서 허용된다고 볼 수 있는 여지는 있다. 그러나 그러한 통신 연결이 저작권 침해 등의 범법 행위의 수단이 되었다면 이를 규제할 필요성 역시 인정된다고 할 수 있다. 만약, 이러한 행위에 대하여 무선랜 운영자의 책임을 부정할 경우 무선랜의 특성상 이를 통하여 이루어지는 저작권 침해에 대한 규제가 매우 어려워지기 때문이다. 또한 자신이 타인에게 인터넷에 접속할 수 있도록 허락하는 의사에 타인이 그를 통하여 불법행위를 하는 것까지 허락하는 의사까지 포함한다고 볼 수는 없기 때문이다.

다음으로 비례원칙에 위반하는 것이 아닌지 알아보면, 우선 목적의 정당성은 전술한 바와 같이 인정되고, 초기 설치시 비밀번호를 설정하도록 하는 것은 무선랜 운영자에게 그다지 큰 노력과 비용을 요하는 것이 아니므로 최소침해의 원칙에도 위배되지 않는다. 마지막으로 이러한 제한으로 발생하는 무선랜 운영자의 권리침해와 온라인 저작권 보호라는 공익을 비교형량해 보았을 때 공익이 작다고 하기 어려울 것이다. 따라서 상당성의 원칙에도 위반하지 않는다고 볼 수 있다.

그러나 이러한 규제수단으로 인하여, 자유롭게 이용할 수 있는 공개 Wi-Fi는 위축될 수밖에 없어서 무선랜의 진흥과 시장의 확대를 정책적 목표로 할 경우 목표 달성에 어려움을 겪게 될 것이다. 스마트폰이 하나의 사회적 신드롬으로 작용하는 상황에서 이미 일반 대중들의 무상의 자유로운 무선랜 이용에 대한 수요는 보안을 이유를 하여 통제시킬 수 있는 차원을 넘은 것으로 생각된다. 모든 AP에 패스워드를 설정하여 이 세상 어디에서도 더 이상 개방된 AP를 찾을 수 없게 되었을 때 제기될 국민들의 불만을 적절히 해소할 수 있는 정치적 능력을 기대하기 어렵다는 점은 이

85) 2010년 5월 13일자 billboard.biz 기사 참조; http://www.billboard.biz/bbbiz/content_display/industry/e3iec86729e87e7d19421ff7bb16c3dfe4c(2010. 7. 27. 방문).

미 영국 디지털경제법 제정과정에서 잘 찾아 볼 수 있다. 그러므로 독일 연방대법원의 판례를 성급하게 정책방향의 유일한 이정표로 삼는 것은 바람직하지 않고, 보다 신중한 자세로 접근하여야 할 것으로 생각된다.

제 2 절 사용자의 권한없는 접근을 금지, 처벌하는 법규

1. 미국 2009 House Bill 1011[86)]

가. 의의

전파를 사용하는 인증(Identification)기기의 사용을 규제하기 위하여 제정된 법안으로 개인의 의사표현이나 동의 없이 고의적으로 사람의 ID를 스캔하는 등의 기기를 금지하는 것을 내용으로 한다.

나. 구체적 규정

예외 규정들[87)]을 제외하고는 국가 또는 회사는 상업적 목적으로 전파를

86) SUBSTITUTE HOUSE BILL 1011, 61st Legislature, 2009 Regular Session, Passed by the House March 3, 2009.

87) 예외에는 상업적 거래, 긴급시의 의료상 목적, 법원의 결정, 연구 및 학술상의 목적 등이 규정되어 있다. 원문 규정은 아래와 같다.
(2) This section does not apply to the following:
(a) Remotely reading or storing data from an identification device as part of a commercial transaction initiated by the person in possession of the identification device;
(b) Remotely reading or storing data from an identification device for triage or medical care during a disaster and immediate hospitalization or immediate outpatient care directly relating to a disaster;
(c) Remotely reading or storing data from an identification device by an emergency responder or health care professional for reasons relating to the health or safety of that person;
(d) Remotely reading or storing data from a person's identification device issued to a

이용한 인증기기[88]를 원격 사용[89]할 수 없다. 단, 인증기기를 그들 자신 또는 제휴기관이 발행받은 경우에는 그렇지 않다[90].

---

patient for emergency purposes;
(e) Remotely reading or storing data from an identification device of a person pursuant to court-ordered electronic monitoring;
(f) Remotely reading or storing data from an identification device of a person who is incarcerated in a correctional institution, juvenile detention facility, or mental health facility;
(g) Remotely reading or storing data from an identification device by law enforcement or government personnel who need to read a lost identification device when the owner is unavailable for notice, knowledge, or consent, or those parties specifically authorized by law enforcement or government personnel for the limited purpose of reading a lost identification device when the owner is unavailable for notice, knowledge, or consent;
(h) Remotely reading or storing data from an identification device by law enforcement personnel who need to read a person's identification device after an accident in which the person is unavailable for notice, knowledge, or consent;
(i) Remotely reading or storing data from an identification device by a person or entity that in the course of operating its own identification device system collects data from another identification device, provided that the inadvertently received data comports with all of the following:
(i) The data is not disclosed to any other party;
(ii) The data is not used for any purpose; and
(iii) The data is not stored or is promptly destroyed;
(j) Remotely reading or storing data from a person's identification device in the course of an act of good faith security research, experimentation, or scientific inquiry including, but not limited to, activities useful in identifying and analyzing security flaws and vulnerabilities;
(k) Remotely reading or storing data from an identification device by law enforcement personnel who need to scan a person's identification device pursuant to a search warrant; and
(l) Remotely reading or storing data from an identification device by a business if it is necessary to complete a transaction.

88) 전파를 이용한 인증기술 또는 얼굴 인식 기술을 이용하는 장치. ("Identification device" means an item that uses radio frequency identification technology or facial recognition technology.)

89) 인증기기와 데이터를 받아들이는 장치 사이의 데이터 교환이 물리적 접촉이 없이 발생함을 의미. ("Remotely reading" means that no physical contact is required between the identification device and the mechanical device that captures data.)

90) (1) Except as provided in subsection (2) of this section, a governmental or business entity may not remotely read an identification device using radio frequency identification technology for commercial purposes, unless that

다. 분석 및 평가

무선랜 보안과 관련하여 타인의 공개되거나 보호되지 않은 WiFi 서비스를 찾아다니는 것을 금지하는 데 적용될 수 있다. 예를 들어 카페에서의 무선랜 사용은 손님이 아닌 비손님의 사용을 승낙한 것으로 볼 수 없으므로 규제할 수 있는 것으로 볼 수 있다.

2. 미국 컴퓨터 사기와 남용에 관한 법률(CFAA)[91]

가. 의의

당해 법률(The Computer Fraud and Abuse Act)은 두 가지 행위에 대한 처벌의 근거규정으로 작용한다. 첫째는 고의적으로 권한없이 타인의 정보망에 접근하거나 권한을 초과하는 접근 및 이를 통해 정보를 획득하는 경우이고, 둘째는 권한없이 고의적으로 보호받는 컴퓨터에 접근하여 그 결과 손해가 발생하였을 경우이다. 정보통신망에 대하여 일반적으로 적용되는 법률이므로 WiFi를 통한 정보접근에 대해서도 확대 적용되고 있다.

나. 구체적 관련 조문 (국문)

§ 1030. 컴퓨터 관련 사기 및 관련 행위[92]

(2) 의도적으로 승인 없이 또는 승인된 접근권한을 넘어서 컴퓨터에 접근하고 다음의 정보를 획득하는 행위[93]

---

governmental or business entity, or one of their affiliates, is the same governmental or business entity that issued the identification device.

91) 18 U.S.C.A. §1030. Fraud and related activity in connection with computers.

92) §1030. Fraud and related activity in connection with computers.

93) (2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains--

(A) section 1602(n) of title 15에서 정의한 금융기관, 카드발행자의 금융기록 또는 신용정보기관의 파일이 들어있는 정보[94]

(B) 미국 정부 산하 부처 또는 기관으로부터의 정보[95]

(C) 보호된 컴퓨터로부터의 정보[96]

(5) (A) 고의로 프로그램, 정보, 코드, 또는 명령의 전송을 발생시키고 그 행동의 결과로써 의도적으로 승인없이 보호된 컴퓨터에 대하여 손상을 발생시키는 행위[97]

다. 분석 및 평가

컴퓨터에 대한 권한없는 사용자의 접근에 대해서 이 법률을 비롯하여 세계 각국에서 규제의 대상으로 삼고 있다.

무선랜과 관련하여 문제되는 것은 규정된 용어의 의미의 범위이다. 이 법률에서 '접근[98]'은 접근의 의도만으로 충분하고, 보호받는 컴퓨터에 대하여 손해를 주려는 의도까지 요구하는 것은 아니다. 그러나 '권한없는' 또는 '권한을 넘는'이라는 용어의 의미에 대해서는 명확히 규정하지 않고 있어 문제가 되고 있다.

한편, 일부 주법은 '권한없는 접근'에 대해 법률에서 정의하고 있다. 캘리포니아 주[99], 콜로라도 주[100] 등은 명시적 동의나 허락이 없으면

---

94) (A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

95) (B) information from any department or agency of the United States; or

96) (C) information from any protected computer;

97) (5)(A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

98) Access

99) CAL. PENAL CODE § 502(c)
(c) Except as provided in subdivision (h), any person who commits any of the following acts is guilty of a public offense:
(1) Knowingly accesses and without permission alters, damages, deletes, destroys,

권한없는 행위로 폭넓게 보는 형태를 취하고 있는 반면, 뉴욕 주[101]는

---

or otherwise uses any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain money, property, or data.

(2) Knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network.

(3) Knowingly and without permission uses or causes to be used computer services.

(4) Knowingly accesses and without permission adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or computer network.

(5) Knowingly and without permission disrupts or causes the disruption of computer services or denies or causes the denial of computer services to an authorized user of a computer, computer system, or computer network.

(6) Knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network in violation of this section.

(7) Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network.

(8) Knowingly introduces any computer contaminant into any computer, computer system, or computer network.

(9) Knowingly and without permission uses the Internet domain name of another individual, corporation, or entity in connection with the sending of one or more electronic mail messages, and thereby damages or causes damage to a computer, computer system, or computer network.

100) COLO. REV. STAT. § 18-5.5-101(1)

(1) "Authorization" means the express consent of a person which may include an employee's job description to use said person's computer, computer network, computer program, computer software, computer system, property, or services as those terms are defined in this section.

101) N.Y. PENAL LAW § 156.00(8)

8. "Without authorization" means to use or to access a computer, computer service or computer network without the permission of the owner or lessor or someone licensed or privileged by the owner or lessor where such person knew that his or her use or access was without permission or after actual notice to such person that such use or access was without permission. It shall also mean the access of a computer service by a person without permission where such person knew that such access was without permission or after actual notice to such person, that such access was without permission.

Proof that such person used or accessed a computer, computer service or

권한없는 접근 방지 조치가 있음에도 불구하고 접속한 때에만 권한없는 행위가 된다고 하여 좁게 보고 있다.

3. 미연방 전자통신프라이버시법(ECPA)

미연방 전자통신프라이버시법(the Electronic Communications Privacy Act) 제2511조는 '누구든 고의로 남의 유무선 전자 통신을 가로채면 이는 유죄이며 범죄다'라고 규정하고 있다[102].

---

computer network through the knowing use of a set of instructions, code or computer program that bypasses, defrauds or otherwise circumvents a security measure installed or used with the user's authorization on the computer, computer service or computer network shall be presumptive evidence that such person used or accessed such computer, computer service or computer network without authorization.

102) United States Code Annotated Currentness

§ 2511. Interception and disclosure of wire, oral, or electronic communications prohibited

(1) Except as otherwise specifically provided in this chapter any person who--

(a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication;

(b) intentionally uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when--

(i) such device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication; or

(ii) such device transmits communications by radio, or interferes with the transmission of such communication; or

(iii) such person knows, or has reason to know, that such device or any component thereof has been sent through the mail or transported in interstate or foreign commerce; or

(iv) such use or endeavor to use (A) takes place on the premises of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or (B) obtains or is for the purpose of obtaining information relating to the operations of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or

(v) such person acts in the District of Columbia, the Commonwealth of Puerto Rico, or any territory or possession of the United States;

(c) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know

4. 미국 플로리다 주

컴퓨터 이용자에 대한 범죄를 규정하고 있는 FLA. STAT. ANN. §815.06은 의도적으로 알면서 권한없이 컴퓨터, 컴퓨터 시스템 또는 컴퓨터 네트워크에 접근하거나 접근하게 되는 결과를 초래하는 행위를 컴퓨터 이용자에 대한 범죄로 규정하였다[103]. 이 규정을 적용하여 2005년 이웃집 근처에 차량을 주차하고 무선인터넷에 접속한 자를 플로리다 주법 위반 혐의로 체포한 사례가 있다.

5. 미국 미시건 주

주법인 MICH. COMP. LAWS ANN. § 752.795에서 권한없는 컴퓨터 네트워크 접속을 규정하여 금하고 있다[104]. 이에 기하여 2007년 5월 매일

---

that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;
(d) intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection; or
(e) (i) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, intercepted by means authorized by sections 2511(2)(a)(ii), 2511(2)(b)-(c), 2511(2)(e), 2516, and 2518 of this chapter, (ii) knowing or having reason to know that the information was obtained through the interception of such a communication in connection with a criminal investigation, (iii) having obtained or received the information in connection with a criminal investigation, and (iv) with intent to improperly obstruct, impede, or interfere with a duly authorized criminal investigation, shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5).

103) FLA. STAT. ANN. § 815.06(1)(a)
(1) Whoever willfully, knowingly, and without authorization:
(a) Accesses or causes to be accessed any computer, computer system, or computer network;

104) MICH. COMP. LAWS ANN. § 752.795
Sec. 5. A person shall not intentionally and without authorization or by exceeding valid authorization do any of the following:

카페 옆에 차를 주차하고 커피숍 WiFi에 접속하여 이메일을 확인하던 사람을 체포한 경우가 있다.

6. 호주 Cybercrime Act 2001[105]

컴퓨터 시스템 등에 권한없이 고의로 접근하는 행위 자체를 금지하고 있다[106]. 그러나 '권한없는 접근'이 무엇인지에 대해서는 명시하지 않고 법원의 판례 등을 통해 해석하는 입장을 취하고 있다.

(a) Access or cause access to be made to a computer program, computer, computer system, or computer network to acquire, alter, damage, delete, or destroy property or otherwise use the service of a computer program, computer, computer system, or computer network .

(b) Insert or attach or knowingly create the opportunity for an unknowing and unwanted insertion or attachment of a set of instructions or a computer program into a computer program, computer, computer system, or computer network, that is intended to acquire, alter, damage, delete, disrupt, or destroy property or otherwise use the services of a computer program, computer, computer system, or computer network. This subdivision does not prohibit conduct protected under section 5 of article I of the state constitution of 1963 or under the first amendment of the constitution of the United States.

105) 호주 형법에 컴퓨터 관련 범죄에 대한 정의규정을 추가함을 주된 내용으로 하고 있다. 접근의 정의 및 컴퓨터 기기 등에 대해 구체화하여 규정하고 있다.

106) 476.1 Definitions

(1) In this Part: access to data held in a computer means:

(a) the display of the data by the computer or any other output of the data from the computer; or

(b) the copying or moving of the data to any other place in the computer or to a data storage device; or

(c) in the case of a program－the execution of the program.

476.2 Meaning of unauthorised access, modification or impairment

(1) In this Part:

(a) access to data held in a computer; or

(b) modification of data held in a computer; or

(c) the impairment of electronic communication to or from a computer; or

(d) the impairment of the reliability, security or operation of any data held on a computer disk, credit card or other device used to store data by electronic means; by a person is unauthorised if the person is not entitled to cause that access, modification or impairment.

7. 영국 '경찰 및 사법절차에 관한 법률'(Police and Justice Act 2006)

기존의 '컴퓨터 오용에 관한 법률[107]'(Computer Misuse Act 1990)을 더욱 강화한 '경찰 및 사법절차에 관한 법률'을 제정하여 고의로 컴퓨터, 컴퓨터시스템 등에 권한없이 접근하는 행위 자체를 금지하고 있다[108].

---

107) 1 Unauthorised access to computer material.
(1) A person is guilty of an offence if－ .
(a) he causes a computer to perform any function with intent to secure access to any program or data held in any computer; .
(b) the access he intends to secure is unauthorised; and .
(c) he knows at the time when he causes the computer to perform the function that that is the case. .
(2) The intent a person has to have to commit an offence under this section need not be directed at－ .
(a) any particular program or data; .
(b) a program or data of any particular kind; or .
(c) a program or data held in any particular computer. .
(3) A person guilty of an offence under this section shall be liable on summary conviction to imprisonment for a term not exceeding six months or to a fine not exceeding level 5 on the standard scale or to both.

108) Computer Misuse Act 1990을 일부 개정하는 내용을 담고 있다. 원문은 아래와 같다.
35 Unauthorised access to computer material.
(1) In the Computer Misuse Act 1990 (c. 18) ("the 1990 Act"), section 1 (offence of unauthorised access to computer material) is amended as follows. .
(2) In subsection (1)－ .
(a) in paragraph (a), after "any computer" there is inserted ", or to enable any such access to be secured"; .
(b) in paragraph (b), after "secure" there is inserted ", or to enable to be secured,". .
(3) For subsection (3) there is substituted－ .
"(3) A person guilty of an offence under this section shall be liable－ .
(a) on summary conviction in England and Wales, to imprisonment for a term not exceeding 12 months or to a fine not exceeding the statutory maximum or to both; .
(b) on summary conviction in Scotland, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both; .
(c) on conviction on indictment, to imprisonment for a term not exceeding two

8. 일본 '부정액세스행위 금지 등에 관한 법률'

가. 의의

권한없이 컴퓨터 시스템에 고의로 접근하는 것을 금지하고 있다. 이를 위반할 경우 1년 이하의 징역 또는 50만엔 이하의 벌금에 처할 수 있도록 규정하고 있다.

나. 관련 법률 조문(국문)

제3조[109]

1). 어느 누구도 부정 액세스 행위를 해서는 안된다.

2) 전항에 규정하는 행위는 다음 각호의 하나에 해당하는 행위를 말한다.

(1) 통신 회선을 통해 액세스 제어 기능이 있는 특정 컴퓨터를 이에 관한 타인의 식별 부호를 입력하여 운영하고 제한되는 특정 서비스를

---

years or to a fine or to both."

109) 第三條

何人も、不正アクセス行爲をしてはならない。

2　前項に規定する不正アクセス行爲とは、次の各号の一に該当する行爲をいう。

一　アクセス制御機能を有する特定電子計算機に電氣通信回線を通じて当該アクセス制御機能に係る他人の識別符号を入力して当該特定電子計算機を作動させ、当該アクセス制御機能により制限されている特定利用をし得る状態にさせる行爲（当該アクセス制御機能を付加したアクセス管理者がするもの及び当該アクセス管理者又は当該識別符号に係る利用權者の承諾を得てするものを除く。）

二　アクセス制御機能を有する特定電子計算機に電氣通信回線を通じて当該アクセス制御機能による特定利用の制限を免れることができる情報（識別符号であるものを除く。）又は指令を入力して当該特定電子計算機を作動させ、その制限されている特定利用をし得る状態にさせる行爲（当該アクセス制御機能を付加したアクセス管理者がするもの及び当該アクセス管理者の承諾を得てするものを除く。次号において同じ。）

三　電氣通信回線を介して接續された他の特定電子計算機が有するアクセス制御機能によりその特定利用を制限されている特定電子計算機に電氣通信回線を通じてその制限を免れることができる情報又は指令を入力して当該特定電子計算機を作動させ、その制限されている特定利用をし得る状態にさせる行爲

얻는 상태를 발생시키는 행위 (액세스 관리자가 해당 액세스 제어 기능을 추가하는 것과 해당 액세스 관리자 또는 해당 식별 부호와 관련된 사용권자의 동의를 얻어 하는 것을 제외한다.)

(2) 통신 회선을 통해 특정 컴퓨터에 해당 액세스 제어 기능을 통해 특정 서비스의 제한을 피할 수 있는 정보 (식별 부호를 제외한다) 또는 지시를 입력하여 해당 전자계산기 운영이 제한되는 특정 고객의 지위를 얻는 상황을 발생시키는 행위 (액세스 관리자가 하는 해당 액세스 제어 기능을 추가와 해당 액세스 관리자의 승낙을 얻어 하는 것을 제외한다. 다음 호에서 동일)

(3) 통신 회선을 통해 연결된 다른 특정 컴퓨터의 액세스 제어 기능을 통해 사용을 제한하는 특정 컴퓨터에 그 한계를 벗어날 수 있는 정보 또는 지침을 입력하여 당해 컴퓨터를 운영하고, 제한되는 특정 서비스를 얻는 상황을 발생시키는 행위

제8조[110]

다음 각 호의 하나에 해당하는 사람은 일년 이하의 징역 또는 50만엔 이하의 벌금에 처한다.

(1) 제3조 제1항의 규정에 위반한 자

(2) 제6조 제3항의 규정에 위반한 자

9. 싱가포르 '컴퓨터 오용에 관한 법률'(Computer Misuse Act)'

영국, 호주, 일본 등과 마찬가지로 권한없는 시스템의 접근을 금지하고 있다[111]. 이웃 주민이 타인의 무선인터넷에 접속한 경우에 이를 '권한없는

110) 第八條　次の各号の一に該当する者は、一年以下の懲役又は五十万円以下の罰金に處する。
一　第三條第一項の規定に違反した者
二　第六條第三項の規定に違反した자

111) PART II OFFENCES 3. Unauthorised access to computer material
(1) Subject to subsection (2), any person who knowingly causes a computer to perform any function for the purpose of securing access without authority to any program or data held in any computer shall be guilty of an offence and

컴퓨터 접근'으로 판단하여 처벌한다.

10. 캐나다 형법

허가 없이 컴퓨터 시스템을 사용하는 행위에 대해서 제342.1조[112]에서 명시적으로 규정하여 이를 금지하고 있다.

---

shall be liable on conviction to a fine not exceeding $5,000 or to imprisonment for a term not exceeding 2 years or to both and, in the case of a second or subsequent conviction, to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both.

(2) If any damage is caused as a result of an offence under this section, a person convicted of the offence shall be liable to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 7 years or to both.

(3) For the purposes of this section, it is immaterial that the act in question is not directed at −

(a) any particular program or data;

(b) a program or data of any kind; or

(c) a program or data held in any particular computer.

112) Unauthorized use of computer

342.1 (1) Every one who, fraudulently and without colour of right,

(a) obtains, directly or indirectly, any computer service,

(b) by means of an electro-magnetic, acoustic, mechanical or other device, intercepts or causes to be intercepted, directly or indirectly, any function of a computer system,

(c) uses or causes to be used, directly or indirectly, a computer system with intent to commit an offence under paragraph (a) or (b) or an offence under section 430 in relation to data or a computer system, or

(d) uses, possesses, traffics in or permits another person to have access to a computer password that would enable a person to commit an offence under paragraph (a), (b) or (c) is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years, or is guilty of an offence punishable on summary conviction.

제 3 절 통신요금의 회피를 목적으로 타인의 서비스를 이용하는 것을 금지하는 법규

1. 미국 알래스카 주

정당한 이용요금을 회피하려는 목적으로 타인의 전기통신서비스를 획득하는 행위를 주법으로 금지하고 있다[113]. 따라서 공개된 무선인터넷 접속을 '전기통신서비스의 부정 획득'으로 판단하여 2007년 2월 WiFi를 이용해 게임 사이트에 접속하여 서비스를 무단사용한 자를 체포한 사례가 있다.

2. 영국 '통신법'(Communications Act 2003)

제125조에서 이용요금 회피를 목적으로 전기통신서비스를 부정하게 이용하는 행위를 명문으로 금지[114]하여 이웃 주민의 무선AP에 접속하는

113) AS 11.46.200. Theft of Services.
(a) A person commits theft of services if
(1) the person obtains services, known by that person to be available only for compensation, by deception, force, threat, or other means to avoid payment for the services;
(2) having control over the disposition of services of others to which the person is not entitled, the person knowingly diverts those services to the person's own benefit or to the benefit of another not entitled to them; or
(3) the person obtains the use of computer time, a computer system, a computer program, a computer network, or any part of a computer system or network, with reckless disregard that the use by that person is unauthorized.
(b) Absconding without paying for hotel, restaurant, or other services for which compensation is customarily paid immediately upon the receiving of them is prima facie evidence that the services were obtained by deception.
(c) A person may not be prosecuted under this section for theft of cable, microwave, subscription, or pay television or other telecommunications service if the service was obtained through the use of a device designed and used to intercept electromagnetic signals directly from a satellite, including a device commonly referred to as a home earth station.

행위를 '전기통신서비스의 부정 이용'으로 판단하고 있다. 이를 적용하여 2005년 차 안에서 노트북을 사용하여 이웃 주민의 무선네트워크에 반복적으로 접속한 자에 대하여 범죄의 고의는 인정하지 않았지만 '전기통신서비스의 부정 획득'을 이유로 벌금 500파운드를 과한 케이스가 있다.

3. 싱가포르 전기통신법(Telecommunications Act)

제43조[115]에서 서비스 이용요금의 회피를 위하여 고의적으로 타인의 전기통신서비스를 이용하거나 다른 사람이 이용하도록 허락하는 행위를 금지하고 있다.

4. 캐나다 형법

법 제326조에서 무보안 무선 AP 접속 행위를 형법 제326조[116]의 '전기

114) Offences relating to networks and services
125 Dishonestly obtaining electronic communications services
(1) A person who−
(a) dishonestly obtains an electronic communications service, and
(b) does so with intent to avoid payment of a charge applicable to the provision of that service, is guilty of an offence.
(2) It is not an offence under this section to obtain a service mentioned in section 297(1) of the Copyright, Designs and Patents Act 1988 (c. 48)(dishonestly obtaining a broadcasting or cable programme service provided from a place in the UK).
(3) A person guilty of an offence under this section shall be liable−
(a) on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum, or to both;
(b) on conviction on indictment, to imprisonment for a term not exceeding five years or to a fine, or to both.

115) 43. Fraudulent use of telecommunication service
Any person who dishonestly uses or permits another person to use any telecommunication service provided by a telecommunication licensee with intent to avoid payment of any charge applicable to the provision of that service shall be guilty of an offence.

116) Theft of telecommunication service
326. (1) Every one commits theft who fraudulently, maliciously, or without

통신 무단 이용'으로 판단하여 처벌하고 있다.

제 4 절 허가제도

1. 러시아

모든 WiFi 기기를 정부에 등록하고 특별한 허가를 받도록 하는 규제를 도입할지에 대하여 논의 중에 있다[117]. 이러한 규제가 시행될 경우 무선 AP 또는 WiFi 라우터 등을 사용하고자 하는 자는 관련 문서를 제출하고 면허를 얻는 등의 복잡한 절차를 거쳐야 할 것이다. 모스크바와 같은 특정 지역에서는 연방 보안국으로부터 특별한 허락을 부수적으로 받아야 한다.

---

colour of right,
(a) abstracts, consumes or uses electricity or gas or causes it to be wasted or diverted; or
(b) uses any telecommunication facility or obtains any telecommunication service.
Definition of "telecommunication"
(2) In this section and section 327, "telecommunication" means any transmission, emission or reception of signs, signals, writing, images or sounds or intelligence of any nature by wire, radio, visual or other electromagnetic system.

117) http://wifinetnews.com/archives/2008/04/russia_requires_WiFi_registration.html (2010. 7. 15. 방문) 2008년 4월 14일자 wifinetnews.com 기사 참조
Russia Requires WiFi Registration
Russian regulator requires registration: The folks at the Rossvyazokhrankultura (Russian Mass Media, Communications and Cultural Protection Service) have decided that every device with WiFi inside requires registration for use by an individual user without a transferrable license, according to The Other Russia, which picked the story up from Russian-language site Fontanka.ru.
While WiFi wasn't as broadly unlicensed in Russia as it is in most other industrialized nations, a state regulator exempted indoor use in certain bands from registration. The Mass Media agency apparently believes that it has the authority to compel this, although there's some doubt by observers as to whether it really falls in their purview.
Setting up a home WiFi network or a hotspot would require what sounds like vast amounts of paperwork, akin to putting a cell tower.

2. 남아프리카 공화국

ICSA가 규제의 주체이다. 무선 네트워크를 통한 인터넷 접속을 매매하기 위해서는 라이센스의 취득을 요구하고 이를 취득하지 않은 채 거래할 경우 트랜스미터 등의 몰수 조치가 이루어진다.

새로운 통신수단의 등장에 따라 통신시장이 변화하게 되었고 이러한 변화를 수용하고자 Telecommunications Amendment Bill of 2001이 새로이 등장하였다[118]. 이 법안에 따른 MEMORANDUM OF OBJECTS OF THE TELECOMMUNICATIONS AMENDMENT BILL, 2001은 통신사들에게 Wireless 통신기술의 이용이 가능하도록 허락하고자 만들어졌다[119].

3. 필리핀

2003년 이전에는 National Telecommunications Commission (NTC)에 의해 WiFi 대역의 사용은 금지되어 있었다. 그러나 2003년 이후 해당 대역 사용에 대한 규제를 풀면서 현재는 합법적으로 사용할 수 있게 되었다. 그러나 여전히 몇 가지 제한이 존재하는데, 실내 WiFi 이용을 위해서는 사전 등록해야 하고, 이는 약 10$정도의 등록비가 든다. 또한 실외 이용을

118) 1. Section 1 of the Telecommunications Act, 1996 (hereinafter referred to as ''the principal Act''), is hereby amended−
(e) by the insertion after the definition of ''fixed-line operator'' of the following definition:
'fixed-mobile service' means a connection to the public switched telephone network that will be provided by the holder of a publicswitched telecommunication service licence by means of a wireless connection between such licencee's end-office and the end-user's premises, provided that nothing in this definition shall exempt the provider of a fixed mobile service from holding a licence under section 30 or section 37;'

119) Purpose 1.2 Convergence and technological development in the communications industry to be recognised through inter alia allowing Telkom and the SNO to use wireless technology in its operations and the award of a multimedia licence to Sentech. This license will allow services such as video-on-demand, pay-per-view and internet over television.

위해서는 별도의 라이센스가 있어야 한다. 그러므로 WiFi 탑재 노트북을 사용할 때는 해당 등록비를 내야 한다[120].

4. 사우디아라비아

---

120) http://www.newswireless.net/index.cfm/article/941 (2010. 7. 15. 방문)
2003년 8월 19일자 newswireless.net 기사 참조
You may be forgiven for thinking that it's now legal to use WiFi in the Philippines. After all, there have been several announcements saying that the obsolete law banning it, has been revoked. But's not quite that simple! - and it might cost you money.
Outcry followed the original shock-horror discovery that Philippine WiFi was illegal. It was blogged by Cory Doctorow back on July 8th, under the headline "WiFi to be banned in the Philippines?" when he revealed that the Philippines spectrum policy didn't permit WiFi.
Doctorow quoted the National Telecommunications Commission (NTC) - which said that WiFi services, and even Bluetooth use, was still "illegal" in certain regions in the Philippines, including Metro Manila.
"I think (commercial WiFi) services have to stop because it is against the law," said Edgardo Cabarios, director of the common carrier department.
The same blog reported today that WiFi was "un-banned" in the Philippines: "The Philippines National Telecommunications Commission has just removed a ban on the use of 2400MHz frequencies" - and pointed to "a final draft of a memorandum circular posted on its website," which set out new rules governing the provision of wireless LAN services.
But the fine print pays reading, according to another commentator. "It sounds like there are still quite a few restrictions on use - including the fact that you need to pay a registration fee (about $10) to set up any indoor WiFi access point. Outdoor access points will require a licence."
In fact, if anybody in authority wanted to be unpleasant, this regulation could be even more restrictive.
Any WiFi-equipped PC normally broadcasts its network identity (SSID) whenever it is switched on. This is intended for talking directly to other wireless-equipped PCs on a "peer to peer" basis - but it's clear that under the terms of this regulation, this makes the computer an access point, requiring a registration fee.
You could sit at your hotel desk working, and be in breach of the regulation.
Finally, the new regulation seems to say absolutely nothing about using Bluetooth, which uses the same frequency, and which therefore is probably covered by the same requirement to be licensed. Almost certainly, it won't be ... unless you offend someone important in some other way.

Wireless Local Area Networks (WLAN/WiFi) Usage Regulations가 관련한 법률적 규제를 규정하고 있다. 무선랜은 CITC의 면허를 얻어야 사용할 수 있다[121]. 모든 기기는 CITC가 규정하는 기술 사용, 적용 범위, 주파수 등의 기준을 충족해야 한다. 보안기준에 대해서도 CITC의 기준을 충족하여야 한다. 무선랜을 통해 제공되는 인터넷 서비스까지 규제함을 그 내용으로 한다[122].

---

121) 4) Network Connections
These WLAN networks can be connected with the internet network by the following CITC licensees:
1. Fixed facility- based providers.
2. Data service providers.

122) 5) Rules of Operating and Using Networks
WLAN can be used as an alternative to wired networks, indoor and outdoor, and can be used to get internet service from CITC licensed ISPs under the CITC bylaw and regulations, on condition of adherence to the following rules:
1. All devices which are used in these networks must comply with the technical specifications, areas of coverage, and frequencies approved by the CITC (as shown in the attached table). It is not permitted to make any modifications in the technical specifications without prior written approval from CITC.
2. All devices which are used must comply with the safety specifications, electromagnetic compatibility, and any other CITC related specifications.
3. To provide to the CITC, when requested, all required documents to prove the compliance of the devices with the technical standard specifications and any other related documents and proofs.
4. To ensure that the operation of the devices and the appropriate places for their installation, especially in terms of improving the level of network security, will prevent any possible hacking or misuse.
5. The operator of these networks for outdoor usage must coordinate with concerned authorities to obtain any required licenses for the implementation of the network.
6. Internet service must be provided only through an internet service provider licensed by the CITC..
7. Internet service providers are responsible for registering users' data and all other technical requirements.
8. Services provided through these networks are considered secondary services; thus they are not protected against any possible interference, and must not, at anytime or anywhere, cause any harmful interference to the primary services. CITC shall not be held liable for any damages following use of these networks.

5. 호주 통신법(Telecommunications Act 1997)

2002년 9월 면제조항[123]을 신설하여 hotspot의 운영에 면허가 필요 없도록 규제를 완화하였다. 보안 문제에 관하여는 기본적인 가이드라인이 제공될 뿐, 구체적인 입법은 이루어지지 않았다.

제 5 절 기타

1. 중국

WiFi 기능을 제공하지 못하도록 규제하여 왔다. 이에 따라 아이폰의 WiFi 기능을 제거하고 판매하여 왔다. 이는 WiFi 스탠다드 대신 자국의 기술 표준인 WAPI를 이용하도록 하려는 목적으로 보인다. 그러나 2009년 시장 지배적 사업자인 China Mobile을 견제하면서 후발사업자들의 시장점유율 확대를 위하여 China Telecom과 China Unicom같은 소규모 통신 사업자에게 선별적으로 WiFi 스탠다드를 채용하도록 허용하였다[124].

---

9. The usage of these networks is subject to all CITC regulations, the anti-crime law and all other related regulations.

123) TELECOMMUNICATIONS ACT 1997 - SECT 51 Exemption--Ministerial determination
(1) The Minister may, by written instrument, determine that section 42 does not apply in relation to:
(a) a specified network unit; or
(b) a specified person; or
(c) a specified use of a network unit.
(2) A determination under this section may be unconditional or subject to such conditions (if any) as are specified in the determination.
(3) A determination under this section has effect accordingly.
(4) A determination under this section is a disallowable instrument for the purposes of section 46A of the Acts Interpretation Act 1901.

124) Relaxation of WiFi restriction could remove iPhone obstacle

2. 호주 전파통신법(Radiocommunications Act 1992)

China has relaxed a long-term restriction on WiFi functions on mobile phones, which will improve the mobile Internet experience and boost sales of smart handsets, Shanghai Daily learned yesterday.

That will probably solve the biggest obstacle for the WiFi-enabled Apple iPhone's entry into the domestic market, insiders said. Motorola Inc and Nokia Corp's two models, which also support home-grown WAPI and WiFi, have debuted in China.

The Ministry of Industry and Information Technology has told related companies to send models for market-entry tests. The models must support WAPI, and optionally WiFi, handset makers told Shanghai Daily.

"A mobile phone without WiFi is like a film with too many scenes cut. It's not complete," said Ashley Liu, an analyst with In-Stat, a United States-based IT research firm.

In the past few years, China had restricted WiFi functions on phones to prevent people using Internet call services such as Skype, which were thought to be against the interests of state-owned mobile carriers.

Now the country is trying to promote WAPI (WLAN Authentication and Privacy Infrastructure), a home-developed wireless connection technology with higher security than WiFi.

This also opened the door to WiFi, which is now widely used in personal computers, game consoles and smartphones, industry officials said.

WAPI and WiFi can be swapped through software so it won't cost much more for handset makers to launch these phones in China.

Motorola, which launched a phone supporting WCDMA (wideband code division multiple access), WiFi and WAPI in China last week, will continue to launch more WiFi-enabled phones in the domestic market, said Derek Li, Motorola's vice president.

Shenzhen-based ZTE also confirmed that a CDMA phone with WAPI and WiFi was being tested.

"With the relaxing of WiFi, our sales in China will jump another 20 percent because we produce smartphones. They require many online applications," said Jackie Zhang, market director of phone maker Dopod.

WiFi allows users to access the Internet where mobile broadband signals are not available or weak. It's seen as vital technology for 3G.

The sales of WiFi-enabled consumer electronics will reach more than 900 million units by 2012, double last year's sales, according to In-Stat.

WiFi will allow relatively smaller mobile carriers, such as China Telecom and China Unicom, catch up with market leader China Mobile. ;

http://www.chinatradeinformation.net/china-trade-news/relaxation-of-WiFi-restriction-could-remove-iphone-obstacle.html (2010. 7. 15. 방문)

2.4GHz 대역을 'Public Park'으로 공공을 위한 영역으로 설정하였다[125]. 사용자 및 서비스 프로바이더는 이 대역에 있어 서비스 보안 문제, 향후 수익 손실 문제, 서비스 질 문제 등을 고려하도록 규정하였다.

125) SECT 32 Frequency band plans
(4) A frequency band plan:
(a) must make provision in relation to the purpose or purposes for which the band or bands may be used; and
(b) without limiting paragraph (a), may provide for:
(i) the one or more purposes for which any part of a band (including any particular frequency or frequency channel) may be used; and
(ii) parts of the spectrum to be reserved for provision of public or community services.

제 4 장 무선랜 보안 침해 사례

제 1 절 해외 무선랜 침해 사례

1. 인증이 필요한 WiFi 침해 사례

가. 인증이 필요한 WiFi에 무단 접속한 사례

인증이 필요한 사설 WiFi에 타인이 무단 접속한 것만을 가지고 처벌하였거나, 특별히 피해가 있었다고 보고된 사례는 특별히 발견되지 않는다. 인증이 필요한 타인의 WiFi에 접속하는 것은 대개 위법한 목적을 가지고 이뤄지는 것이 대부분으로, 대표적인 사례에 대해서는 아래에서 다루도록 한다.

나. 인증이 필요한 WiFi에 무단 접속하여 추가적인 위법행위를 한 사례

- 슈스터 사건 (미국)

(1) 사실관계

2000년부터 슈스터는 위스콘신주 워소의 알파컴퓨터서비스(용역업체) 소속의 기술자로 일하였다. 그의 업무는 무선랜 인터넷서비스업체인 CWWIS에 대하여 기술지원 서비스를 제공하는 것이었다. 슈스터는 CWWIS의 유료 가입자이기도 하였다.

2003. 5. 14. 슈스터가 CWWIS의 한 가입자에게 기술지원제공을 거절한 것을 이유로 알파사는 슈스터를 해고하였다. 같은 날 CWWIS는 슈스터에게 CWWIS 무선인터넷 접속을 종료한다는 내용의 등기우편을 보냈고

월사용료 잔액을 환급하였다.

이에 분개한 슈스터는 그동안 알게 된 다수의 CWWIS 가입자들[126]의 무선랜접속 암호를 이용하여 그의 집에서 계속하여 CWWIS 무선랜 네트워크에 접속하였다. 슈스터의 이러한 무선랜 접속 행위로 인하여 피해자들은 인터넷 연결에 장애를 겪게 되었고, 업무 생산성이 저하되는 피해를 입었다.

슈스터는 2003. 10. 6. 경찰관이 수색영장을 집행하여 슈스터의 컴퓨터를 압수할 때까지 이러한 CWWIS 네트워크의 무단 사용을 계속하였다.

(2) 법원 판단

2004. 10. 27. 연방대배심은 생산성 저하와 추가비용 등 피해액을 6,014불로 산정하여 5,000불 이상의 손해의 발생 요건을 충족시킨다고 하며, CFAA(Computer Fraud and Abuse Act)법의 18 U.S.C. §1030(a)(5)(A)(I) 위반[127]과 18 U.S.C §1030(a)(5)(A)(ii) 위반[128] 두 가지 혐의로 기소하였다.

2005. 5. 13. 슈스터는 유죄를 인정하였다(pleaded guilty). 그러나 1심법원의 손해배상액 산정(19,060불)이 과다함을 이유로 항소하였다

2. 개방된 무선 네트워크(오픈 WiFi) 침해 사례

가. 타인의 공개 무선 네트워크의 무단 이용(Piggybacking) 사례

---

126) T.D. Fischer Group, Riverbend Properties, the Wausau/ Central Wisconsin Convention & Visitors Bureau, and Straight Shot Express

127) knowingly causing the transmission of a code, program, command, or information to a protected computer used in interstate commerce and communication and intentionally causing damage of at least $5,000 to the computer and to the computer's user and customers

128) intentionally accessing a protected computer used in interstate commerce and communication without authorization and recklessly causing damage of at least $5,000 to the computer and its user and customers.

(1) Gregory Straszkiewicz 사건 (영국)

(가) 사실관계

2005년 영국에서 Gregory Straszkiewicz라는 이름의 한 남자가 타인의 무선 브로드밴드 네트워크를 강탈한 혐의로 체포되어 500파운드의 벌금과 12개월의 조건부 석방을 구형받았다[129].

Straszkiewicz는 자신이 살던 주거지역 내에 타인의 건물 밖에서 무선 접속이 가능한 노트북을 들고 서 있다가 체포되었다. Straszkiewicz는 타인의 가정에서 이용하는 무선 네트워크를 무단으로 이용하려고 했다고 진술했으며, 경찰에 체포되기 전에도 몇 차례 이러한 이용을 시도한 바 있었다고 진술했다.

(나) 법원 판단

런던의 Islewoth 법원은 Straszkiewicz이 무단으로 타인의 전자 통신을 습득하고, 사기적인 목적으로 통신 서비스를 이용하기 위한 장비를 가지고 있다는 이유로 Communications Act 위반으로 유죄를 선고했다.

(2) Kauchak 사건 (미국)

(가) 사실관계

David M. Kauchak는 위네바고 카운티에 있는 공원에서 차를 주차한 채 컴퓨터로 타인의 네트워크에 접속하다가 체포됐다.

---

129) Den llett, "Wireless network hijacker found guilty", Silicon.com, 2005. 7. 22. see http://management.silicon.com/government/0,39024677,39150672,00.htm(2010. 7. 17 방문).

(나) 법원 판단

이 후, Kauchak는 타인의 컴퓨터 시스템에 허락을 받지 않은 채 무단으로 접속한 혐의로 유죄를 선고받았다. 그는 250$의 벌금형과 법원으로부터 1년간 감시감독 받을 것을 선고 받았다.

이와 유사한 사례로, 2005. 4. 20. 미국의 템파베이 경찰은 타인의 공개된 residential WiFi 네트워크에 접속한 남자를 '서비스 절도'를 이유로 3급 사기 혐의로 체포한 바 있다.

(3) Garyl Tan Jia Luo 사건 (싱가포르)

2006년 싱가포르의 Garyl Tan Jia Luo라는 10대 소년은 이웃의 무선 네트워크에 접속하다가 기소됐다. 싱가포르의 경우 이러한 경우 최대 3년형과 10,000 싱가포르 달러의 벌금형을 선고할 수 있으나 법원은 Tan이 빨리 국가의무를 수행할 경우 이를 완화할 수 있다고 밝혔다.

나. 오픈 WiFi에 접속하여 추가적인 위법행위를 한 사례

(1) Barry Vincent Ardolf 사건 (미국)[130]

미네소타에 사는 45살의 Barry Vincent Ardolf는 이웃의 무선 네트워크를 해킹하고, 그의 개인정보를 사용하여 이메일 계정을 만든 뒤 부통령을 살해하겠다고 협박하는 이메일 등을 발송한 혐의로 2010년 6월 미네소타 연방법원에 기소되었다[131].

검찰에 따르면 Ardolf는 2009년 2월부터 'Aircrak'이라는 해킹 소프트

130) 미네소타 주 검찰의 보도자료를 참고하여 작성, 원문은http://www.cybercrime.gov/ardolfIndict.pdf 참조(2010. 7. 17 방문).

131) Thomas Calburn, "WiFi Hacker indicted in Veep Threat", Information Week, 2010. 6. 25. see http://www.informationweek.com/news/software/showArticle.jhtml?articleID=225701522.

웨어를 사용하여 이웃의 WiFi의 암호를 해제, 그의 네트워크를 무단으로 사용할 수 있었다고 한다. 그는 이웃의 개인정보를 이용해서 여러개의 야후 메일 계정을 만든 뒤 이웃의 직장동료 등에게 아동 포르노그라피를 보내고, 미네소타 주지사, 부통령 등에게 테러를 하겠다는 협박 메일 등을 보냈다.

검찰은 Ardolf의 유죄가 확정될 경우, 아동 포르노그라피 배포 및 소지 혐의로 각각 최대 20년과 10년, 타인의 컴퓨터 네트워크에 침입한 혐의로 각각 5년, 타인의 개인정보를 훔친 혐의로 각각 2년형을 선고받을 수 있다고 주장하고 있다.

(2) Brian Salcedo 사건 (미국)

(가) 개요

차 안에 특별히 장치가 달린 노트북과 안테나를 갖춘채 공개된 무선 네트워크를 찾는 것을 Wardriving이라고 하는데, 이를 해킹에 활용한 대표적 사례다.

(나) 사실관계

2003년 미국 디트로이트의 교외에서 Brian Salcedo와 그의 공범인 Adam Botbyl이 North Carolina의 한 대형철물점(Lowe's)의 주차장에 차를 주차하고, 그 안에서 그 상점의 보호되지 않은 WiFi 정보망을 해킹하여, Lewe's의 전국 체인의 고객 신용카드 리스트 등 주요 정보를 획득하고자 하였다가 적발되었다.

Salcedo 등은 해킹 등에 사용하려던 목적으로 무료로 공개된 WiFi Hotspot을 찾다가 우연히 Lowe's의 미시건 사우스필드지점의 무선 네트워크가 보안 설정이 되어있지 않다는 것을 알아냈다. 이 후 이를 범죄에 악용하기 위해 알아보던 중 지역 소매지점의 네트워크를 통해 노스캐롤라이나

주에 위치한 고객의 데이터를 관리하는 중앙 데이터센터에 접근할 수 있다는 것을 발견했다.

그러나 이들이 해킹을 시도하는 과정에서 Lowe's 측이 먼저 자신의 네트워크 침입 흔적을 발견하고, 이를 이상하게 여겨 FBI에 미리 신고하였고, 이에 미리 잠복해 있던 수사관들에게 이들이 신용카드 정보를 수집하기 위해 주차장에 있는 것이 적발되어 체포되었다.

특히, Salcedo 등은 Lowe's가 고객의 신용카드 결제를 관리하는 소프트웨어인 'tcpcredit'를 수정하여, 신용카드 정보를 은닉하였다가 자신들이 필요할 때 가지고 나올 수 있도록 하였다고 한다. 적발 당시 해당 프로그램은 6개 정도의 신용카드 정보를 저장하고 있었다고 보고되었다.

(다) 법원 판단

Justice Deartment는 CFAA를 근거로 Salcedo를 기소하였고, 2006년 7월 10일. 항소심은 Salcedo에게 9년 징역을 선고하였다[132].

(라) 시사점 등 기타

이 사안에 대한 법원의 판단이 주목받았던 이유는 Salcedo 등의 범죄는 미수로 적발되었기 때문에, 실제로는 어떠한 손해도 발생시키지 않았는데도 불구하고, 이는 미국 해킹 관련 판결 중 가장 긴 징역을 선고받은 것에 해당하였기 때문이다.

이렇게 긴 징역이 선고된 것은 만약 그들의 계획이 성공했을 경우 초래할 수 있는 위험에 기반하였던 것으로 풀이되고 있다. 법원 역시 만약 Salcedo가 성공했다면 적어도 250명 이상의 희생자가 자신의 정보를 도난당했을 것이므로 그의 징역을 늘린 것이라는 취지의 판결을 내렸다[133].

---

132) see http://pacer.ca4.uscourts.gov/opinion.pdf/054147.U.pdf

133) Rovert V. Hale Ⅱ, Esq., Current Developments in WiFi Liability and Regulation, Hottest Issues in Cyberspace Law Cyberspace Committee, Business

그러나 이들이 실제로 범죄에 성공하지 않았는데도 불구하고 너무 지나치게 긴 형량을 내린 것이 아니냐는 비판도 적지 않다. 예를 들어 Salcedo에 대한 판결이 있기 불과 1달 전, 피싱과 스팸기술을 이용해 고객들의 신용카드 정보를 훔치는 데 성공한 Andrew Mantovani 사건의 경우 Mantovani에게 32개월의 징역이 선고되었는데, 이에 비하면, Salcedo의 징역은 지나치게 길어 형평에 맞지 않다는 의견도 존재한다[134].

(3) Albert Gonzales 사건 (미국)[135]

(가) 사실 관계

2009년 미국에서 "Soupnaz"라고 알려진 해커들로 이뤄진 갱단이 오픈된 WiFi망을 이용하여 7 Eleven, TJ Maxx와 같은 여러 상점의 현금수납기 인증시스템을 해킹, 수천만달러 규모의 고객 신용카드 기록을 탈취하였다가 적발되어 기소됐다.

이 사건을 주도한 사람은 마이애미에 살고 있던 28살의 Albert Gonzales로 그는 위와 같은 방식으로 TJ Maxx에서만 무려 4천만개가 넘는 신용카드 정보를 수집한 것으로 알려졌다. 또한 Gonzales가 정보를 탈취한 대상으로 Heartland Payment Systems도 포함되었는데 이는 미국 내 주요 신용카드 발급회사로, 그는 이곳에서 약 1억 3천만개의 신용카드 번호를 훔친 것으로 알려져 충격을 주었다.

Gonzales는 이 전에도 레스토랑 체인의 네트워크를 해킹하는 등 유사한 범죄를 저지른 경력이 있었는데, 자신을 포함하여 여러 해커로 구성된

Law Section State Bar of California (2006)

134) Kevin Poulsen, "Crazy-Long Hacker Sentence Upheld", Wired, 2007. 11. 06. see http://www.wired.com/science/discoveries/news/2006/07/71358

135) James Gordon Meek, "Hacker Albert Gonzalez charged with largest ID theft ever involving 130M credit, debit cards", NY Daily news, 2009. 08. 19. see http://www.nydailynews.com/news/national/2009/08/17/2009-08-17_hacker_albert o_gonzales_charged_with_larged_id_theft_ever_involving_130m_credit_.html .

갱단을 조직, 신용카드 정보를 탈취하는 범죄를 저질렀으며 이로 인해 수백만개의 신용카드가 재발급되어야 했다고 한다.

(나) 법원 판단

2010년 3월 법원은 Gonzales에게 20년 징역형을 선고하였고, 이는 현재까지 미국 내 사이버 관련 범죄에 선고된 형 중 가장 긴 것으로 기록되었다.

(다) 관련 민사 소송

특히 이 사건으로 인해 피해를 입었던 TJ Maxx는 이 후 엄청난 민사상 손해배상 요구에 시달렸다. TJ Maxx의 이사회 등은 고객의 중요한 개인정보를 제대로 지킬 의무를 다하지 못했다는 이유로 Louisiana police retirement fund를 비롯한 투자자, 신용카드 발급자, 소비자 등으로부터 소송 위협을 당하였다. TJ Maxx는 무려 1억 7천8백만불을 이 사건과 관련한 위로금으로 마련해두었고, 이 예산을 활용해 소송을 화해로 종결시키고 있다고 알려졌다[136].

(4) Wake Internal Medicine Consultants 사건 (미국)

(가) 사실 관계

2003년 노스캐롤라이나 주의 Clayton Dillard는 Wake Internal Medicine Consultants의 무선 인터넷에 접속해 2,000명이 넘는 환자의 진료기록을 무단으로 가져가다 적발되었다.

---

136) Hiawatha Bray, "Investor, TJX settle suit over data theft", The Boston Globe, 2010. 7. 7., see http://www.boston.com/business/articles/2010/07/07/investor_tjx_settle_suit_over data_theft/?rss_id=Boston.com+--+Top+business+news(2010. 7. 17 방문).

(나) 법원 판단

Dillard는 자신이 해당 의료시설의 무선 인터넷 관리 및 환자 진료기록 보안이 얼마나 취약한지에 대해 증명하기 위해 이와 같은 해킹을 시도하였다고 주장하였으나, 위법행위를 하였다는 것은 변함없다고 법원은 밝혔다고 한다.

Dillard는 18개월의 보호관찰과 1만 달러의 벌금형에 처해졌다. 특히, 이 사건은 미국 무선 인터넷 해킹으로 인해 해킹범이 유죄판결을 받은 첫 번째 사례로 기록되었다.

(5) Nicholas Tombros 사건 (미국)[137]

(가) 사실 관계

2004년 마흔살의 Nicholas Tombros는 공개된 WiFi 망을 찾아다니며 스팸을 발송한 혐의로 체포되었다. FBI에 따르면, Tombros는 LA의 Venice 해변의 도로를 노트북과 안테나를 가지고 다니면서, 보안을 적용하지 않은 가정용 사설 무선 AP를 찾아다니는 방법으로 범죄를 행했다고 한다.

그는 이러한 AP를 찾은 뒤에는 이 AP가 추적이 불가능하다는 점을 악용하여, 포르노 사이트 광고를 담은 수천개의 스팸메일을 발송하였다.

이러한 방법으로 그는 5개 이상의 IP주소를 훔쳐 스팸을 발송했다고 한다.

특히, Tombros는 이와 같은 범죄를 하기 전 신용카드 관련 회사에서 일한 경험이 있어 다량의 고객 메일 주소를 습득하였고, 이를 범죄에 활용하였다고 한다. 그는 스팸을 보내면서 자신의 출처를 숨기기 위해 스팸 메시지를 정교하게 속이고, 가명으로 4~5개의 메일 계정을 만들어 발송하였다.

---

137) John Leyden, "WiFi spam man avoids can Probation for smut site junk mail miscreant", The Register, http://www.theregister.co.uk/2007/08/01/smut_spam_wifi/(2010.7.17 방문).

(나) 법원 판단

Tombros는 Federal Can-Spam Act.에 있는 타인의 컴퓨터를 스팸을 보내는데 사용하는 것을 금지한 규정을 위반한 혐의로 법원으로부터 유죄를 선고받았다. 검찰은 Tombros에게 약 3년형의 징역을 주장했으나, 이후 유죄 협상(Plea Bargaining) 10,000달러의 벌금을 무는 것으로 사건이 종결되었다.

(6) Myron Tereshchuk 사건 (미국)[138]

2004년 미국 워싱턴 D.C.에서 공개된 무선 네트워크를 통해 한 특허 회사에게 위협메일을 줄곧 발송하던 Myron Tereshchuk가 FBI 감시팀에 적발되었고, 유죄를 인정하였다.

Tereshchuk는 피해자인 특허회사, MicroPatent에게 그가 취득한 정보를 발설하지 않는 조건으로 1천 7백만 달러를 요구하였다가, 통상에 영향을 미치는 부당이득 시도(attempted extortion affecting commerce)로 기소되었다.

이 사건이 있기 전에 Tereshchuk은 작은 특허 문서 서비스를 제공해 오다가, U.S 특허 및 상표 사무국으로부터 특정한 파일을 삭제하였다는 이유로, 설비 이용 등이 금지되는 처분을 받게 되었다. 이 처분에 대해 앙심을 품은 Tereshchuk은 자신이 특허 및 상표 사무국의 부정으로 인한 희생양이 되었다는 의심을 품게 되었고, 특히 MicroPatent라는 회사를 비난하기 시작, 그 사무소의 고객들과 대표 등을 괴롭히는 메일 등을 발송하였다.

이로 피해를 입고 있던 MicroPatent의 대표는 메일을 발송하는 자가 누구인지 알기 위해 추적하였으나, 그 메일은 추적이 불가능하였다. FBI가 추적한 결과 문제의 메일은 각각 가정집이나 치과 등에서 설치한 802.11b 공개 네트워크를 통해 발송된 것으로 밝혀져 범인을 잡는 것이 어려워질 것으로 여겨졌다.

---

138) Kevin Poulsen, “WiFi hopper guilty of cyber-extortion”, Security Focus, 2004. 6. 25. http://www.securityfocus.com/news/8991(2010. 7. 17 방문).

그러다가 과거 Tereshchuk가 MicroPatent와 언쟁을 벌여왔던 사실이 알려지면서 Tereshchuk가 유력한 용의자로 떠올랐고, 그가 이후 MicroPatent에 1천 7백만 달러를 요구하면서 이러한 정황은 더욱 분명해져, FBI는 그를 감시해왔다고 한다. 그 결과 Tereshchuk가 매릴랜드 대학의 컴퓨터 연구실로 운전하여, 학생들의 메일 계정을 훔쳐 위협하는 메일을 보내는 것을 FBI가 적발해 기소에 이르게 되었다.

다. 구글 스트리트뷰 사례

(1) 개요

구글이 자사의 3차원 지도서비스 GSV(Google Street View)를 위해서는, 자동차를 이용해 데이터를 수집하는데 이 과정에서 불법적인 개인정보 수집이 있는지가 문제가 되고 있다. 구글의 스트리트뷰는 지도에 사람의 눈높이에 맞는 360도 사진을 더해 이용자가 거리를 걸으면서 보는 듯한 효과를 주는 서비스다.

이 서비스가 논란을 불러일으키게 된 발단은 이 서비스를 제작하기 위하여, 특수 카메라를 장착한 스트리트뷰 차량이 곳곳을 촬영하는데, 이 과정에서 사생활이 그대로 노출된다는 점이 지적이 제기되면서이다. 지난 3월 대만에선 여성이 자신의 아파트에서 알몸으로 서있는 모습이 찍히기도 했다.

특히 무선 인터넷과 관련하여 문제가 되는 것으로는 구글의 스트리트뷰 서비스를 위한 전용 자동차에 무선 패킷을 수집하는 장치가 있다고 알려지면서, 이 정보들이 수집되는 것이 개인 사생활을 침해할 우려가 있다는 것이다. 문제가 된 장치는 무선 인터넷 유저들만의 특정한 WiFi 네트워크명(SSID 정보), 이용자들의 기지국 위치정보, 하드웨어 식별번호(MAC 어드레스) 외에도 무선망을 통한 이메일, 비디오, 오디오, VoIP 정보들까지 수집할 수 있었던 것으로 알려졌다.

스트리트뷰 전용차량이 360도 회전할 수 있는 특수카메라를 장착한 채 도심을 달리고 있다(왼쪽). 영국의 웨스트미들랜즈 윔본 지역 스트리트뷰에 남녀 한 쌍이 풀밭에서 키스하는 장면(원안)이 찍혀 있다. 출처=더선

(그림 4-1) 구글 스트리트 뷰 관련 사진

(2) 각국의 반응

(가) 미국

미국 오레곤주와 워싱톤주에서 암호화되어있지 않은 가정용 무선 네트워크를 운영하고 있는 이용자들이 구글을 상대로 연방 개인정보 및 데이터 수집법(federal privacy and data acquisition laws)을 어긴 혐의로 집단소송을 제기하였다.

원고측은 구글이 Title 47 of the U.S. Code도 어겼다고 주장하고 있으며, 구글이 정보를 획득한 사람들에게 개인당 최대 10만 달러까지 배상할 것을 요구하고 있다.

또한, 원고들은 당초 개인정보 수집에 관련한 혐의뿐만 아니라, 구글이 와이파이 탐지 기술(WiFi sniffing technology)을 이미 일년 반 정도 전에 특허를 받았고, 이 기술은 구글이 자동차에 여러 개의 안테나를 탑재해, 발송기의 더 정확한 위치를 측정할 수 있는 것이라고 주장하고 있으며, 이 기술은 이용자의 무선AP의 위치를 계산해, 특정이용자로부터 더 다양하고 많은 무선 정보를 얻고, 분석할 수 있다고 한다. 특히, 구글의 “gslite”라는 코드는 GSV용 자동차에서 이용하는 암호화되지 않은 무선 네트워크를

통해, 보내진 개인정보의 일부를 기록한다고 한다.

한편 미국의 FTC (Federa Trade Commission) 역시 구글의 스트리트 뷰 서비스에 대해 조사에 들어간 것으로 알려졌다.

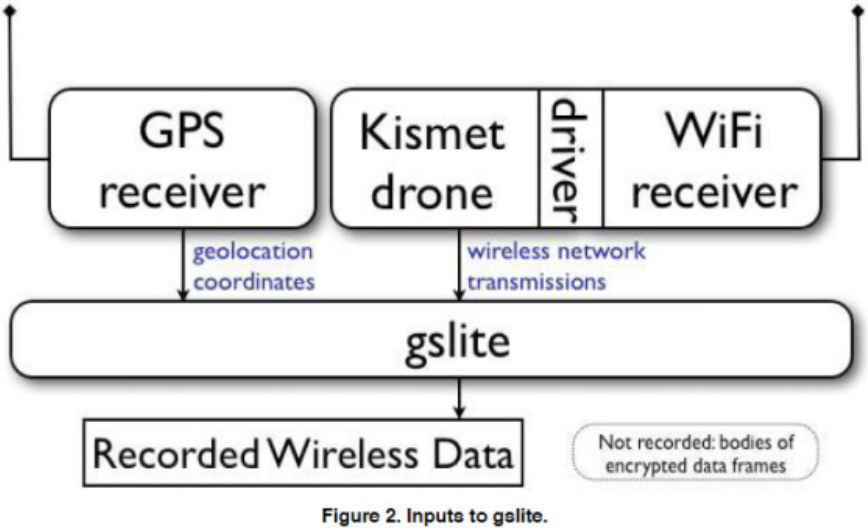


Figure 2. Inputs to gslite.

(그림 4-2) 구글의 “gslite"

(나) 독일

구글의 스트리트뷰 차량이 일반인들의 공개된 WiFi 네트워크를 통해 활용되어, 무선 인터넷 정보를 수집할 수 있다는 우려를 처음으로 제기한 국가가 바로 독일이다.

독일 함부르크 자료보호국(DPA)은 위와 같이 구글 스트리트 뷰 서비스가 사생활을 침해할 수 있음을 지적, 구글에 정보 제출을 요구하였다. 특히 독일에서는 구글이 ‘인건비 명세’ 등 사적 데이터까지 수집한 것으로 확인돼 경찰이 조사에 나섰다.

일제 아이그너 독일 농업·소비자부 장관은 구글의 3차원 지도 서비스를 막기 위해 “법적 조치와 법률 개정을 검토 중”이라고 밝혔다고 한다.

특히 독일의 DPA측은 구글이 WiFi 네트워크에 대한 다양한 정보

(위치, 이름, 프로텍션 프로토콜 등)들을 수집하는 것에 대해서 무척 우려하고 있다고 한다. DPA 위원 Peter Schaar에 따르면, 이러한 정보들이 결국에는 물리적 맥 어드레스 정보로 이어지고, 이는 곧 실제 이용자들의 현재 위치 정보를 알려주는 IP 주소들로 연결될 수 있기 때문에 문제된다고 한다.[139]

(다) 프랑스[140]

프랑스는 구글이 스트리트뷰 서비스가 개인 정보를 수집하고 있다는 혐의 아래 조사에 착수하였다. 그 과정에서 WiFi를 통해 수집된 개인정보에 무선 인터넷 이용자들의 이메일 비밀번호와 메시지 내용까지 포함되어 있다는 조사결과가 밝혀졌다.

프랑스의 정보처리와 자유에 관한 국가심의회(National Commission on Computing and Liberty·CNIL)는 "구글이 제출한 자료를 조사한 결과 이메일 비밀번호와 일부 내용이 기록돼 있음을 확인했다"고 전했다.

CNIL은 2010년 6월 4일 구글로부터 하드디스크 2개, 서버 접속 관련 자료 등을 제출받아 조사에 착수했다.

또한 구글은 CNIL측에 스트리트뷰 자동차로 수집한 데이터가 구글 지도, 구글 래티튜드(Google Latitude) 등 친구와 자신의 위치를 공유하는데 활용되는 다른 서비스에도 사용됐다고 밝혔다고 한다.

아직 CNIL이 구글에 어떤 사법조치를 취할 것인지 알려져 있지는 않다.

(라) 호주[141]

---

139) Lucian Parfeni, "German Officials 'Horrified' by Google Street View WiFi Snooping", Softpedia, 2010. 4. 23. http://news.softpedia.com/news/German-Officials-Horrified-by-Google-Street-View-WiFi-Snooping-140439.shtml(2010. 7. 17 방문).

140) Tom Espiner, "Google's WiFi net caught passwords, says France", ZDnet, 2010. 6. 21. see http://www.zdnet.co.uk/news/security/2010/06/21/googles-WiFi-net-caught-passwords-says-france-40089304/(2010. 7. 17 방문).

141) 정지원, "호주 "구글 스트리트 뷰 사생활 침해", CNB 뉴스, 2010. 7. 11. see http://news.cnbnews.com/category/read.html?bcode=119323(2010. 7. 17 방문).

호주 정부도 구글의 스트리트 뷰가 개인의 사생활을 침해한다는 결론을 2010년 7월 10일 도출했다. 호주 사법당국은 구글의 스트리트 뷰 차량이 지도를 작성하는 과정에서 개인의 무선 데이터 통신 정보를 수집한 것이 호주 사생활 보호법을 침해했다고 규정했다.

사법당국은 어떤 종류의 개인정보를 수집하든 호주의 사생활 보호법을 위반하는 것이라고 설명했다. 다만, 호주 당국은 현행 사생활 보호법을 적용해 구글에 대한 제재를 내릴 수는 없다면서 대신 사과를 요구했다고 한다.

(마) 영국[142]

영국 ICO(Information Commissioner's Office)는 구글이 수집한 자국 관련 정보를 지울 수 있음을 경고하고 구글이 이를 삭제할 것을 요청했다고 밝혔다. 또한 Privacy International 측은 구글의 무선 네트워크 정보 수집에 대해 민형사상 조치를 취할 것이라는 입장이다.

더 나아가 영국은 구글이 무선 WiFi의 AP 정보를 수집한 것에 대해 경찰 수사에 착수했다고 전해졌다. 관계 당국에 따르면 구굴의 무선 AP 정보 수집은 the regulation of investigatory powers act (RIPA) 위반에 해당될 수 있다고 한다.

영국 Metropolitan 경찰은 구글 UK 사무국에 있는 직원을 소환해 조사하고, 구글이 수집한 정보를 조사할 것이라고 전해졌다.

(바) 홍콩, 싱가포르 등 아시아

142) Charles Arthur, "Google keeps Street View's UK WiFi data as privacy group seeks legal action", Guardian.co.uk, 2010. 5. 21. see http://www.guardian.co.uk/technology/2010/may/21/google-street-view-uk-data ; 이외에 Jamie Pert, "Google Street View WiFi Data Collection – Sparks UK Investigation", PR News, 2010. 6. 22 http://www.product-reviews.net/2010/06/22/google-street-view-wifi-data-collection-sparks-uk-investigation 도 참조.

유럽이 구글의 스트리트 뷰 서비스의 무선 네트워크 정보 수집에 대해 반대하는 입장을 명백히 하는데 반해 아시아 국가들은 아직 이에 대해 침묵을 지키고 있다고 보여진다[143].

홍콩의 PCPD(Privacy Commissioner for Personal Data)는 아직까지 "고려 중"이며, 명확한 입장을 밝히지 않고 있다. 또한 싱가포르의 Infocomm Development Authority of Singapore(IDA) 역시 구글이 무선 네트워크 정보를 수집하는 지 여부에 대해 알아보고는 있으나 현재로서 특별한 입장은 없다고 밝혔다고 한다.

(3) 구글의 항변 및 사후 조치

구글에 따르면, 구굴의 위치정보 수집 소프트웨어(SW)가 잘못 짜여져 인증 기능이 없는 사설 와이파이를 통해 스트리트뷰 서비스를 위한 정보 외에 부가정보를 소프트웨어가 추가적으로 수집하면서 문제가 발생한 것이라고 한다.

구글은 구글이 GSV 준비 과정에서 암호화되지 않은 무선 네트워크를 사용하면서, 기본적인 무선 네트워크 정보 등이 수집된 것은 사실이지만, 이는 고의적인 것이 아니었다고 항변하고 있다.

특히 앨런 유스타스 구글 엔지니어링·연구 담당 수석부사장은 개인정보가 암호 등 보안체제를 갖추지 않은 와이파이(WiFi) 망에서만 수집됐다면서 "구글의 어떤 서비스에도 이 정보를 사용하지 않았다"고 말했다.

또한 호주 등에서 개인의 무선 네트워크 통신 정보를 수집한 것이 사생활 보호법 위반이라는 논란이 일자, 구글은 9일 호주 블로그를 통해 이번 사건은 실수로 일어난 것으로 유감스럽게 생각한다면서 지도작성 차량에서 와이파이 수신장치를 제거했다고 말했다.

---

143) Vivian Yeo, "Google, Asia mum about Street View fate", ZDNet, 2010. 7. 16, http://www.zdnetasia.com/google-asia-mum-about-street-view-fate-62201392.htm(2010. 7. 17 방문).

(4) 국내 대응 현황 및 분석

국내에서도 구글의 스트리트뷰 서비스 준비과정에서 와이파이를 통해 개인정보가 수집된 것으로 알려져 방송통신위원회가 구글측에 확인 자료 요청에 나선 것으로 전해졌다. 국내에는 아직 스트리트뷰 서비스가 정식 도입되진 않았지만, 구글코리아는 지난해 10월 14일 도입을 위해 서울지역 거리 촬영에 나섰다고 밝힌 바 있다.

구글의 의도나 정보의 공개 여부와 관계없이 무단수집 자체만으로도 국내법을 위반했을 가능성이 있다. 먼저 구글이 차량을 이용해 무단으로 수집한 정보에 개인의 이메일이나 검색 정보 등 개인정보가 포함됐다면, 이 경우 구글코리아는 정보주체의 동의없이 개인정보를 무단으로 수집한 것이 되어, 정보통신망법 제22조 제1항을 위반하여 동법 제71조의 벌칙에 따라 5년 이하의 징역 또는 5천만원 이하의 벌금에 처하게 된다.

또한 정당한 접근권한 없이 정보통신망(사설 와이파이)에 침해한 것으로 판단될 경우 정보통신망법 제48조 제1항을 위반하여 동법 제72조 제1항의 벌칙에 따라 3천만원 이하의 벌금이나 3년 이하의 징역에 처해질 수 있으나, 후술하는 바와 같이 개방된 AP에 접근한 것 그 자체만으로 정당한 접근권한이 없이 침해한 것으로 해석하기는 어려울 것이다. 이 밖에도 통신비밀보호법이 금지하는 '감청'에 해당되는가를 판단할 수도 있는데, 통신비밀보호법에 따르면 발신기지국 위치정보는 통신사실확인자료가 돼 감청의 영역에 포함되므로, 법원의 영장없이 감청한 경우로 판단되면 10년이하의 징역이나 5년 이하의 자격정지를 받게 된다. 그러나 사설 AP를 통신비밀보호법상의 발신기지국에 해당된다고 볼 수는 없으므로, 역시 통신비밀보호법상의 감청에 해당된다고 보기는 어려울 것이다.

결국 구글 사건의 경우에 사실관계를 파악하여 구글이 수집한 정보가 개인정보에 해당하는 정보였다면, 정보통신망법 제22조를 위반한 것이 되어 위법한 행위로서 처벌되어야 할 것이다. 그러나 구글이 단순히 무선랜 AP가 존재하는가 그리고 그것이 개방되어 있는가 아니면 보안이 설정되어 있는가를 판단하고 또 AP의 특성에 관한 순수히 기술적인 정보만을 수집

하거나 개방된 AP에 접속한 사실 그 자체만으로 정보통신망법을 위반했다고 보기는 어려울 것으로 생각된다.

법적용의 어려움과 별도로 구글 사건은 개방된 AP가 가져올 정보유출의 위험성을 잘 보여주는 실례로서, 무선랜 보안의 위험에 대한 경각심을 불러일으키는 좋은 계기가 될 수 있을 것이라 생각된다. 특히 개방된 무선랜을 통해서 유통되는 개인정보는 제3자가 마음만 먹으면 손쉽게 그리고 대량으로 확보할 수 있다는 사태의 심각성을 전 세계에 널리 일깨워주는 사례라고 할 수 있다.

3. 오픈 WiFi 제공자의 책임

가. 무선 AP 최초 설정시 암호 설정 의무 인정 (독일)[144]

(1) 개요

독일 연방대법원은 2010년 5월 무선 인터넷 이용자는 자신의 개인 무선 네트워크가 제3자로 하여금 저작권을 위반하는 목적으로 사용되지 않도록 암호를 설정할 의무가 있다는 취지의 판결을 내렸다.

이 판결에 따르면 무선 인터넷 이용자는 만약 자신의 AP에 적절히 보안을 유지하지 않음으로써 제3자가 이를 통해 불법적으로 음악이나 다른 파일들을 다운로드 받을 경우, 최대 100 유로(약 123달러)의 벌금을 물 수 있다.

(2) 사실관계

독일 연방대법원 판결이 나오게 된 사실관계를 보다 자세히 살펴보면, 독일의 한 음악가가 한 인터넷 이용자를 고소했다. 음악가는 그 인터넷 이용자의

144) Kirsten Grieshaber, "German court orders wireless passwords for all", AP, 2010. 5. 12. see http://www.msnbc.msn.com/id/37107291/ns/technology_and_science-security/등 참조.

무선 네트워크가 불법적으로 음악 파일을 다운로드 받는데 이용되었고, 결국 그 파일이 온라인 파일 공유 네트워크에 제공되었다고 주장했다. 이에 그 이용자는 자신이 문제의 음악파일이 자신의 무선 네트워크를 통해 다운로드 되던 당시에 휴가 중으로 집을 비웠다는 사실을 입증했다.

하급심에서는 저작권 침해에 대해 구체적인 인식이 있는 경우가 아니라면, 타인의 위법한 행위에 대해 보호조치를 취한 의무가 일반적으로 있는 것은 아니라고 판시한 바 있었다.

(3) 법원의 판단

법원은 이 판결에서 "개인 이용자들은 권한없는 제3자(unauthorized third parties)가 저작권을 위반하는 목적으로 사용하는 것을 방지하기 위해, 자신의 무선 네트워크가 적절히 보안을 유지하고 있는지 (adequately secured) 확인할 의무가 있다"고 판결했다.

그러나 독일 연방대법원은 무선 인터넷 이용자가 다른 제3자가 다운로드한 그 불법 컨텐츠 자체에 대해 책임을 지는 것은 아니라고 보았다. 또한 더 나아가 이용자가 그의 무선 네트워크의 보안을 지속적으로(constantly) 업데이트할 의무까지 지는 것은 아니라고 하여 이용자가 지는 의무를 제한했다.

즉, 이러한 독일 판례의 태도는 이용자들은 무선 인터넷 접속 최초 설정 시(first install) 암호를 설정함으로써 자신의 무선 네트워크를 어느 정도 보호하는 수준의 의무만 인정된다는 것이다.

(4) 독일 내 및 해외 여론

이 판결에 대해 독일의 국내 여론은 긍정적인 편이다. 먼저, 독일의 소비자 보호협회(The national consumer protection agency)는 이 판결에 대해 적절히 균형을 이루고 있다고 평가했다. 또한 독일의 뉴스 에이전시인 DAPD의 Carola Elberecht 대변인은 이용자가 처음 무선 네트워크를 설치

할 때 적절한 보안조치를 요구받는 대신, 그 것을 꾸준히 기술적으로 업데이트 할 것까지는 요구받지 않는 것은 상식적으로 이해된다고 밝혔다.

그러나 이러한 독일 법원의 태도에 대해 해외 여론은 부정적인 편이다.

영국의 지적재산권 법정 변호사(barrister) David Harris는 이 평결에 대해 "괴상하다(eccentric)"고 밝혔다고 한다. 그에 따르면 영국의 어떤 법 조문도 이용자로 하여금 WiFi 연결을 보안화할 의무를 지울 수 없다고 한다. 또한 다른 사람의 잘못된 무선 인터넷 이용으로 인해 책임을 지울 수도 없다고 한다.

나. Javier Perez 사건 (미국)[145]

(1) 개요

이 사안은 피고인이 운영하던 무선 네트워크에서 발송된 메시지가 유죄의 강력한 증거를 발견하는 근거로 활용되었는데, 피고인은 이에 대해 자신이 운영하는 무선 네트워크가 오픈되어 있으므로 이는 타인이 언제든지 사용할 수 있다고 항변하는 것을 법원이 부정한 사례이다.

(2) 사실 관계

사안을 보다 구체적으로 보면, 2007. 4. 한 여성에게 저급한 성적 이미지가 담긴 IM(Instant Message)가 발송되었던 것이 발단이 되었다.

이 여성이 이를 경찰에 의뢰하고, 경찰 조사 결과 이 IM은 텍사스 오스틴에 있는 Javier Perez가 운영하는 무선 네트워크를 통해 발송된 것으로 밝혀져, 그에게 수색영장이 발부되었다.

경찰 수사결과 Perez의 방에는 아동포르노가 발견되었고, Perez는 곧 아동포르노 소지 혐의로 기소되었다. 그러나 야후의 기록에 따르면,

145) Declan McCullagh, "Police blotter: Open WiFi blamed in child porn case", CNET News, 2007.4.18. http://news.cnet.com/2100-1036_3-6177095.html(2010.7.17 방문).

문제의 메시지가 발송된 야후 계정은 'Mr. Rob Ram'에 속한 것이었는데 당시 페레즈는 Robert Ramos라는 이름의 룸메이트가 있었다고 한다.

(3) 법원의 판단

항소심에서 그는 자신의 오픈된 WiFi는 누구나 접속하여 사용할 수 있으므로, 이를 통해 IM이 발송되었다는 것을 근거로 자신에게 수색영장이 발부된 것은 부적법하다고 주장했다. 따라서, 부적법한 수색영장을 근거로 수집한 아동포르노 증거는 유죄의 증거로 사용할 수 없다는 취지의 항변을 하였다.

그러나 앞서 살펴본대로, 항소심은 오픈된 무선 네트워크라 할지라도, 그 네트워크를 운영하는 페레즈에 의해 문제의 메시지가 발송되었을 가능성이 가장 높다는 이유로 이를 근거로 발부된 수색영장이 위법하다고는 볼 수 없다고 판단, Perez의 항변을 배척하였다.

다. US v. John Henry Ahmdt 사건(미국)[146]

(1) 사실관계

2007. 2. 21. 워싱턴주 알로하(Aloha)에서 피고인의 이웃에 사는 한 여성(JH)이 자택에서 개인용 컴퓨터와 자신이 소유한 무선랜 AP를 사용하여 인터넷에 접속하고 있었다.

그 여성(JH)의 무선랜 AP에 문제가 발생하여 작동하지 않게 되자 JH의 컴퓨터가 자동적으로 인근에 있던 "Belkin54G"라는 SSID를 가진 무선랜 신호를 수신하여 피고인의 무선랜 AP를 통하여 인터넷에 접속하게 되었다.

JH는 자신의 컴퓨터에서 아이튠즈 소프트웨어를 실행시켰다. 아이튠즈

146) 오레곤주 1심 2010. 1. 28. 선고(United States District Court, D. Oregon).

소프트웨어는 공유모드로 설정되는 경우 사용자가 다른 컴퓨터에 저장된 음악 파일과 사진 파일을 읽을 수 있게 되어 있다. JH가 아이튠즈 소프트웨어를 실행하였을 때 그녀는 타인의 라이브러리가 공유상태로 되어 있음을 인식하였다. JH가 그 공유된 라이브러리를 열었을 때 “Dad’s Limewire Tunes"라는 이름의 서브폴더를 발견했다.

JH가 그 서브폴더를 열어보니 “11-yr old masturbating”라는 파일과 “tiny”, “fuck”, “cunt”라는 단어와 “5yoa”나 “8yoa”와 같이 나이를 나타내는 줄임말로 이루어진 이름을 가진 30여개의 파일들을 발견했다. 그러나 JH는 아동포르노와 관련이 있는 그러한 파일들을 열어보지는 않았다.

JH는 와싱턴 카운티 경찰서에 신고하였고 경찰관인 맥컬러우는 2007. 2. 21. 오전 11시 30분 경 출동하여 JH가 문제의 서브폴더에 접근하였던 방법을 사용하여 재현하였다. 맥컬러우는 JH에게 그 파일 중 한 파일을 열어보라고 시켰고 두 사람은 미성년자의 성행위가 담겨진 사진을 목격하였다.

2007. 2. 23. 워싱턴 카운티 경찰서 형사인 레이 마르컴과 제임스 콜이 이 사건에 대하여 JH를 인터뷰하였다. JH는 가끔 무선랜 인터넷 연결에 장애가 있었고 인식하지 못하는 사이에 Belkin54G 무선랜 AP에 연결되곤 하였으며, 그녀의 집에서 다른 무선랜 신호도 잡혔지만 모두 패스워드 보안이 설정되어 있었기 때문에 JH는 다른 무선랜 AP에 접속하지 못하였다고 진술하였다.

JH는 그녀가 현재 자택으로 이사를 오던 무렵 처음으로 Belkin 54G 무선랜 AP에 접속하였으며, 당시에는 주변에 있던 이웃은 단지 두 집이었고, 그 중 한 집은 외관상 수상한 점이 많았다고 진술했다. 맥컬러우는 150피트 떨어진 그 수상한 집 앞에 세워진 자동차의 차량번호를 조회하여 피고인의 신원을 확인하였다.

2007. 4. 2. 콜 형사는 혐의자의 IP주소를 파악할 목적으로 Belkin54G 무선랜 네트워크에 접속하는 내용의 수색영장을 법원으로부터 발부받았다.

2007. 4. 7. 콜 형사는 혐의자의 집 근처에 차를 세우고 Belkin54G 무선랜 네트워크에 접속하여 IP 주소를 알아내고 관리사인 Comcast사에

조회하여 Belkin54G 무선랜 AP의 소유자가 피고인임을 알아냈다. 2007. 4. 17. 콜 형사는 아동포르노그래피 파일 수색목적의 제2의 수색영장을 발부받고, 다음날 아침 피고인의 집에서 PC, 무선 AP, 하드디스크와 CD를 압수하였다.

(2) 법적 쟁점

본 사건에서는 보안이 설정되어 있지 않은 무선랜에 연결된 개인컴퓨터에 저장된 공유모드의 아이튠즈 라이브러리의 콘텐츠가 미국 수정헌법 제4조[147] 내지 프라이버시권에 의하여 보호될 수 있는지 여부가 쟁점이 되었다.

미국 수정헌법 제4조를 원용하기 위하여는 행위자가 주관적으로 그 행위가 사생활에 관한 것("private")이라고 기대하였을 것과 행위자의 기대가 사회의 관점에서 합리적일 것의 두 가지 요건이 충족되어야 하기 때문이다.

(3) 법원의 판단

피고인측은, 2007. 2. 21. 경찰관 맥컬러우는 피고인 소유의 무선랜에 무단접속을 함으로써 피고인의 컴퓨터 파일의 프라이버시에 관한 합리적인 기대권을 침해하였고 맥컬러우의 무단접속이 ECPA법(the Electronic Communications Privacy Act)으로 금지된 행위이므로 피고인의 컴퓨터 파일의 프라이버시에 대한 기대는 합리적이라고 주장하였다.

따라서 독수독과이론에 의하여 위법한 수사에 의하여 수집된 증거는 증거능력이 없다고 항변하였다.

이에 법원은 아래와 같이 판단하였다. 서로 다른 통신하드웨어와 기술의 경우 프라이버시에 대한 기대 수준이 서로 다르다. 예컨대 유선 전화 사용자가 일반적으로 자신의 대화의 프라이버시에 대하여 합리적인 수준의 기대를 가지는 반면에 무선(cordless) 전화기 사용자는 일반적으로 그렇지

147) 미국의 수정헌법 제4조는 국민의 사생활 침해를 금지하여 부당한 수색, 체포, 압수에 의한 국민의 권리의 침해를 금지하고 있다.

않다. 왜냐하면 무선 신호를 도청하는 것이 비교적 용이하기 때문이다.

무선랜의 사용자가 가지는 프라이버시에 대한 기대수준은 무선(cordless) 전화기 사용자의 경우와 유사하다. 무선랜 신호 또한 도청하는 것이 비교적 용이하기 때문이다. 그러나 무선(cordless) 전화기 신호와 달리 무선랜 신호는 승인되지 않은 사용자(joyrider[148])가 무선랜 AP 소유자의 비밀정보에 접근하지 않고 단지 인터넷 접속으로만 사용할 수 있다. 대부분의 조이라이더들은 보안설정이 되어 있지 않은 무선랜에 접속하는 것이 합법이라고 믿고 있고 인구밀도가 높은 도시환경에서는 우연히 타인의 무선랜에 무단 접속하는 일은 상당히 흔히 일어나고 있다. 뿐만 아니라 의도적인 무단접속도 널리 퍼진 관행으로 볼 수 있다.

피고인은 Belkin54G 무선랜 AP를 사용하면서 패스워드 보안을 설정하지 않아 그 무선랜은 누구든지 근거리에서 접속할 수 있는 상태에 있었다.

JH는 그 Belkin54G 무선랜에 수차례 접속하였다. Belkin54G 무선랜 AP는 패스워드 보안을 설정하지 않는 것이 디폴트 설정으로 되어 있으나 패스워드를 설정할 수 있고, 그에 대한 상세한 설명이 매뉴얼로 제공되었다.

타인의 무선랜을 사용하는 것의 용이성과 그 높은 빈도를 고려하면, 유선 네트워크나 패스워드 보안이 설정된 무선랜과 비교하여 패스워드 보안이 설정되지 않은 무선랜에 대한 사회 내지 일반인이 가지는 프라이버시에 대한 기대수준은 낮다고 볼 수 밖에 없다.

아이튠즈 라이브러리를 타인도 볼 수 있도록 공유모드로 설정할 것인지는 사용자가 선택할 수 있다. 그렇다면 보안이 설정되어 있지 않은 무선랜 상에서 아이튠즈 라이브러리를 공유하는 행위에 대하여는 사회 내지 일반인이 가지는 프라이버시에 대한 합리적인 기대는 없다고 보아야 한다.

ECPA법은 무선랜과 아이튠즈 소프트웨어가 일반인이 접근할 수 있도록 설정되어 있는 경우에는 그 접근은 위법하지 않다고 규정하고 있다[149].

---

148) A “joyrider” is someone who “use[s] an openWiFiconnectiontoaccesstheInternet.” BenjaminKern,Whacking, Joyriding, and War-Driving: Roaming Use of WiFi and the Law, 21 Santa Clara Computer & High Tech. L.J. 101, 138 (2004)

결국 피고인은 프라이버시에 대한 합리적인 기대를 입증하지 못하였으므로 수정헌법 제4조 내지 프라이버시권을 주장할 수 없다.

라. Partners Coffee v. Oceana[150] (미국)

(1) 사실 관계

원고 파트너스와 피고 오세아나는 커피의 로스팅, 생산과 커피 및 관련 제품의 판매를 영업으로 하고 있다. 2008년 파트너스는 오세아나의 1인주주인 길슨과 오세아나의 자산 전부에 대한 讓受渡계약을 체결하였다.

자산양수도 계약과 관련하여 길슨은 회사를 대표하여 회사의 재정상태, 계좌의 상태, 장비의 상태에 대한 진술보증(representations and warranties)을 제공하였다.

2008. 5. 2. 파트너스와 오세아나는 자산양수도 계약을 체결하였고, 동시에 길슨이 컨설팅과 자문 서비스를 초기 3년간 제공하고 파트너스는 매월 보수와 고객유지성과와 수익에 따른 성과급 보너스를 지급하는 것을 내용으로 하는 별도의 컨설팅 계약을 체결하였다.

원고의 진술에 의하면, 파트너스가 오세아나의 영업을 이어받은지 얼마 후 파트너스는 자산양도계약상 진술보증의 다수의 내용이 사실과 다름을 발견하게 되었다. 예컨대 길슨이 제공한 오세아나의 재무보고서가 위조되었고 커피 로스팅 장비의 상태에 대한 보고 내용이 허위였으며 일부 회사채권자의 존재를 開示(disclosure)하지 않았다.

나아가 파트너스는 오세아나가 컨설팅 계약을 위반하고 있다고 주장했다.

---

149) "[i]t shall not be unlawful under this chapter or chapter 121 of this title for any person ... to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public." 18 U.S.C. § 2511(g)(i)

150) PARTNERS COFFEE COMPANY, LLC, Plaintiff, v. OCEANA SERVICES AND PRODUCTS COMPANY and James S. Gilson, Defendants. U.S. Distric Court(1심) 펜실베니아주, 2009. 12. 4. 선고

특히 길슨과 오세아나는 컨설팅 계약의 2년의 존속기간 동안 競業을 금지한다는 합의를 위반했다고 보았다. 파트너스는 또한 길슨이 몰래 파트너스의 컴퓨터에 무선랜 AP를 설치하고 이를 이용하여 파트너스의 컴퓨터 시스템에 로그인하여 영업비밀과 영업에 관한 기록을 편취하였다고 원고는 주장했다.

(2) 법적 쟁점

이 사건의 쟁점은 길슨이 파트너스의 컴퓨터에 몰래 무선랜 AP를 설치하고 이를 이용하여 영업비밀을 외부의 컴퓨터로 전송한 행위가 불법행위에 해당하는지 여부와 함께, 길슨이 파트너스의 컴퓨터에 몰래 무선랜 AP를 설치한 행위 자체가 불법행위에 해당하는지 여부가 되었다.

(3) 법원의 판단

법원은 이에 대해 아래와 같이 판단하였다. 길슨이 파트너스의 컴퓨터에 몰래 무선랜 AP를 설치하고 이를 이용하여 영업비밀을 외부의 컴퓨터로 전송한 행위는 그 소유자의 동의 없이 정보를 취하거나 사용하거나 개시하는 행위(“possessed, used, or disclosed")에 해당한다. 따라서 이러한 행위를 한 피고인은 ‘부정한 정보의 취득(improper procurement of information)’으로 인한 불법행위책임[151]을 진다.

길슨이 파트너스의 컴퓨터에 몰래 무선랜 AP를 설치한 행위 자체는 "타인이 점유하는 동산에의 간섭(intermeddling with chattel in the possession of another)"에 해당한다. 그러한 행위는 그렇게 취득한 정보를 부정한 목적으로 사용하는지 여부와는 별개의 문제이다. 따라서 피

151) Under Section 759 of the Restatement of Torts, “One who, for the purposes of advancing a rival business interest, procures by improper means information about another’s business is liable to the other for the harm caused by his possession, disclosure, or use of the information.”

고인이 그렇게 취득한 정보를 파트너스와 競業 목적으로 사용하지 않았다 하더라도, 나아가 무선랜을 통하여 비밀정보를 아예 취득하지 않았더라 하더라도 '동산 침해'[152]의 책임이 성립함에는 아무 영향이 없다.

마. Cobell v. Kempthorne (미국)[153]

(1) 사실 관계

인디언 신탁(Indian Trust)의 수익자들이, 내무부가 보관하고 있는 인디언 신탁 관련 정보(Individual Indian Trust Data)를 보호하기 위한 컴퓨터 보안 수준이 충분하지 않음을 이유로 미국 내무부(Department of Interior)를 상대로 집단소송을 제기하였다.

신탁수익자(원고)들은 소송전 보전조치로서 인디언 신탁에 관련된 정보를 저장하거나 그 정보에 접속할 수 있는 모든 정보기기와 시스템을 인터넷과 내부전산망으로부터 분리할(disconnect) 것을 내용으로 하는 가처분신청을 하였다.

내무부 감사기관 소속의 NISO(the National Information System Office)가 IT 보안테스트를 담당하였다. 2003. 10. 과 2004. 4. 사이에 NISO가 실시한 내무부내에 설치된 무선랜 네트워크의 보안심사 결과는 다음과 같은 문제점을 지적하였다.

과거 4년 간 내무부에서는 기존의 유선네트워크에 다수의 무선랜 AP를 설치하였으나 사실상 무선랜에 대한 보안정책이나 절차가 전혀 없었다.

내무부 직원들은 파이어월(firewall), 암호화 등의 무선랜 보안 설정에 익숙지 않았고, 외부인도 보안 통제를 받지 않고 무선랜을 통하여 유선네트워크에 접속할 수 있는 위험에 놓였다. 대부분의 내무부 무선랜은

---

152) Pennsylvania law defines "trespass to chattels" as the act of intentionally "(a) dispossessing another of their chattel, or (b) using or intermeddling with chattel in the possession of another."

153) U.S. Distric Court(1심) 워싱턴 DC, 2005. 10. 20. 결정, U.S. Court of Appeals(2심) 워싱턴 DC, 2006. 7. 11. 결정.

WEP 암호화방식이 설정되어 있었으나, 관련 업계에서 WEP 방식은 정보보호에 충분한 보안조치로서 인정받지 못하고 있다. 특정 부서에 설치된 무선랜 AP의 경우에는 리셋버튼을 누르면 패스워드나 암호화가 없는 무보안 상태로 돌아가도록(default setting) 되어 있었다. 외부인이 리셋버튼을 누르면 쉽게 무선랜에 접속할 수 있는 위험이 존재하였다.

NISO는 무선랜 감지기를 사용한 테스트(wardriving)에서 700여개의 무선랜과 무선랜 신호를 전송하는 노트북 컴퓨터를 식별할 수 있었다. 그 중에는 외부 용역업체 직원들(contractors)들이 사용하는 기기들이 상당수 있었다, NISO는 이러한 외부인들이 무선랜 노트북을 이용하여 내무부 유선네트워크에 접속할 위험이 존재한다고 경고했다. 무선랜 신호의 전송거리가 통제되지 않고 있어서 내무부 건물에서 떨어진 곳에서 무단접속할 위험도 있었다.

NISO는 무선랜 SSID의 식별하지 못하게 할 것, 무선랜 무단접속을 금지할 것, 무선랜을 통한 침입으로부터 유선네트워크를 보호할 것의 강화된 보안 조치를 취할 것을 권고했다. NISO의 평가와 제3의 보안 전문가의 평가에 의하면 현재 내무부의 IT 보안 점수는 최저등급("F")에 해당한다고 한다.

(2) 법원의 판단

1심 법원은 증거자료에 비추어 보건대 그러한 낮은 등급이 정당하다고 판단하고, 원고의 가처분신청을 인용하였다.

이에 반해 2심 법원은 IT 네크워크 특히 무선랜의 보안을 완벽하게 구축하는 것은 불가능하다는 것이 관련 업계의 일반적인 견해라는 점에 주목했다. 이렇게 IT 보안이 내재적으로 불완전하다는 점을 고려하건대 내무부에 대한 보안상의 급박한 위협이 존재하거나 내무부가 공격의 대상이 될 것으로 믿을 만한 합리적인 이유가 있는 경우에 한하여 가처분명령을 내릴 수 있다고 2심 법원은 보았다.

즉, 2심 법원은 가처분 대상으로 특정된 컴퓨터들을 전산망으로부터

분리하게 되면 내무부의 다수의 기능이 마비될 것이라고 보았다. 가처분 명령에 따라 일단 컴퓨터들을 분리한 후 내무부가 전산망 접속 없이 업무를 수행하면서 IT 보안 개선책을 찾는 것이 IT 보안을 개선하면서 동시에 정상 업무를 계속 수행케 하는 것보다 더욱 공익에 부합한다고 볼 수 없다. 따라서 1심법원의 가처분명령은 위법하다는 판결을 내렸다.

바. 시사점

조사 결과, 독일을 제외하고 다른 국가에서 사설 AP를 보유하는 개인에 대해 접속인증 조치를 취하도록 법적인 의무를 인정한 사례는 거의 찾아보기 어려웠다.

이는 영국, 미국 등 독일을 제외한 주요 국가들이 오픈 WiFi 운영자의 책임을 다루는데 있어서, 소유권행사의 공공복리적합이라는 가치보다는 사적 자치의 원칙을 보다 중요하게 보았다고도 해석할 수 있다. 또한 이는 각국의 적극적인 무선랜 보급 및 활성화 추진 정책과도 무관하지 않을 것이다.

또한 독일 역시 사설 AP 보유자의 기술적인 보안 업데이트 의무나, WiFi 망에서 일어난 위법행위에 대한 책임에 대해서는 명백히 부정함으로써, 오픈 WiFi 운영자의 책임을 어느 정도 제한하고자 했다는 점에 대해서도 주목할 필요가 있다.

제 2 절 무선랜 취약성 보고 사례

1. 해외 무선랜 취약성 보고 사례

가. 소셜 네트워크에 대한 취약성 보고 사례 (미국)

간단한 트릭을 사용해 WiFi 관리자의 WPA 암호를 무력화 시킬 수 있다는 점에서 특히 최근 급격히 인기를 끌고 있는 페이스북, 트위터 등 소셜 네트워크 서비스의 취약성에 대한 우려가 보고되고 있다[154].

지난 2010년 7월, 소셜 네트워크 서비스인 페이스북의 보안관련 팀에 근무하는 Pedram Keyani씨는 자기 동료의 무선 네트워크의 WPA 암호를 알아낸 뒤, 이에 접속하여 그 동료의 인터넷 사용 내역 및 암호 등을 알아내는 것에 성공하였다고 전해졌다.

Keyani에 의하면 이 시도는 트위터에 비해 페이스북이 보안관련 우월하다는 점을 증명하기 위한 것이었다. 즉, 무선랜을 통한 접속 방법으로 동료의 페이스북 계정에 접근할 수는 있었으나, 페이스북의 관리 및 회사 시스템에 접근할 수는 없었다고 한다. 그러나 이 보고로 인해 무선랜 보안의 취약성을 악용한 트위터, 페이스북 등 소셜 네트워크 서비스 해킹 우려는 더욱 높아졌다[155].

나. 가정용 무선공유기

미국의 한 보안 전문가가 Linksys 공유기 등으로 실험해 본 결과 UPnP를 통해 해커가 주요 DNS 서버에 접근하여, 해당 공유기를 좀비로 바꿀 수 있다고 보고되었다.[156] 특히, 미국의 경우 90% 이상의 가정용 무선 공유기 등이 UPnP를 지원하고 있어 침해가 우려된다고 한다.[157]

한편 중국에서는 WiFi의 인증시스템의 약점을 공격, 암호를 깰 수 있

154) 무선 네트워크의 WPA 암호를 쉽게 알아내는 방법에 대해 공유하는 한 토론방 사이트도 존재하고 있다. http://webcache.googleusercontent.com/search?q=cache:VArK7JzNMyUJ:www.hackforums.net/archive/index.php/thread-321253.html+hack+wpa+via+fake+ssid&cd=2&hl=en&ct=clnk&gl=us&client=safari 참조(2010. 7. 17 방문).

155) Michael Arrington, "Employees challenged to crack facebook security, succeed", Techcrunch, 2010. 7. 5. see http://techcrunch.com/2010/07/05/employees-challenged-to-crack-facebook-security-succeed/(2010. 7. 17 방문).

156) 이에 관련한 자료는 see http://www.zdnet.com/blog/soho-networking/WiFi-routers-vulnerable-to-upnp-attack-from-hackers/120(2010. 7. 17 방문).

157) UPnP는 네트워크 세팅이나 커뮤니케이션을 위한 포트를 자동으로 공개하는 등 자동으로 관리기능을 수행하는데 필요한 프로토콜.

는 kit이 USB 형태로 판매되고 있다고 한다.

다. 공항 등에 설치된 Hotspot

Authentium의 조사에 따르면, 시카고 오헤어 공항에 설치된 76개 핫스팟 중에서 3개는 허위 주소나 조작된 주소로 해커로 추정되었다고 한다.

라. 스마트폰

(1) Apple iPhone

아이폰에 침투하기 위해 제작된 단순한 수준의 멀웨어(malware)가 보고된 바 있으나, 아직까지 국내에서 심각한 침해사례가 보고된 바는 없다.[158]

아이폰에 전파되고 있는 것으로 의심되는 바이러스 중에는 아이폰이 스스로 전화부내의 다른 사람에게 전화를 걸게 만드는 증세를 일으키는 것도 있다.[159] 참고로 국내에서도 발견된 '트레드 다이얼(TredDial)'이라는 악성코드는 윈도우 모바일 기반 스마트폰을 전염시켜, 50초마다 한번씩 국제 전화번호로 전화를 걸어 이용자로 하여금 국제전화 요금을 물게하는 것으로 알려졌다.[160]

Smobile systems의 리포트에 따르면 아이폰 이용자가 암호화되어

158) Sophos, Security threat report:, 2009.11.

159) 아이폰이 자동으로 전화를 건다는 불만에 대해서는 다음 아이폰 관련 포럼에서 발견할 수 있음. http://forums.macrumors.com/showthread.php?t=845237 ; http://discussions.apple.com/message.jspa?messageID=9973308 ; http://www.barcampabidjan.info/virus-makes-call-by-itself-on-cellphones-a-new-wave-of-attacks-to-come.html(2010. 7. 17 방문)에서는 이러한 증상이 바이러스로 인한 것이라고 주장.

160) 감염된 스마트폰은 국제전화 발신 제한이 설정돼 있거나, 번호가 존재하지 않아 실제로 요금이 청구되지는 않았다. 바이러스는 모바일 3D게임과 함께 배포되었다. http://www.ohmynews.com/NWS_Web/view/at_pg.aspx?CNTN_CD=A0001372247&PAGE_CD(2010. 7. 17 방문).

있지 않은 핫스팟에 접속하는 경우 이용자가 접속한 사이트의 암호 및 패스워드를 기존에 알려진 방법으로 쉽게 해킹할 수 있다고 한다[161].

아이폰의 취약성에 대해 가장 널리 알려진 사례는 2009년 말 호주에서 발생한 Ikee worm이다. 이 웜은 아이폰의 배경화면이나 기능에 일부 영향을 주는 것이었는데, 이는 아이폰을 이용하는 사람들에게 그 보안의 취약성에 대해 경고를 줄 목적으로 제작되었다고 한다.

아이폰의 보안 취약을 노려 수익을 얻을 것을 목적으로 한 웜이 최초로 보고된 것은 네덜란드였다. 네덜란드의 한 해커가 모바일 봇넷을 제작해 온라인 뱅킹관련 정보를 얻는 웜을 배포했는데, 이는 네덜란드 은행을 아이폰으로 접속하는 고객들로 하여금 피싱 사이트로 유도하는 형식으로 이뤄졌으나 특별한 피해가 보고되지는 않았다.

이 아이폰용 웜바이러스는 사용자 해킹 시 설치되는 무선 원격 통신 프로토콜인 SSH(Secure Shell)가 대부분 기본 패스워드를 사용하고 있는 것을 악용해 전파되고 있었다. 특히 같은 무선 네트워크 AP를 사용하고 있는 다른 아이폰들을 검색해 감염시키는 기능도 갖추고 있으며, 웜 바이러스의 소스코드도 공개된 상태라 언제든지 악질적인 변종이 등장할 수 있는 것으로 알려진 바 있다.[162] 1차 공격대상은 이른바 무료 애플리케이션을 즐기기위해 보안장치를 임의로 해제한 유저들이었다고 한다.[163]

(2) Google Android

구글의 안드로이드의 경우 어플리케이션에 보다 개방된 태도를 취하고 있어, 현재까지 심각한 피해사례가 보고된 것은 없으나 아이폰의 경우보다 malware 등에 더 취약할 것으로 예상되고 있다.

---

161) http://threatcenter.smobilesystems.com/wp-content/uploads/2009/11/MIMT-Whitepaper031.pdf 참조(2010. 7. 17 방문).
162) http://www.betanews.net/article/478293(2010. 7. 17 방문).
163) http://www.itdaily.kr/news/articleView.html?idxno=21037(2010. 7. 17 방문).

2010년 3월에는 구글의 안드로이드를 탑재한 보다폰의 HTC 매직이 여러 종류의 멀웨어에 감염되었다고 스페인 보안업체 팬더 시큐리티(Panda Security)가 밝혔다. 이에 따르면 안드로이드 OS가 탑재된 모바일을 USB를 이용해 컴퓨터에 연결시키면 해당 바이러스가 그 컴퓨터가 전염시킨다고 한다.[164]

또한 미국 '퍼스트테크 크레딧 유니온(First Tech Credit Union)'에 따르면 2009년 12월말 안드로이드 마켓에서 'Droid09'라는 아이디를 가진 판매자가 사용자의 계좌 비밀번호를 가로채는 악성 모바일뱅킹 애플리케이션을 판매해온 사실도 발견됐다고 한다.[165]

2010년 6월 모바일 보안업체인 에스모바일시스템즈(SMobile Systems)가 발표한 안드로이드 앱의 보안 위협에 대한 보고서에 따르면, 현재 안드로이드 마켓에 등록된 앱들 중 20%가 사용자의 개인정보와 같은 민감한 정보를 사용하는 것으로 나타났다고 한다. 따라서 향후 마켓이 활성화 될 경우 이가 악용되어 범죄로 사용될 위험이 있다고 보고했다.[166]

2. 국내 무선랜 취약성 보고 사례

가. 침해 사례

2008년 5월 은행의 무선 인터넷 공유기를 해킹해 관리자 아이디와 패스워드를 탈취하려던 피의자들이 경찰에 붙잡힌 사례가 있었다[167]. 그러나 이는 미수에 그친 사안이며, 이 후 현재[168]까지 특별히 국내에서 무선 랜 침해 사례가 보고된 바는 없다.

---

164) http://news.cnet.com/8301-27080_3-10466230-245.html(2010. 7. 17 방문).
165) http://www.boannews.com/media/view.asp?idx=18722&kind=1(2010. 7. 17 방문).
166) 에스모바일시스템즈가 수행한 안드로이드 앱에 대한 보안분석 보고서 전문은 http://threatcenter.smobilesystems.com/wp-content/uploads/2010/06/Android-Market-Threat-Analysis-6-22-10-v1.pdf 참조(2010. 7. 17 방문).
167) http://news.naver.com/main/read.nhn?mode=LPOD&mid=tvh&oid=057&aid=0000079426 (2010. 7. 17 방문).
168) 2010년 7월 현재.

나. 취약성 보고 사례

2007년 국내 유명백화점을 대상으로 진행했던 무선해킹테스트에서 무선암호화의 취약성으로 인해 데이터가 쉽게 해킹할 수 있다는 사례가 발표돼 화제가 된바 있다[169]. 또한, 2009년도 국정감사에서 국회 문광위 소속 허원제 의원이 '카인과 아벨'이라는 해킹 프로그램을 이용해 무선 인터넷 해킹이 가능하다는 점을 지적한 바 있다[170].

최근에는 지하철이나 버스 같은 대중교통 그리고 거리나 공공장소에서 간헐적으로 나타나는 무선랜 중에는 해킹을 위한 바이럴 SSID(무선인터넷 식별신호) 형태의 에드혹(Ad-hoc) 네트워크가 존재할 가능성이 있다는 주장도 제기되고 있다. 특히 HP의 프린터의 에드혹 신호인 'hpsetup'가 자주 뜨고 있는 것에 대해 해킹을 위해 설치된 것 아니냐는 우려의 목소리가 제기되고 있다. HP측은 이에 대해 프린터가 거리나 지하철 등 외부에서 사용될 확률은 극히 낮으므로 HP 프린터 에드혹을 가장한 제3자의 네트워크일 가능성이 높다고 공식적으로 밝힌바 있다[171].

169) 오병민, "위협적인 무선인터넷 해킹 '무방비 시대'", 보안뉴스, 2009. 11. 26., see http://www.boannews.com/media/view.asp?idx=18717&kind=1(2010. 7. 17 방문).
170) 오병민, "무선 인터넷, 간단히 해킹과 전화도청 가능해". 보안뉴스, 2009. 10. 7., see http://www.boannews.com/media/view.asp?idx=18055&kind=1(2010. 7. 17 방문).
171) 오병민, "지하철 출몰 공짜 무선랜...정체는 무선 해킹?". 보안뉴스, 2010년 5월 6일. http://www.boannews.com/media/view.asp?idx=20827&kind=1(2010. 7. 17 방문).

제 5 장 무선랜 보안 정책 방향

제 1 절 서론

1. 무선랜 활용의 장애요인 분석

무선 인터넷접속을 가능하게 하는 이른바 무선랜, 즉 WiFi가 우리나라에 도입된 지는 2000년 이후 부터이므로 10년 정도 되었지만, 그리 활성화 되어 있지 않았다. 그러다가 2009년 겨울 스마트폰이 우리나라에 도입되면서 무선랜에 대한 사회적인 인식이 변화되어 주목을 끌게 되었고, 무선랜의 수요와 공급이 급격하게 확산되었다. 이와 같은 급격한 변화를 가져오기 까지 우리나라에서 무선랜에 대한 인식이 극히 저조한 이유는 다음과 같은 점에서 분석해 볼 수 있을 것이다.

가. 수요측면의 장애요인

첫째로 무선랜에 접속하여 인터넷에 접속할 디바이스가 제대로 보급되지 않았다는 점을 들 수 있다. 노트북을 제외하고 무선랜에 접속할 수 있는 디지털 디바이스라고는 거의 미미한 수준으로 보급되어 있는 스마트폰과 PSP와 같은 휴대용 게임기나 이미 사양길에 접어든 PDA 정도가 전부였다. 또 스마트폰을 이용해서 WiFi에 접속하기 위한 설정은 기술에 대한 이해도가 낮은 일반인으로서는 매우 어려운 것이었고, 스마트폰 자체도 간편하게 무선랜에 접속할 수 있도록 하드웨어나 소프트웨어가 설계되어 있지 아니하였다. 또 노트북은 그 부피의 제약으로 인해 일상적으로 휴대하는 것이 불가능하였고, 학교, 회의장, 소수의 시설에서 특정한 용도로 제한적으로 무선랜을 사용할 뿐이었으므로 사회전반에 걸친 주목의 대상이 되지 못하였다. 이는 무선랜의 수요측면의 장애요인

이라고 할 수 있다.

나. 공급측면의 장애요인

둘째로 무선랜을 제공하는 AP의 보급이 충분하지 않았다는 점이다. 우리나라 인터넷접속의 대부분을 차지하는 가정내 초고속통신망에 개인이 공유기를 설치하는 경우는 매우 빈번하지만, 가정 내에서 굳이 무선으로 인터넷접속을 할 필요성을 느끼지 않았으므로 초기에 유선공유기의 보급은 매우 활발한 반면 무선공유기의 보급은 충분하지 아니하였다.

또 개방된 장소에서의 Hot-spot 역시 수도권을 중심으로 한 인구밀집 지역에 국한된 것이었을 뿐, 전국적인 범위를 커버하는 수준에 이르지 못하고 있었다. 이는 무선랜의 공급측면의 장애요인이라고 할 수 있다.

다. 정책측면의 장애요인

셋째로 정책적으로 휴대전화에서 무선 인터넷 접속을 하기 위한 방법으로 WiFi를 통한 접속이 아니라 기간통신사업자가 제공하는 WIPI 플랫폼을 이용한 접속을 유도하여 왔다. 그 대표적인 정책이 모든 휴대전화에 WIPI탑재를 의무화하는 것이었다.[172] 그러나 WIPI는 접속비용이 매우 높은 수준이었으므로, 휴대전화를 구입하자마자 오히려 WIPI에 접속하는 기능을 봉쇄하기에 급급한 정도로 오히려 무선인터넷 접속에 대한 공포심을 사회적으로 확산시키는 결과를 낳게 되었다. 이는 무선랜의 정책측면의 장애요인이라고 할 수 있다.

라. 무선랜에 대한 인식 변화

172) 2005년 4월 1일, 당시 정보통신부는 "전기통신설비 상호접속기준"을 개정하여 대한민국에서 판매되는 이동 통신 휴대 단말에는 WIPI 플랫폼이 의무적으로 탑재되도록 결정하였다.

이와 같은 다방면의 활성화 장애요인으로 인해 사회적으로 주목받지 못하고 있던 무선랜에 대한 인식이 변화되게 된 계기는 매우 우연한 것이었다. 세계적으로 높은 상품성을 인정받은 스마트폰을 우리나라에 도입하기 위해서 가장 중요한 선결문제는 당시로서는 의무화사항이었던 WIPI의 포함 여부에 관한 논란이었다. WIPI 포함을 거부하는 애플사로 인해 논란이 확산되던 중 결국 2008년 12월 방송통신위원회가 국내 유통되는 휴대전화의 WIPI지원 의무화규정을 폐지할 것을 발표하여, 2009년 4월 1일 이후 발매되는 휴대전화는 WIPI운영체제를 지원하지 않아도 무방하게 되었다.[173] 이로써 특정 스마트폰이 우리나라에 도입될 수 있는 선결문제가 해결되어 2009년 11월말 공식적으로 발매된 이후 빠른 속도로 판매량이 증가하였다.

스마트폰은 무선랜 신호를 검색하여 매우 간편하게 자동으로 접속상태를 유지하는 장점을 갖고 있어서 무선랜을 이용할 수 있는 일상 휴대용 디바이스의 보급이 이루어지게 되었다. 또 스마트폰의 장점인 어플리케이션의 설치와 실행을 위해서는 무선 인터넷 접속이 요구되는데, 유상의 3G네트워크를 통한 접속보다는 무료의 WiFi 무선랜을 통한 접속에 대한 사회적 관심이 높아지게 되었고, 이에 부응하여 Hot-spot의 무상접속과 같은 영업전략[174]이 시행됨으로써 무선랜의 사회적 수요와 공급이 급속히 팽창하게 되었다.

무선랜에 대한 사회적 인식의 변화의 배경에는 이러한 스마트폰과 같은 무선랜을 수요로 하는 디바이스의 보급 뿐만 아니라 유선 초고속 인터넷 네트워크가 이미 잘 구축되어져 있다는 점도 자리잡고 있다. 무선랜은 WiFi단말기와 AP구간이 무선으로 구축되는 것이고 AP이후의 노드는 유선으로 구성되는 것이 일반적이므로, 유선 초고속 인터넷 네트워크가 완비되어 있지 아니하면 무선랜의 공급은 현실적으로 크게 제약을 받게 된다. 거의 모든 가정과 사무실에 초고속 인터넷이 보급되어 있는 상

173) http://blog.naver.com/btaiji?Redirect=Log&logNo=150040880250(2010. 6. 10 방문)
174) iPhone에 한하여 KT가 운영하는 Netspot에 Mac인증을 통해 무상으로 접속이 가능하다.

태에서는 무선랜의 공급은 불과 3-4만원에도 구입이 가능한 AP를 연결하는 것으로 개인적인 차원에서도 충분히 가능하게 되었으므로 무선랜의 사회적 인식의 변화가 매우 신속하게 이루어질 수 있었다.

무선랜에 대한 사회적 관심의 증가는 초고속 통신망 사업을 통해 정액제로 무제한 유선 인터넷접속이 가능하게 함으로써 전 국민이 인터넷을 일상적으로 사용할 수 있는 환경을 조성했던 것처럼, 무료 또는 낮은 비용으로 무선 인터넷 접속을 가능케 하는 IT환경을 조성하는 중요한 계기가 될 것이다. 이로서 무선인터넷 활용에 한해서는 선도적인 지위를 확보하지 못했던 우리나라의 사회적 기반에 일대 변혁이 이루어지게 되었다.

2. 무선랜 보안의 필요성

가. ISM대역의 특성

무선랜은 비면허의 ISM대역을 이용하여 무선으로 인터넷에 접속하기 위한 설비이므로 기간통신사업자들이 제공하는 3G네트워크를 통한 인터넷접속 보다는 보안에 취약할 수 밖에 없는 생래적 한계를 가질 수 밖에 없다. 무선 인터넷 접속에서 중요한 보안요소는 크게 '접속인증'과 '데이터암호화'로 구별해 볼 수 있는데, 무선랜은 접속인증과 데이터암호화 모두 3G네트워크를 통한 접속보다는 보안에서 취약할 수 밖에 없다. 물론 무선랜에 대해서도 강력한 접속인증과 데이터암호화가 기술적으로 불가능한 것은 아니지만, 무선랜 접속을 위한 AP의 종류가 매우 다양하고 스펙트럼이 넓으므로 평균적인 관점에서는 무선랜 보안의 취약성이 무선랜 활성화의 장애요소로 작용할 우려도 존재한다.

나. 개방 형태의 접속가능

무선랜 보안의 또 다른 필요성은 상당수의 무선랜이 다양한 이유로

공개적으로 개방된 상태로 존재하고 있는 만큼, 임의의 디바이스가 접속할 가능성이 매우 높다는 점이다. 즉 아예 인증프로세스 조차 없는 사설 AP경우 불법적인 행동의 출발점이 될 가능성이 매우 높으므로 무선랜에 대한 보안통제가 제대로 되지 않는다면, 인터넷 전체 환경에서 혼란을 가져올 우려가 있다.

다. 데이터 암호화의 곤란

또한 무선랜 보안의 중요성은 데이터 암호화의 측면에서도 찾아볼 수 있다. 무선랜은 비면허대역에서 이용자의 자유로운 이용을 전제로 하는 것이므로 무선랜을 통해 주고 받는 데이터의 보안보다는 가볍고 편리한 무선통신을 주된 장점으로 하는 것이다. 따라서 적은 비용으로 간편하게 데이터를 주고 받는 것이 더 중요하지 데이터 암호화에 필요한 많은 노력을 들여서 사용하는 것은 무선랜의 취지와 잘 부합되는 것은 아니다.

물론 WEP, WPA, WPA2 등의 데이터 암호화 기술이 실용화되어 채택되어 있지만, WEP는 거의 암호화로서의 의미를 상실한 상황이고 WPA나 WPA2의 일반적인 보급은 요원한 실정이다.

그러나 무선랜의 활용이 사회전반에 걸쳐 급속히 증가하고 일반 대중들의 무선랜에 대한 수요가 폭발적으로 팽창하게 되면, 무선랜의 보안에 대한 관심과 우려도 높아질 수 밖에 없다. 그러므로 지금까지는 큰 관심이 집중되지 아니하였던 무선랜의 보안이 중요한 사회적 이슈로 대두되게 되었다. 최근 WPA방식의 데이터 암호화를 KT가 도입하여 무선랜 보안을 강화한다는 언론보도[175]는 이러한 경향을 잘 보여주고 있다.

3. 무선랜 보안과 활성화와의 상관관계

가. 보안과 활성화의 반비례

175) http://news.khan.co.kr/kh_news/khan_art_view.html?artid=201007131757035&code=930201 (2010. 7. 17 방문).

무선랜의 보안의 사회적 관심이 높아진다고 해서 무선랜의 보안수준을 높이는 것 만이 능사라고 할 수는 없다. 왜냐하면 무선랜의 보안과 무선랜의 활성화와의 관계는 매우 복잡하고 미묘하기 때문이다. 우선 접속인증을 강화하게 되면 무선랜 활성화에 부정적인 영향을 줄 가능성이 있다. 예를 들어 무선랜 보안을 위해 반드시 엄격한 인증절차를 요구하면, 무선랜에 접속할 수 있는 디바이스를 보유하고 있다고 하더라도 특별히 허가받은 경우가 아니면 일상생활에서 언제 어디서든지 원하는 대로 무선랜에 접속하는 것은 불가능하게 된다. 또 무선랜을 통해 주고 받는 데이터의 암호화를 위해서는 AP와 디바이스 모두 하드웨어적으로나 소프트웨어적으로나 복잡한 설비가 필요하므로 높은 비용과 노력이 수반되므로 활성화에 지장을 주게 될 것이다. 즉 무선랜의 보안과 활성화는 반비례관계에 있을 가능성도 있다.

나. 보안과 활성화의 정비례

반대로 보안을 강화함으로써 무선랜의 안전에 대한 신뢰가 높아져서 활성화를 도모할 가능성도 고려해 볼 수 있다. 즉 무선랜의 보안과 활성화는 정비례관계에 있을 수도 있다. 만약 무선랜의 보안이 확보되지 않아서 무선랜을 통해서 주고 받는 데이터를 가로채거나 변조가 가능하다면, 신뢰성에 대한 불안감으로 인해 무선랜을 이용하는 것을 꺼리게 될 것이다. 무선랜을 통해 주고 받는 데이터의 보안이 확보되고 그에 대한 신뢰가 사회에서 인정될 때 안심하고 자유롭게 무선랜을 이용하는 환경이 조성될 수도 있을 것이다. 따라서 무선랜의 보안과 활성화와의 이러한 미묘한 상관관계를 조화하는 무선랜 보안정책이 요구된다.

다. 서비스 내용에 따른 차별화

무선랜 보안과 활성화의 관계에서 보면, 무선랜의 활성화를 위해 요구되는 보안의 수준은 경우에 따라서 정반대일 수도 있다. 무선랜을 통해

이용하는 서비스의 종류에 따라서 무선랜 보안의 정도는 결정되어야 한다. 먼저 공개된 UCC를 감상하거나 신문이나 관광정보와 같이 일방향으로 컨텐츠를 제공받는 경우이거나 콘텐츠가 보안을 요하지 않는 경우에는 구태여 높은 보안 수준을 요구하지 않을 것이며, 보다 싸고 간편하고 신속한 접속을 선호할 것이다. 반면에 인터넷 뱅킹이나 인터넷 쇼핑, 전자정부를 위한 서비스 등의 경우에는 매우 높은 수준의 보안을 필요로 한다고 할 것이므로, 간편하고 신속한 접속보다는 번거롭더라도 안전한 접속을 오히려 선호할 것이다. 그러므로 정책적인 측면에서 엄격하게 구별할 수 있다면, 무선랜을 통해 이용하고자 하는 서비스의 종류에 따라서 그 보안의 수준을 달리하는 차별화 방안을 모색할 필요가 특히 공공부문의 무선랜에서 강조될 것이다.

4. 무선랜 공급주체의 구분

무선랜 보안정책을 수립하기 위한 구조의 큰 틀은 무선랜을 운영하는 주체가 누구인가를 구별하는 것이다. 무선랜 보안을 위해서는 무선랜 이용자들의 올바른 이용도 중요하지만, 보안이라는 것은 어차피 일탈적 행동을 자행하는 자들의 침해행위를 전제로 하여 이로부터 보호하는 것이 핵심이므로, '무선랜을 공급하는 자에게 어떠한 안전대책을 마련하도록 할 것인가'에 정책이 집중되어야 할 것이다. 특히 무선랜 보안을 위해 공급자가 어떠한 조치를 하도록 강제나 의무화 또는 유도할 것인가에 무선랜 보안정책의 내용이 형성될 것이므로, 무선랜 운영주체가 누구냐에 따라서 어떠한 형태의 정책이 수립되어야 할 것인가를 구분하여야 할 것이다.

먼저 무선랜 보안을 위해 무선랜 운영 및 공급주체가 민간인가 아니면 공공인가로 구분되어야 할 것이다. 당연히 민간이 주체가 되는 경우에는 국가의 정책은 최소한의 개입에 머물러야 하는 것이 법이론상의 원리인 동시에 규제개혁이라는 가치에도 부합하는 것이다. 반면에 공공이 주체가 되는 경우라면 특별권력관계에 따라서 심도있는 통제가 가능하게 되고,

또 공익적 관점에서 보안이 조명되어야 할 것이다.

민간이 운영 및 공급주체가 되는 무선랜의 경우에도 민간의 스펙트럼이 매우 다양하므로 보안정책은 차별화되어야 한다. 예를 들어 KT나 SKT와 같은 영리목적의 대기업인 기간통신사업자가 무선랜을 공급하는 것과 개인이 가정에 무선공유기를 임의로 부착해서 무선랜을 공급하는 것을 동일하게 다루어서 무선랜 보안정책을 적용하여서는 아니될 것이다.

무선랜 보안을 위한 정책은 전술한 바와 같이 무선랜을 운영하는 주체가 누구인가에 따라서 크게 공공 부문과 민간 부문으로 대별될 수 있다.

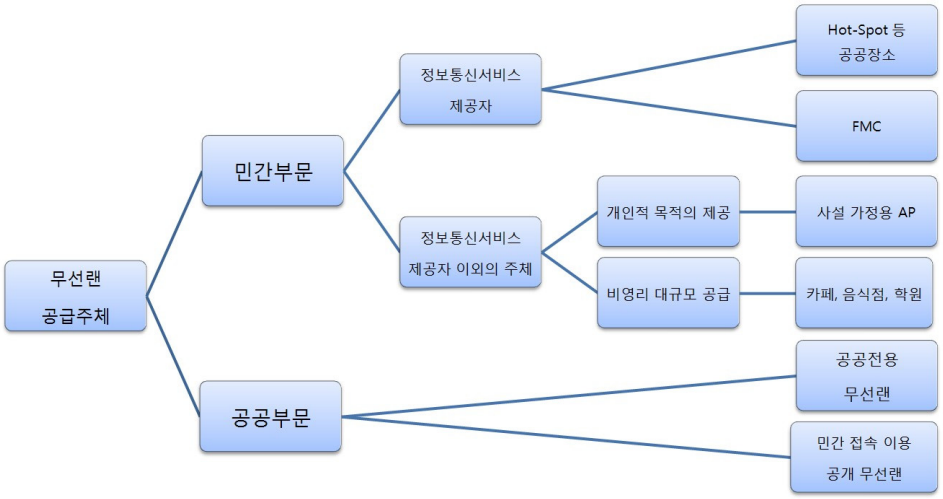
먼저 공공 부문은 공공기관이 무선랜을 공급하는 경우가 이에 해당될 것이다. 공공기관의 범위는 각 개별법령에 따라 다르지만, 국가중앙행정기관, 지방자치단체, 각급 학교, 공공기관의 운영에 관한 법률에 따른 공공기관, 특별법에 의해 설립된 특수법인과 지방공기업법에 의거 설립된 공기업 등을 망라하는 매우 다양한 주체라고 할 수 있다.[176]

이들 공공기관은 특별권력관계에 따라서 국가 정책으로 직접적인 규제가 가능하며, 그 내용 또한 공공성의 원칙에 반하지 않는다면 비교적 광범위한 가능성을 갖게 될 것이다.

민간부문은 정보통신망법에서 정보통신서비스 제공자로 개념정의되는 주체와 정보통신서비스 제공자에 포함되지 않는 주체로 구별하는 것이 실익있는 구분이다. 왜냐하면 정보통신망법은 정보통신서비스 제공자를 주로 수범자로 상정하고 규율을 하고 있으므로, 정보통신서비스 제공자에 해당되지 않는 민간 주체는 정보통신망의 이용자로서는 몰라도 제공자로서는 특별한 규율대상이 되지 못한다. 정보통신서비스 제공자는 전기통신사업자 및 영리목적의 정보제공자 및 정보제공매개자이므로 비교적 대규모의 설비를 갖춘 영리기업이 여기에 해당이 될 것이다. 이러한 기업들은 높은 수준의 보안이 유지되지 않으면 영리사업 자체의 존립이 어려우므로 자발적으로 스스로 보안조치에 최선을 다할 것이다. 그러나 대학교, 도서관, 카페와 같이 불특정 다수를 상대로 무선랜을 공급하지만 비영

176) 공공기관의 개인정보보호에 관한 법률 제2조 1호에 따른 범위를 예시하였다.

리인 주체는 보안의 필요성은 정보통신서비스 제공자와 별 차이가 없지만 그 개념에 포함되지 않는다는 점에서 보안의 취약점이 될 가능성이 높다. 따라서 정책도 이러한 주체의 구별에 따른 규율의 차이를 고려하여 마련되어야 할 것이다.



(그림 5-1) 무선랜 공급주체의 구분

제 2 절 민간 부문의 무선랜 보안 정책 방향

1. 기본원칙

가. 사적자치의 원칙

민간 부문에서 무선랜 접속을 위한 AP는 사유재산이므로 그 소유권자에게 소유권이 인정되며, AP소유자는 AP의 사용권능과 수익권능 그리고 처분권능을 보유하는 것이 원칙이다. 또 무선랜 AP 소유자는 AP가 발

생시키는 무선랜 전파에 대해서도 소유권에 준하는 권리를 갖는다고 하여야 할 것이므로 기기뿐만 아니라 특정 기기가 발생시키는 특정 신호에 대해서도 사용, 수익, 처분권능을 보유한다고 할 것이다. 근대 이래 민법의 최고원리인 사적 자치의 원칙에 따라 사적 소유권자는 자유롭게 그 소유권을 행사할 수 있으므로,[177] AP소유자가 AP를 어떻게 사용, 수익, 처분할 것인지는 자신의 자유의사에 달려있는 것이다.

나. 공공복리에 의한 제한

사적 자치의 원칙의 현대적 변용에 따라 소유권 절대의 원칙은 이미 '소유권 상대의 원칙'으로 수정되었고, 사유재산의 소유권자라 하더라도 그 소유권의 행사는 규범내재적 한계를 갖는 것으로 정리되었다. 특히 헌법 제23조 2항에서 "재산권의 행사는 공공복리에 적합하도록 하여야 한다."라고 명시함으로써 소유권의 행사도 공공복리를 침해하지 않는 한도에서만 인정될 수 있게 되었다. 따라서 AP보유자의 재산권 행사도 공공복리에 적합한 한도에서만 가능한 것이고, 공공복리에 반하는 AP에 대한 권리행사는 제한되어야 하는 것이 사적 자치의 적용범위의 한계라고 할 것이다. 따라서 AP소유자라고 해서 무한하고 무제한의 재산권 행사를 주장할 수 있는 것은 아니다. 그러므로 민간 주체의 사유재산인 AP에 대한 소유권 행사가 공공복리에 적합하지 않은 경우에 국가가 재산권행사에 대한 제한을 가할 수 있으며, 민간 부문의 AP에 대한 국가의 통제와 간섭이 넓은 의미의 공공복리에 적합한 것이라면 허용될 수 있다.

2. 접속인증

가. AP보유자에 대한 정책방향

177) 김준호, 민법강의(신정8판), 법문사, 25-26면.

(1) AP보유자의 접속인증 의무화 여부

무선랜 보안을 위한 가장 기초적인 조치는 접속을 위한 인증절차를 두어, 이로써 제3자가 임의로 자유롭게 무선랜에 접속하지 못하도록 하는 것이다. 물론 무선랜 AP보유자는 스스로 자신의 AP에 접속인증을 요구할 것인가의 판단을 자유롭게 결정하여, AP에 기술적으로 설정할 수 있다. 이와 관련하여 접속인증의 가장 뜨거운 이슈는 민간 사설 AP보유자가 자신의 AP에 패스워드 등의 접속인증절차를 반드시 설정하여 임의의 제3자가 자유롭게 무선랜에 접속하지 못하도록 하여야 할 의무를 부과하여야 할 것인가이다.

2009년 국정감사시 사설 AP에 대한 보안강화가 논란이 되면서, 사설 AP에 대해 무단 접속이 불가능하도록 접속인증을 의무화하여야 한다는 주장이 일각에서 제기된 바 있다.[178] 이에 대해 무선랜의 자유로운 접속에 대한 제한은 이용자의 부담과 이용활성화에 역행하므로 신중하게 다루어져야 한다는 반론도 제기된 바 있다.[179]

전술한 바와 같이 AP보유자에게 접속인증을 의무화할 것인가는 사적 자치의 원칙을 어느 범위까지 인정할 것인가의 정책적인 사항이고, 접속인증을 의무화해서는 아니되는 법이론적 근거는 사적 자치의 원칙의 고수로부터 도출될 수 있는 반면, 접속인증을 의무화하도록 하는 법이론적 근거는 소유권행사의 공공복리적합이라는 사적 자치의 수정원리로부터 도출될 수 있는 것이다. 즉 어떠한 정책도 법이론적 근거가 뒷받침되지 못하는 어불성설인 것은 아니다.

사설 AP보유자의 접속인증을 의무화하는 입법례는 현재 세계적으로 찾아보기 어려웠고, 또 이에 대해 참고할만한 의미있는 판례도 존재하지 아니하였다. 그러나 최근 독일 연방대법원에서 사설 AP보유자에게 접속인증조치를 의무화하는 판결(Sommer unseres Lebens Case)을 행한 바

178) http://www.zdnet.co.kr/ArticleView.asp?artice_id=20091028083013(2010. 7. 17 방문).
179) http://itnews.inews24.com/php/news_view.php?g_serial=452210&g_menu=020300 (2010. 7. 17 방문).

있다. AP보유자는 제3자가 그 무선랜에 접속하여 위법한 행위를 할 수 없도록 임의의 무단접속을 방지할 수 있는 접속인증조치를 취할 의무를 부담한다고 위 판결에서 명시적으로 밝히고 있다. 다만 이 접속인증조치를 취할 주의의무를 위반하는 바람에 제3자가 그 무선랜에 무단으로 접속하여 위법한 행위를 하더라도 그 위법한 행위에 대한 책임을 부담하는 것은 아니고, 단지 접속인증조치를 취하지 않은 그 자체에 대해서만 책임을 부담한다고 책임범위를 제한적으로 인정하고 있다.[180]

위의 독일 연방대법원의 판단이 과연 우리의 법이론에 잘 부합하는 것인가는 앞서 지적했듯이 다음과 같이 신중하게 검토되어져야 할 것으로 생각된다.

첫째로, 사적 자치의 원칙의 적용이다. 사설 AP보유자는 자신의 재산권을 모든 사람들이 널리 이용할 수 있도록 할 권리를 보유하고 있으므로, 자신의 무선AP에 누구나 접속할 수 있도록 개방된 상태를 취할 수 있는 자유를 부정하기는 어려울 것으로 생각된다.

둘째로, 공공복리에 의한 소유권 행사의 제한에 관한 법리가 사설 AP의 보안의무화에도 적용될 수 있는가의 의문이다. 생각해보건대 사설 AP보유자의 접속인증을 의무화하는 것은 사유재산제에 대한 심각한 침해가 될 가능성이 높으며, 임의의 제3자가 자유롭게 접속하여 정당하게 이용하는 한도에서 개방하겠다는 의사로 접속인증조치를 취하지 않는 것이 오히려 공공의 복리에 적합한 재산권 행사라고 이해되어야 할 것이다.

끝으로 사회부조적인 관점의 중요성이다. 소유권자가 자기의 재산을 타인이 널리 이롭게 사용할 수 있도록 허여하겠다는 의사는 사회부조적인 관점에서 인정되어야 하며, 이를 위험발생 가능성을 이유로 해서 완전히 제한하는 것은 지나친 규제가 아닐 수 없다. 다만 자신의 AP가 위법한 행위의 출발점이 되는 것을 의욕하거나 혹은 그러한 위험에 대한 구체적인 인식이 있으면서도 자신의 무선랜을 개방된 상태로 두겠다고 하

180) BGH, Urteil vom 12. Mai 2010, ZR 121/08.

는 것도 허용되어서는 곤란하다.

즉 무선랜 소유자는 자신의 AP를 타인도 정당한 방법으로 무해하게 합법적으로 사용하는 한도에서는 자유롭게 이용하도록 하겠다는 묵시적인 의사를 갖고 있는 것으로 이해되어야 할 것이다. 그리고 이러한 묵시적인 의사가 존재하는 한도에서만 무선랜을 개방하는 것이 허용되어야 할 것이고, 독일의 하급심판결과 같이 자신의 무선랜을 이용하여 타인의 권리를 침해하는 행위가 일어나는 것을 구체적으로 인식하는 특별한 경우에는 자신의 무선랜에 대해 보안조치를 취해야 할 의무가 존재하는 것으로 판단되어야 할 것이다.

따라서 사설 AP보유자에게 일률적으로 접속인증조치를 취할 의무를 법적으로 부과하는 것은 타당하지 않고, 개방된 상태로 자신의 AP를 두는 것은 AP를 타인이 부당한 방법으로 접속하거나 유해하고 위법하게 사용하는 것은 금지한다는 묵시적인 의사가 전제된 것으로 해석하는 것이 타당하다고 할 것이다.

(2) 이용자에 대한 고지의무

위와 같이 AP보유자에 대해서 접속인증을 의무화하는 것은 적절하지 않지만, 개방된 AP에 대해 접속하는 이용자에 대해 보안의 중요성과 위험성을 고지하는 것은 무선랜 보안을 위해서 필요할 것이라 생각된다. 다만 이러한 이용자에 대한 고지는 사적인 용도로 사용하기 위해서 사설 AP를 설치한 개인에게 까지 부과할 것은 아니고, 카페나 레스토랑 등처럼 고객과 같은 불특정 다수가 수시로 접속할 가능성이 높은 AP보유자에 대해서 인정되어야 할 것이라고 생각된다.

특히 이러한 AP보유자는 AP를 통한 무선랜 접속제공 그 자체를 영리로 하는 것은 아닐지라도, 영업상의 목적으로 운영하는 것이므로 사적인 목적으로 AP를 설치한 개인과는 차별화되어야 할 필요가 있다. 또 정보통신서비스 제공자는 정보통신망법상의 규정을 통해 어느 정도 보안조치를 취할 의무를 직접 부과할 수 있으나, 이러한 주체들은 정보통신서비

스 제공자에 해당되지 않으므로 무선랜 보안의 사각지대에 놓여있다고 볼 수 있다. 따라서 이러한 이용자에 대한 고지의무를 부과하는 것은 적절할 것이며, 이를 위해서는 후술하는 바와 같이 ISP와의 ISP계약관계를 통해 계약상의 의무로 부과하는 것이 바람직할 것이라 생각한다.

(3) AP의 무단 설치의 규율

사설 무선랜 AP의 대부분은 기간통신사업자가 각 가정에 유선으로 공급하는 초고속통신망의 단말에 임의로 무선AP를 설치하는 경우에 해당될 것이다. 이 경우 개방된 상태의 무선랜 공유기를 설치하는 것이 ISP계약의 위반으로 다루어져야 하는 것은 아닌가 하는 법적 문제가 발생한다.

만약 ISP계약의 약관에서 무선랜 공유기를 설치하는 것을 금지하는 내용이 포함되어 있다면 법리상으로 계약위반(채무불이행)이 되는 것은 자명하다. 그러나 현실적으로 이미 무단으로 무선랜 공유기를 설치하는 것이 보편화되어 있고, 기간통신사업자들도 그 사실을 알면서도 묵과하는 것이 일반적인 거래현실이므로 이제 와서 무선랜 공유기를 설치하였다는 사실만으로 채무불이행 책임을 묻는 것은 실효의 원칙[181]을 적용하여 신의칙에 반하는 것이라고 해석될 여지도 없는 것은 아니다.

기간통신사업자와 개인 간의 ISP계약의 거래 현실에서는 일반적으로 ISP가 2개 회선까지의 단말설치는 허용하고 있으므로, 그 한도 내에서의 AP의 설치는 이용자의 자유이다. 만약 3개 이상 회선의 단말을 설치하면 별도의 과금이 이루어지게 되고 추가로 단말을 설치하는 경우도 추가 3대(총4대의 단말)까지만 가능하며[182] 이를 위반하는 경우에는 ISP계약을

181) 실효의 원칙이란 신의성실의 원칙의 파생원칙 중 하나로서, 일정한 기간동안 권리가 행사되지 않아서 의무자에게 권리자가 그 권리를 더 이상 행사하지 않을 것이라는 정당한 기대를 갖게된 경우에 권리자가 그 권리를 새삼 행사하는 것은 신의칙상 인정되지 않는다는 독일 판례와 학설에 의해 형성되었고, 우리 판례와 학설에 의해 수용되고 있다; 김준호, 전게서, 49-50면 참조; 대법원 1992.1.21 선고, 91다30118 판결 등.

해지할 수 있는 것이 거래계의 약관이다.[183]

생각해보건대, ISP계약을 체결한 일반 이용자들의 행태를 살펴보면 대체로 가정용 초고속통신망에 1개의 사설 유무선 AP를 설치하여 여기에 PC, 노트북, 스마트폰을 유무선으로 연결해서 사용하는 것이 일반적이라고 할 것이다. 이 경우에 ISP계약을 위반한 것이라고 보기는 어렵기 때문에, 개인 이용자들에게 ISP계약위반을 주장하기는 용이하지 않아 보인다.[184]

(4) 개방 무선랜을 통한 위법행위에 대한 AP보유자의 책임

무선랜을 개방된 상태로 둘 것인가의 여부는 AP보유자의 자유로운 선택에 두도록 하고, 개방된 무선랜에 접속하여 정당한 방법으로 무해하게 합법적으로 사용하는 것은 적법한 것으로 정당화된다고 하더라도, 개방된 무선랜에 제3자가 접속하여 위법한 행위를 추가적으로 하는 경우에는 다른 관점에서 검토되어야 할 것이다.

이에 관한 사례들을 살펴보면, 공개된 무선랜에 접속하여 타인의 데이터센터에 접근하여 신용카드정보를 유출하려고 시도하였고 일부 신용카드정보를 저장시켜 둔 상태에서 적발된 경우에 해킹에 대한 책임을 물어 미국 연방항소심이 징역 9년을 선고한 판례[185]가 있으며, 공개된 무선랜에 접속하여 스팸을 발송하여 추적을 회피하려 한 사례에 대해서도 미국 연방스팸금지법 위반으로 유죄선고를 한 바 있다.[186] 이와 같이 타인의

182) KT QOOK 인터넷서비스이용약관 제8조 3항; [별표1 이용요금] 4. 부가서비스규정.
183) KT QOOK 인터넷서비스이용약관 제13조 6항 8호.
184) 대체로 무선 AP는 4개 채널의 접속이 가능한데, 동시에 2개 채널을 초과하여 접속하는 것을 AP보유자가 통제하는 것이 기술적으로 용이하지 않은 것이 일반적이므로, 동시에 3개 채널 이상 무선 접속하는 것에 대한 책임을 전적으로 이용자에게 부담시킬 수는 없을 것이다.
185) http://pacer.ca4.uscourts.gov/opinion.pdf/054147.U.pdf(2010. 7. 17 방문).
186) John Leyden, "WiFi spam man avoids can Probation for smut site junk mail miscreant", The Register, 2007. 8. 1.(2010. 7. 17 방문).
http://www.theregister.co.uk/2007/08/01/smut_spam_wifi/(2010. 7. 17 방문).

공개된 무선랜에 접속하여 위법한 행위를 한 자에 대해서 범죄로 처벌하는 것은 극히 자연스러운 것이다.

문제는 이러한 경우에 무선랜을 개방된 상태로 두어서 타인이 위법행위를 할 수 있는 환경을 조성한 AP보유자에게 책임을 부과할 수 있겠는가 하는 점이다. 이 문제는 법적으로는 매우 까다로운 것이다. 그 이유는 민법 제756조의 공동불법행위의 하나의 유형으로 불법행위자의 불법행위에 기여한 일체의 행위인 방조에 의한 불법행위도 공동불법행위로서 불법행위자와 동일한 책임을 연대하여 부담하도록 되어 있으며, 판례[187]에 따르면 과실에 의한 방조도 가능하다고 인정하고 있으므로 AP보유자도 위법한 행위를 한 접속자와 연대하여 불법행위책임을 부담해야 한다고 볼 여지도 있다. 특히 과거 P2P서비스제공자가 업로더와 다운로더의 불법행위를 방조한 것으로 보아 공동불법행위책임을 지워온 우리 판례[188]의 경향을 살펴보면, 무선랜을 개방된 상태로 두어 제3자가 불법행위를 할 수 있는 여건을 결과적으로 조성하는 것을 위법하다고 볼 가능성도 배제할 수 없다.

전술한 독일 연방대법원판례에서는 공개된 무선랜에 접속하여 저작권으로 보호되는 음악파일을 다운로드 한 자의 불법행위에 대해 AP제공자는 저작권침해의 책임을 부담하지는 아니한다고 판시한 바가 있다.[189] 이러한 판례는 AP제공자에게 타인의 위법행위에 대한 책임을 부담시키지 아니할 근거로 적용될 수 있을 것이다.

법이론적으로 살펴보면, 무선랜 보유자에게 접속인증조치를 설정할 의무를 부과하지 아니하고 정당한 방법으로 무해하게 합법적으로 사용하는 것을 허용한다는 묵시적 의사가 있는 것으로 해석한다면, 무선랜 보유자는 접속자의 불법행위에 기여한 자라기보다는 접속자에 의해 자신의 무선랜에 대한 권리를 침해받는 또 다른 피해자라고 보는 것이 법리상 타당하다고 생각된다. 왜냐하면 무선랜을 공개하는 전제에는 정당한

187) 대법원 2000. 4. 11. 선고 99다41749 판결.
188) 대법원 2007.1.25. 선고 2005다11626 판결.
189) BGH, Urteil vom 12. Mai 2010, ZR 121/08.

방법으로 무해하게 합법적으로 사용하는 경우에만 이용하도록 허용한 것이나 이를 접속자가 위반하여 위법한 행위를 추가적으로 한 것이므로, AP보유자의 권리가 침해된 것으로 보아야지 AP보유자가 접속자의 공동불법행위자라고 보는 것은 타당하지 않다.

나. AP제조자에 대한 정책방향

(1) 접속인증 기능 의무화

사설 AP보유자가 접속인증조치를 취할 것인가의 여부는 법으로 강제할 것이 아니라, 사설 AP보유자의 자유로운 판단에 맡기어야 한다. 그러나 사설 AP보유자가 스스로 자신의 AP에 접속인증조치를 취하고자 하는 경우에 이를 용이하게 실행할 수 없다면, 무선랜 보안의 확보를 위해서는 심각한 장애요소로 작용하게 될 것이다. 왜냐하면 접속인증조치를 실행하기 위해서는 이미 AP에 접속인증을 위한 기능이 기술적으로 포함되어야 있어야만 현실적으로 가능하며, 이러한 기능을 사설 AP보유자가 AP를 구매한 이후에 추가하는 것은 불가능에 가깝게 기대하기 어렵기 때문이다. 따라서 사설 AP의 접속인증조치를 위해서는 AP제작자가 접속인증기능을 AP에 포함시키는 것이 매우 중요하다.

무선랜 보안을 위해 AP제작자에게 무선랜 접속인증기능을 포함시키는 것을 의무화하는 정책에 대한 논의도 활발하게 이루어지고 있다. 미국 캘리포니아주 Business and Professions Code 22948.6조에서는 소프트웨어에 그 장치의 환경설정과정 중에 발생할 수 있는 보안경고를 포함시킬 것, 사용을 하기 위해 경고 스티커를 장치에 부착하여 자신의 무선 네트워크 연결을 보호하는 방법을 알릴 것, 소비자의 동의없이 활성화된 기기의 경우 사용전 보호방법을 제공할 것 등을 규정하고 있다.

그러나 아직 AP제작자에게 무선랜 접속인증기능을 반드시 포함시킬 것을 의무화하거나, 혹은 출하 시에 접속인증을 요구하는 상태를 초기값으로 설정할 것을 의무화하는 법률은 비교법적으로도 찾아보기 어렵다.

AP제조자에 대한 무선랜 보안 정책의 가장 기초로서 AP제조자에게 접속인증 기능을 포함시킬 것을 의무화하는 것은 무난할 것으로 생각된다.

왜냐하면 이미 모든 AP에 접속인증을 위한 초보적인 형태의 패스워드를 설정하는 정도의 기능은 예외없이 다 포함되어 있기 때문에 전혀 새로울 것이 없이 100% 실천되고 있는 사양을 의무화하는 것이기 때문이다.

(2) 구매자에 대한 보안관련 설명의무

AP를 구입하여 이용하는 자가 자신의 AP를 개방된 상태로 둘 것인지 아니면 보안을 설정할 것인지는 자유로운 의사에 맡기어야 하며, 보안설정을 국가가 강제해서는 곤란하다고 판단한 바 있다. 하지만 무선랜 보안을 위해서 가장 중요한 점은 AP보유자가 자신의 AP에 보안을 설정하고자 하나 보안을 설정하는 방법이 너무 복잡하고 어려워서 사실상 불가능하기 때문에 원치 않게 개방된 상태도 두는 것은 반드시 방지해야 한다. 기술에 대해 문외한인 일반 이용자가 AP에 보안을 설정하는 것은 현재로서는 그리 손쉬운 일은 아니라고 생각된다. 지금도 WPS(WiFi Protection Setup)기능이 내장된 AP가 대부분이지만, 일반 이용자들이 무선랜 보안을 설정하는데는 여전히 어려움을 겪는 것이 현실이다.

그러므로 AP제조자가 AP를 판매하면서, 구매자가 원한다면 손쉽게 보안을 설정할 수 있도록 그 방법을 상세히 알기 쉽게 설명하는 것이 매우 중요하다. 따라서 AP제조자에게 이용자의 보안설정에 관한 상세하고 이해하기 쉬운 안내를 포함시킬 의무까지 부과하는 것도 하나의 정책으로 고려해 볼 수 있을 것이다.

(3) AP 출하시 보안 설정 의무

무선랜 보안을 위해 AP에 보안기능을 반드시 포함시키고, 이용자에 대해 보안설정 방법에 대해 상세하고 이해하기 쉬운 안내를 제공하여야 하는 동시에, 아예 공장출하시 초기값을 접속인증이 요구되는 상태로 두

는 것 까지 의무화하는 것도 가능할 것이다. 만약 특정 제조업자가 생산하는 특정 모델의 AP의 패스워드를 다 다르게 설정하면 이용자가 패스워드를 잊어버렸을 때를 고려하면 편의성이 저해될 것이고, 모든 패스워드를 다 동일하게 설정하면 실질적으로 패스워드를 설정하지 않은 것과 아무런 차이가 없을 것이다.

따라서 이에 대한 대안으로는 AP제조자가 AP기기를 제조할 때 각 기기의 일련번호(serial number)를 자동으로 패스워드로 설정하는 방법을 고려해 볼 필요가 있다. 기기의 일련번호를 패스워드로 설정하면, 기기의 밑면 등에 일련번호가 기재된 스티커가 붙어있는 경우가 일반적이므로 설령 패스워드를 잊어버린다고 하더라도 이용자의 편의성에는 아무런 지장이 없다. 또 임의의 제3자는 기기의 일련번호를 쉽게 알아낼 수 없을 것이고, 기기 밑면의 일련번호를 알 정도로 소유자와 긴밀한 관계에 있는 사람의 이용까지 제한할 필요는 없으므로 적절한 보안이 유지될 수 있을 것이다.

그러므로 모든 AP에 대해 기기의 일련번호를 패스워드로 하여 초기값을 보안설정상태로 출하할 의무를 부과하는 것도 무선랜 보안을 위한 AP제조자에 대한 보안대책 중 하나로 신중히 검토될 수 있을 것이다. 다만 이 경우에도 AP보유자가 자신의 AP를 다른 패스워드로 바꾸거나 혹은 아예 무인증의 개방된 상태로 전환하는 것이 매우 용이하도록 하여야 할 것이다.

다. AP접속 이용자에 대한 정책방향

(1) 인증이 필요한 AP에의 무단 접속

사설 AP보유자가 접속인증조치를 취하였음에도 불구하고 무단으로 제3자가 접속한 경우는 이미 잘 알려진 '해킹' 개념에 해당된다고 할 수 있다. 정보통신망법 제48조에서는 "누구든지 정당한 접근권한 없이 또는 허용된 접근권한을 넘어 정보통신망에 침입하여서는 아니 된다"라

고 규정하고 있어서 인증이 필요한 무선랜에 무단으로 접속하는 것을 이미 금지하고 있다. 즉 AP보유자가 패스워드를 통해 정당한 접근권한을 부여하는 경우에만 접속하도록 한 경우에, 이 패스워드를 몰래 알아내서 접속한 경우에는 정보통신망법 제48조를 직접 위반한 것이 된다. 그러므로 정보통신망법 제72조의 벌칙이 적용되어 3년 이하의 징역 또는 3천만원 이하의 벌금에 처할 수 있게 된다. 접속인증이 설정된 AP에 무단으로 접속하는 것에 대한 법적 통제장치는 이미 확보되어 있으므로, 추가적으로 고려할 정책사항은 없다고 생각된다.

(2) 개방 무선랜의 접속 규제

임의의 제3자가 타인의 개방된 무선랜에 접속하는 것이 합법적인 행위로서 허용되어야 하는 것인가의 문제도 무선랜 보안과 관련하여 심각한 논쟁점 중에 하나이다. 특히 영국의 사례를 살펴보면, 2005년 영국의 Gregory Straszkiewicz라는 청년이 주거지역에서 타인의 건물 밖에서 무선접속이 가능한 노트북을 들고 타인의 무선 네트워크를 무단으로 이용하려고 했다는 이유로 Comminication Act 위반으로 유죄를 선고한 사례가 있다.[190]

그러나 우리나라의 현실을 살펴보면, 인구가 밀집해있는 수도권의 경우에는 상당수의 지역에서 개방된 상태의 무선랜이 검색되고 스마트폰에서는 자동으로 무선랜 신호를 검색하여 개방된 무선랜에는 접속할 수 있으며 심지어 이미 접속한 적이 있는 개방된 무선랜은 기기가 별도의 절차없이 자동으로 접속하는 기능까지도 갖고 있다. 이런 상태에서 개방된 무선랜에 접속하는 그 자체를 법적으로 금지하는 것은 무선랜에 대한 사회적 요구에 정면으로 반하는 규제가 될 가능성이 높고, 이는 무선랜의 이용활성화에 부정적인 영향을 줄 것이라고 생각한다.

전술한 바와 같이 AP보유자가 자신의 AP를 개방된 상태로 둘 것인가

190) Den llett, "Wireless network hijacker found guilty", Silicon.com, 2005. 7. 22. see http://management.silicon.com/government/0,39024677,39150672,00.htm(2010.7.17 방문).

아니면 인증된 자만이 접속할 수 있도록 할 것인가의 여부는 자유롭게 결정할 수 있으며, 설령 개방된 상태로 두더라도 모든 방법의 이용을 다 허락하는 것이 아니라 정당한 목적으로 무해하게 합법적으로 사용하는 것만을 허용한다는 묵시적인 의사가 있다고 볼 수 있다. 따라서 접속자도 정당한 목적으로 무해하게 합법적으로 무선랜을 이용하는 것이라면 AP제공자의 묵시적인 의사와 합치되는 이용으로서 정당화되어야 할 것이라고 생각된다.

라. ISP에 대한 정책방향

ISP(Internet Service Provider)는 무선랜 보안에서 상당히 중요한 역할을 할 수 있을 것으로 기대된다. 왜냐하면 무선랜에서 무선구간은 AP와 단말기기와의 직접적인 접속노드에 불과하므로 극히 짧은 부분이고, 그 뒤쪽 단은 모두 유선으로 구성되어 있기 때문에 유선 인터넷접속을 제공하는 ISP가 없으면 거의 대부분 무선랜을 통한 인터넷접속은 불가능해질 것이다. 특히 카페나 레스토랑과 같이 사설 AP를 보유하여 소규모로 접속을 제공하지만, 그 접속이용 가능자는 불특정 다수인 경우가 가장 무선랜 보안에 취약함은 이미 영국의 디지털경제법 제정과정에서의 논란에서 잘 살펴볼 수 있다.

이와 같이 대중을 상대로 제공하는 사설 AP의 경우에 전술한 바와 같이 접속인증 보안설정을 의무화할 수는 없지만, 카페나 레스토랑과 ISP와의 ISP계약을 통해 사설 AP보유자에게 이용자에게 보안의 중요성과 위험성을 고지하도록 하는 계약상의 의무를 부과할 수는 있을 것이다. 즉 가입자와 ISP와의 ISP계약에서 “가입자가 무선 AP를 설치하는 경우에는 개방된 상태로 AP를 운영할 수는 있으나, 고객과 같은 이용자가 접속할 때에 보안의 중요성과 위험성을 알리는 초기화면을 제공하고 이용자가 쉽게 알아볼 수 있는 곳에 동일한 내용의 정보를 게시하여야 한다. 이를 위반하는 경우에는 ISP계약을 해지할 수 있다.”라는 계약내용을 포함시키는 것이다. 또 이러한 계약내용이 ISP계약에 포함될 수 있도록

국가가 적절히 ISP에 대해 계도하고 홍보하는 것이 필요할 것이다.

마. 개인정보취급자에 대한 정책방향

무선랜을 통해 개인정보를 취급하는 정보통신서비스 제공자에 대해서는 특히 정보통신망법 제28조 제1항 제2호에서 이미 “개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단시스템 등 접근 통제장치의 설치·운영”을 할 의무를 부과하고 있으므로, 기존의 법규를 통해서 충분히 보안이 유지될 수 있다. 따라서 특별한 추가적인 정책은 필요하지 않다고 생각된다.

3. 데이터 암호화

가. 사설 AP보유자의 데이터 암호화

무선랜 보안을 위해 민간 AP에 데이터암호화를 의무화할 것인가의 문제는 정보통신서비스 제공자가 아닌 사설 AP에 적용하기에는 정책적으로 부적절하다. 현재 일반적으로 개인이 구입해서 사용하는 저가형 AP에 포함된 WEP(Wired Equivalency Protocol)수준의 데이터암호화가 가능할 뿐이다. 그러나 이러한 수준의 데이터 암호화는 기술적으로는 상당히 취약한 것이어서 의도하기만 하면 그리 어렵지 않게 보안침해가 가능하다. 그러나 그 이상의 WPA2수준의 암호화를 사설 AP보유자에게 요구하는 것은 사실상 불가능하다.

무선랜 보안을 위해서 데이터 암호화보다 간편한 ID/PW방식의 접속인증 조차 사설 AP에 대해서 의무화하는 것이 적절하지 않은데, 그보다 한걸음 더 나아간 데이터 암호화를 의무화하는 것은 더욱 타당하다고 보기 어렵다. 따라서 사설 AP에 대해서는 WEP나 WPA 등 기존의 AP에 내장되어 있는 암호화 기능을 사용하도록 권장하는 것 이상의 부담을 지워서는 아니될 것이다.

나. ISP의 데이터 암호화

Hot spot과 같이 기간통신사업자들이 제공하는 상용서비스의 경우에는 데이터 암호화를 고려해볼 여지가 있다. 최근 언론에 따르면 WPA방식의 데이터암호화를 KT가 도입하여 무선랜 보안을 강화한다는 보도가 발표된 바 있다.[191] 정보통신서비스 제공자인 ISP들이 유상으로 제공하는 무선랜의 경우에는 보안이 확보되지 않으면 영업목적을 달성하기 어려우므로 자발적으로 이러한 데이터암호화를 도입할 것이다. 그러므로 국가가 우회적인 방법으로 데이터 암호화를 유도하는 것도 고려해 볼 수 있을 것이다.

다. 암호화된 데이터의 침해

암호화된 데이터를 침해하는 것은 이미 해킹에 대한 법적 규율에 포함될 수 있는 것이므로 현행 정보통신망법 제48조에 의해 규율이 가능하므로 별도의 정책이 추가적으로 필요하다고 생각되지는 않는다.

제 3 절 공공부문의 무선랜 보안 정책 방향

1. 원칙

가. 공공성의 원칙

민간 부문의 무선랜에는 사유재산제 하에서 사적 자치의 원칙이 적용되는 것과 대조적으로 공공 부문의 무선랜에 대해서는 당사자의 자유의

191) http://news.khan.co.kr/kh_news/khan_art_view.html?artid=201007131757035&code= 930201(2010.7.17 방문).

지에 따른 사적 자치의 원칙이 적용될 여지가 없다. 공공부문의 무선랜에 적용되어야 할 가장 중요한 원칙은 공공성의 원칙이다. 특정 개인이나 단체만을 위해 존재하는 것이 아니라 일반 사회 구성원 전체의 이익을 위해 존재해야 하는 본질적인 지향점을 가질 수 밖에 없다.

그러므로 어떠한 공적 주체가 설치하였는가에 관계없이 일반 사회 구성원 전체의 이익이라는 공공의 목적의 달성을 최우선의 원칙으로 설정하여야 할 것이고, 보안정책 역시 이러한 공공성의 원칙에 따라야 한다.

무선랜을 제공하는 공공의 목적을 달성하기 위해서 어떠한 보안정책이 필요한가는 합목적적인 관점에서 파악되어야 한다. 공공의 목적 달성을 위해서 개방된 상태로 모든 사람이 자유롭게 접속하고 사용하는 것이 더 바람직한 것인지, 아니면 일정한 절차를 통해 인증된 사람들에 국한해서 접속하여 이용하도록 제한하는 것이 더 중요한 것인지는 일률적으로 판단하기 어렵다. 왜냐하면 전술한 바와 같이 무선랜 보안과 활성화라고 하는 추구해야 할 가치들은 한편으로는 서로 상충하기도 하고, 다른 한편으로 서로 조화를 이루기도 하기 때문이다.

따라서 공공 부문의 무선랜을 개방된 상태로 둘 것인지 아니면 접속인증을 요구할 것인지는 전적으로 구체적인 정책 판단의 문제이고, 어느 하나만이 반드시 옳다고 보기는 어렵다. 이러한 점은 각국의 무선랜 보안 정책에서도 쉽게 살펴볼 수 있다. 현실적으로도 대만이나 홍콩과 같은 좁은 영토를 가진 국가에서는 자유로운 무선랩 접속이 가능하게 하는 정책을 채택하여 활성화에 더 중점을 두고 있는 반면, 독일과 같은 국가에서는 연방대법원 판례에서 심지어는 민간 소유 AP에 대해서도 접속인증을 위한 조치를 취할 것을 법적 의무로 인정하고 있는 등의 보안에 더욱 중점을 두는 정책을 채택하고 있다. 그러므로 우리나라에서는 어떠한 수준의 보안을 취할 것인지 또 보안의 구체적인 내용을 무엇으로 할 것인지는 우리 사회에 가장 적합한 정책이 무엇인가의 판단문제로 다루어져야 할 것이다. 즉 각국 마다 서로 상이하기 때문에 외국의 입법례나 정책은 결과적으로 공공성이라는 측면에서는 큰 시사점을 주지 못한

다고 생각된다.

그러나 공공부문의 무선랜에는 공공성이라는 원칙이 관철되어야 하므로, 민간부문과 같이 무선랜 운영주체의 자유로운 판단에 맡길 수는 없으며, 반드시 일정한 수준의 보안은 확보되어야만 한다. 어떠한 경우에도 공공부문의 무선랜이 저작권침해나 개인정보 유출과 같이 타인의 권리를 침해하거나 해킹 등과 같은 범죄의 수단이나 도구로 전락해서는 공공성의 원칙에 정면으로 반하기 때문이다. 국가 또는 지방자치단체가 운영하는 무선랜을 이용해서 누구나 임의로 접속해서 타인의 권리를 침해하거나 범죄행위가 자행되도록 두는 것은 국민의 재산권 보호와 치안유지라는 공공부문의 가장 기본적인 의무를 방기하는 것이라고 할 것이다. 다만 그 수준이 어느 정도이어야 하는지, 그리고 어떠한 기술적 방법으로 보안을 확보할 것인지는 뒤에서 조금 더 상세히 살펴볼 필요가 있다.

나. 비례성의 원칙

민간 부문의 무선랜은 설치 주체에 따라서 그 용도가 무엇인가가 명확히 결정되는 것이 일반적이다. 무선랜을 설치하여 이용하고자 하는 서비스의 수준과 내용에 따라서 설치 주체는 어느 정도의 보안을 유지할 것인지를 스스로 결정할 수 있게 된다. 무선랜을 이용하고자 하는 서비스의 본질에 맞는 적절한 수준의 보안을 스스로 확보하게 될 것이므로, 어느 정도의 보안 수준을 유지해야 한다는 강제적인 의무화 보다는 당사자의 자율에 맡기는 것이 최적의 해결방법이다.

공공 부문의 무선랜에 적용될 보안의 정도도 비례성의 원칙에 따라 무선랜을 통해 이용하고자 하는 서비스이 무엇인가에 의해 결정되어야 한다. 만약 공공 부문의 무선랜이 전자정부 서비스를 위해서 사용되는 경우에는 매우 높은 수준의 보안이 유지되어야 할 필요가 있다. 예를 들어 관청의 민원서류의 접수나 발급을 위해 민원실에 AP를 설치하고 민원인들이 그 무선랜에 접속하여 전자정부 서비스를 활용하는 경우라면, 그 보안의 수준은 최고수준으로 유지되어야 하며 무선랜에 접속하기 위한

인증절차도 간편할 것보다는 보다 엄격할 것이 요구된다. 반면에 불국사나 석굴암 또는 국립박물관과 같이 관람객이 유물의 설명을 듣기 위해 제한된 사이트에 접속하는 AP라면, 외국관광객들을 위해서라도 접속인증절차가 생략될 필요도 있고 데이터 암호화는 전혀 불필요한 낭비일 수도 있다. 이와 같이 공공 부문의 무선랜에 적용될 서비스는 다종 다양하므로 그 서비스의 특성을 고려하여야 하며 일률적인 보안수준의 적용은 지양되어야 한다.

위와 같은 비례성의 원칙에 따라 공공 부문의 경우에 서비스의 본질에 맞는 적절한 수준의 보안이 유지될 필요가 있으나, 민간 부문과 달리 설치주체의 자유로운 판단에 맡기기 보다는 서비스의 수준과 내용에 따라서 보안의 정도가 결정될 수 있는 어느 정도 획일화되어있는 기준이 필요할 것이라 생각된다. 즉 비례성의 원칙에 따라서 적절한 보안이 유지되어야 하지만 그 판단을 공공 부문의 AP설치 주체의 판단에 맡기는 것이 아니라 정책적으로 결정된 기준을 적용하여야 한다는 점이다.

다. 균질성의 원칙

공공 부문의 무선랜의 설치주체는 매우 다양하다. 공공 부문의 무선랜 보안에 대한 정책이 설치주체에 따라서 각각 달라서는 공공성의 원칙이 확보될 수 없을 것이므로, 설치 주체와 관계없이 균질적인 보안이 유지될 필요가 있다.

특히 접속인증의 경우에는 각 주체에 따라 접속인증절차가 완전히 상이하게 되면, 공공 부문 무선랜을 이용하려는 일반 국민이 접속에 필요한 절차를 마련하는데 혼란을 겪게 되고 또 그 비용도 낭비하게 된다. 예를 들어 국가가 운영하는 공공 부문 무선랜은 공인인증서를 이용해서 접속하는 반면, 지방자치단체는 각 지방자치단체가 발급하는 인증서를 이용해서 인증하고, 또 학교에서는 주민등록번호를 이용해서 인증하고, 정부산하기관은 별도의 ID와 패스워드를 이용하여 인증한다고 한다면, 이용하고자 하는 일반 국민은 매우 혼란스럽기도 하거니와 서울

시민은 부산시가 운영하는 무선랜에는 접속이 불가능한 문제도 생길 수 있다.[192]

그러므로 공공 부문 무선랜에서 유지되어야 할 마지막 원칙으로서는 균질성의 원칙을 들 수 있다. 어느 주체가 설치한 공공 부문 무선랜이든 일반 국민으로서는 동일한 방법으로 인증이 가능하여야 하고, 또 동일한 수준의 보안이 유지되어야 만 공공성이 완전히 보장될 수 있을 것이다. 다만 전술한 바와 같이 비례성의 원칙에 따라서 각각의 서비스의 특성에 따른 전국 공통의 획일적인 보안이 유지되어야 할 것이다.

즉, 비례성과 균질성의 조화를 통해서 공공 부문 무선랜의 공공성의 원칙이 완전하게 담보될 수 있을 것이다.

2. 접속인증

가. 접속인증의 필요성

(1) 보안설정 의무화

공공 부문 무선랜의 경우에 공공성의 원칙에 따라 접속인증이 전혀 필요없이 개방된 상태로 두는 것은 적절하지 않다. 공공 부문 무선랜은 공공의 목적을 가지고 운영되는 것이므로 아무나 접속할 수 있는 상태로 두는 것은 위법행위의 온상을 국가가 적극적으로 제공하는 것과 다를 것이 없다. 그러므로 공공 부문 무선랜을 설치한 주체가 원한다고 하더라도 민간 무선랜과 같이 개방된 상태로 서비스를 제공하는 것은 원칙적으로 허용되어서는 아니 된다.[193]

---

192) 마치 대중교통수단에 이용되는 교통카드의 시스템이 달라서 각 지역마다 호환성이 없는 불편함과 유사한 현상이 벌어질 것이다.

193) 예외적으로 불국사나 박물관 등의 유명 관광지와 같이 극히 제한적으로는 자유롭게 무인증으로 접속할 수 있는 무선랜도 필요하지만, 그에 상응하는 제한이 필요하다. 이에 대해서는 뒤에서 상술한다.

(2) 공개적 운영

공공 부문 무선랜에서 중요하게 구분되어야 하는 정책은 '개방'과 '공개' 그리고 '무상'의 구분이다. 먼저 공공 부문의 무선랜은 일반 국민들에게 널리 '공개'되어야 하지만, 자유롭게 '개방'되어서는 아니된다. 공공 부문 무선랜은 합리적인 이유 없이 이용자의 자격에 제한을 두는 폐쇄적인 방법으로 운영되어서는 아니 되며, 모든 국민이 이용할 수 있도록 '공개'적으로 운영되어야 한다. 그렇다고 해서 모든 국민이 아무런 통제 없이 마음대로 접속할 수 있도록 개방된 상태로 두어서는 아니된다. 공공 부문의 무선랜을 이용하고자 하는 국민이라면 그것을 이용할 수 있으나, 일정한 요건을 충족하여 접근 권한을 획득한 자 만이 이용할 수 있도록 하여야 한다. 그러나 일정한 요건을 충족하여 접근권한을 획득하는 인증절차가 매우 복잡하고 어려운 것이라면 그것은 실질적으로는 폐쇄적인 운영이므로 공공 부문 무선랜에 접속할 수 있는 인증절차는 보통의 일반적인 국민이라면 어렵지 않게 충족시킬 수 있는 수준으로 마련되어야 한다.

(3) 무상이용

또한 공공 부문 무선랜은 개방이 아닌 공개된 상태로 운영되더라도, 원칙적으로 모든 국민이 무상으로 이용할 수 있어야 한다. 즉 개방된 상태가 아니라 일정한 인증절차를 밟아서 공공 부문 무선랜에 접속하도록 하더라도, 인증절차의 요건으로 유상성을 전제로 하여서는 아니 된다.

인증절차가 요구된다고 하더라도 인증절차의 주된 내용은 보안과 관련된 것에 국한되어야지 유상의 회원가입과 같은 유료를 전제로 하는 인증이라면, 역시 공공 부문 무선랜의 공공성과 공개성을 완전히 충족시키기는 어렵다. 결론적으로 공공 부문의 무선랜은 접속인증을 필요로 하는 것을 원칙으로 하고, 또한 접속인증에 대가를 요구하지 않는 무상성을 기본으로 하여야 할 것이다.

나. 접속 인증의 방법

(1) 접속인증의 기본 방침

공공 부문의 무선랜은 일정한 요건을 충족하여 접근권한을 획득한 경우에만 접속이 가능하도록 인증절차를 두는 것을 원칙으로 하여야 한다. 또 공공 부문 무선랜의 접속인증에 필요한 요건은 무선랜 운영주체가 사전에 공개하여야 한다. 즉 공공 부문 무선랜에 접속할 단말기기가 갖추어야 될 요구조건을 사전에 공개하고 그것을 준수하는 단말기기에만 접속이 가능하도록 하여야 한다. 이렇게 인증에 필요한 요건을 사전에 공개하는 것은 공공 부문 무선랜의 공개성을 실질적으로 확보하기 위해서 매우 중요한 일이 아닐 수 없다.

또 공공 부문 무선랜에 접속인증이 요구된다고 해서 매우 어렵고 복잡한 절차를 거치도록 하는 것도 바람직한 것은 아니다. IT에 전문적인 지식이 부족한 일반인이 손쉽게 접속할 수 있는 정도의 인증보안수준을 넘는 것은 무선랜 활성화에 장애요소로 작용할 수 있을 것이기 때문이다. 즉, 일반 국민이라면 접속하기에 불편하지 않은 수준의 접속인증이 가능하도록 구성되어야 할 것이다.

특히 사설 AP와 달리 공공 부문 무선랜을 추진하기 위해서 많은 예산 지원이 요구되므로 이에 접속인증에 필요한 예산을 반영하여 일정한 수준의 접속인증 설비를 확보하는 것이 무리라고 할 수 없다. 공공이 주체가 되어 추진하는 만큼, 무선랜 공급의 속도를 낮추더라도 안전한 접속이 가능하도록 접속인증이 확보된 공공 부문 무선랜의 제공이 적절할 것이다.

(2) 사용자 인증의 불가피성

공공 부문 무선랜 접속을 위한 인증 방법은 다양하겠지만, 접속단말의

기기인증의 방법 뿐만 아니라 접속자를 인증하는 사용자인증의 방법을 취하는 것도 바람직하다고 생각된다. 3G 네트워크와 USIM Chip을 이용하는 스마트폰을 이용해 무선랜에 접속하는 경우라면 단말기기와 이용자가 결합되어 있으므로 기기인증방식으로도 보안요건을 충족시킬 수 있을 것이다.[194] 그러나 공공 부문의 무선랜에 접속하는 단말이 반드시 실제 이용자와 긴밀하게 결합되기 보다는 단말기기와 이용자와는 특별한 연관성이 없는 경우도 상당한 비중을 차지할 것으로 예상된다. 예를 들어 넷북이나 아이패드같은 태블릿 컴퓨터, 휴대전화서비스에 가입되어 있지 않은 스마트폰 등은 이용자와의 결합도가 낮아서 누가 그 단말기기를 사용하고 있는 것인지 알기 어려운 것이 일반적이다. 또 공공 부문 무선랜에 접속하기 위해서 특정한 사용자가 특정기기를 사전에 해당기관에 등록하여 기기 인증을 받을 것을 요구하는 것은 지나치게 번거로운 인증절차가 아닐 수 없다. 그러므로 공공 부문 무선랜에 접속하기 위한 인증은 기기인증과 사용자인증 중 구체적인 사정에 가장 적합한 것을 선택할 수 있어야 할 것이다.

(3) 사용자 인증의 구체적인 방법

접속인증을 위한 구체적인 방법으로는 단순한 ID/Password 방식보다는 전국민이 널리 사용하고 있는 공인인증서를 경량화하여 접속인증을 위한 수단으로 사용하는 것이 경제적이면서도 효과적인 대안이 될 것이라고 생각한다. 현재 iPhone에서도 공인인증서를 통해 금융거래가 가능한 상황을 고려하면, 무선랜에 접속하고자 하는 디바이스에 공인인증서를 설치하고 그것을 이용해서 공공 부문의 무선랜에의 접속인증을 실시하는 것이 기술적으로 불가능한 것은 아니다. 또 공인인증서는 전국적

194) 현재 iPhone으로 네스팟에 접속하는 것은 기기인증의 방식을 취하고 있으며, 이 경우에는 iPhone과 이용자가 긴밀하게 결합되어 있으므로, 즉 타인이 자신의 iPhone을 무단으로 사용한다는 것은 극히 드문 일이므로, 보안에 심각한 문제가 발생하지 않는다.

인 유효범위를 갖는데다, 이미 일상생활에서 널리 활용될 정도로 보급되어 일반인들이 사용하기에 어려움이 없고, 발급비용 또한 무료이거나 극히 소액이므로 이용자의 인증비용부담도 문제가 없으며, 보안의 품질 또한 '공인'인증서이므로 매우 높은 수준이라는 점에서 최적의 인증수단 중 하나가 아닐까 생각된다.

(4) 접속인증절차의 통일성

또한 공공 부문 무선랜이 전국적인 범위에서 단일한 망으로 제공되는 것이 아니라 지방자치단체 등에 의해서 지역범위에서 개별적으로 제공된다고 하더라도 일반 국민으로서는 어느 곳에서나 공공 부문 무선랜에 접속할 수 있도록 되어야 할 것이다. 즉 Seamless한 무선랜 접속인증이 요구된다고 할 것이다. 이러한 통일성은 모든 공공부문의 무선랜이 공인인증서를 통한 접속인증을 하게 되면, 자연스럽게 확보될 수 있을 것이라 생각된다. 이러한 점도 공인인증서를 통한 접속인증의 하나의 장점으로 들 수 있다.

다. 공공 부문의 개방 무선랜 도입

(1) 필요성

공공 부문 무선랜에는 접속인증이 요구되는 것이 원칙이지만, 극히 예외적인 경우에는 접속인증을 요구하지 않는 것도 고려해 볼 수 있다.

특히 외국인 관광객 등이 자주 찾는 유명 관광지의 경우에는 비교적 짧은 시간동안 머무를 뿐이고 또한 관광안내 등의 목적으로 보다 간편하게 정보에 접속하는 것이 요구되므로 개방된 상태로 공공 부문 무선랜을 운용하는 것도 바람직할 수 있다.

(2) 공간적 제한

다만 예외적으로 개방 AP를 운영하게 되면 보안의 취약성이 문제가 되므로 이를 보완하기 위한 정책적 고려가 요구된다. 먼저 개방AP에 대해서는 공간적 제한을 두어야 할 것이다. 즉 유명관광지와 같은 특정한 장소에서만 개방 AP의 접속이 가능하도록 하여야 한다. 이러한 공간적 제한은 AP의 개수나 출력의 조절을 통해 아주 간단히 가능하므로 기술적으로는 전혀 문제가 되지 않는다.

(3) 시간적 제한

둘째로 개방AP를 통해 접속할 수 있는 세션의 길이를 제한하여야 할 것이다. 개방AP의 운영은 일시적으로 접속하여 꼭 필요한 정보만을 접속하는 것에 그쳐야 하므로 기기의 접속이 오랜 시간동안 유지되어야 할 필요가 없을 것이다. 그러므로 개방AP를 통해 접속하는 경우 접속세션을 통제하여 1회 접속에 일정한 시간동안만 접속이 유지되도록 제한을 두어야 할 것이다. 다만 접속세션의 시간은 개방AP를 운영하는 구체적인 사정과 특성에 맞도록 적절히 개별적으로 결정되어야 할 것이다.

(4) 정보의 제한

끝으로 개방AP를 통해 접속하여 얻을 수 있는 정보를 제한하는 것도 고려할 필요가 있다. 개방AP를 운영하는 취지에 부합되는 정보만을 제공하는 것으로 개방AP의 목적은 달성가능하므로 개방AP를 통한 접속이 위법한 행위의 출발점으로 악용되는 것을 예방하기 위해 접속할 수 있는 정보를 제한하는 것도 가능하다. 따라서 특정한 사이트에의 접속, 예를 들면 박물관이면 박물관 소장품의 정보가 게시된 사이트, 유명 사찰이면 사찰에 대한 소개가 게시된 사이트, 경기장이면 경기장이나 당해 경기와 관련된 내용이 소개된 사이트에 국한하여 접속이 가능하도록 통제하는 것도 구체적인 정책으로 제안할 수 있을 것이다.

3. 데이터 암호화

가. 제공서비스의 차별화에 따른 암호화 판단

공공 부문 무선랜에 접속하여 이용하는 서비스의 질에 따라 보안의 수준은 각각 달리 운영되는 것이 효율적이다. 관광지에서 관광정보에 접속하기 위해서 행해지는 무선랜 접속이라면 보안수준은 극히 낮아도 되고, 주고 받는 데이터도 구태여 암호화 할 이유가 없다. 반면에 인터넷뱅킹이나 인터넷쇼핑 또는 전자정부 서비스를 위한 접속이라면 접속인증 외에 데이터 암호화도 요구된다고 할 것이다. 이러한 서비스에 따라 망차별화가 기술적으로 가능하다면, 망에서 행하여지는 서비스의 종류에 따라 암호화도 구별되어야 할 것이다.

그러나 공공 부문 무선랜의 성격상 보안이 중요하므로 기본적으로 데이터 암호화는 반드시 실시하는 것을 원칙으로 하여야 할 것이다.

다만 WEP수준의 암호화는 현재 실질적으로 암호로서의 기능을 더 이상 하기 어렵다고 생각되므로, 그 이상의 '기술적으로 적정한' 수준의 암호화를 기반으로 하여야 할 것이다.[195]

나. 전자정부 서비스에 따른 요구 조건

전자정부 서비스를 위해서는 높은 수준의 암호화가 요구된다고 할 것이다. 그러므로 접속인증은 다른 서비스와 달리 할 것이 아니라 하더라도 주고 받는 데이터의 암호화는 매우 높은 수준으로 이루어져야 할 것이다.

그러므로 공공 부문 무선랜을 통해 전자정부서비스에 접속하는 경우에는 인터넷 뱅킹과 유사한 수준의 데이터암호화 수단을 확보하도록 하여야 할 것이다. 현재로서는 무선랜의 데이터 암호화에서 상당한 수준이라고

195) 구체적으로 어떠한 기술이 적용되는 것이 바람직한가는 이 연구보고서의 범위를 넘는다고 생각되므로, 과학기술적인 평가를 통해 결정되어야 할 것이다.

평가받고 있는 WPA2 수준의 데이터암호화 정도를 구비하는 것이 바람직할 것이다.

다. 암호화된 데이터 침해

공공 부문 무선랜에서의 암호화된 데이터를 침해하는 것은 이미 민간 부문에서 살펴본 마와 같이 해킹에 대한 법적 규율에 포함될 수 있는 것이므로 현행 정보통신망법 제48조에 의해 규율이 가능하므로 별도의 정책이 추가적으로 필요하다고 생각되지는 않는다. 다만 공공서비스에 대한 해킹은 개인간의 데이터 교환과 달리 가중하여 처벌하는 것도 고려해 볼 수 있을 것이다.

제 4 절 구체적인 법제도 정비 방안

1. 입법론적 정비 방안

가. 정보통신망법 제2조 제3호의 정보통신서비스 제공자의 개념정의

(1) 현행 규정의 의의

정보통신망법 제2조 3호는 정보통신서비스 제공자라 함은 “「전기통신사업법」 제2조 제8호에 따른 전기통신사업자와 영리를 목적으로 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자를 말한다.”라고 개념정의하고 있다. 이 개념정의에 따르면 정보통신서비스 제공자는 전기통신사업자와 영리목적의 정보제공자 또는 정보제공매개자이므로 공공기관이나 영리목적이 아닌 개인은 이에 해당되지 않게 된다.

이와 같이 정보통신서비스 제공자의 개념을 좁게 정의하는 것은 첫째로 지금까지 정보통신서비스를 제공하기 위해서는 막대한 시설투자가 소요되는 것이 일반적이므로 전기통신사업자 또는 영리를 목적으로 하는 자들 외에는 이와 같은 행위를 할 가능성이 매우 낮다는 현실적인 이유를 들 수 있다. 둘째로 정보통신망법은 주로 정보통신망에 대한 규제의 수범자로서 '정보통신서비스 제공자'만을 규정하는 경우가 매우 많다.[196] 이러한 규제는 일반 국민인 개인을 수범대상으로 하기에는 강도가 높은 것으로서 일정한 규모 이상의 사업자를 대상으로 하여야 하므로 고도의 영리성을 추구하는 제한된 주체만을 따로 수범자로서 구분하여 정의할 필요가 있었다.

(2) 현행 규정의 문제점

정보통신서비스 제공자를 '전기통신사업자와 영리목적의 정보제공자 또는 정보제공매개자'로 매우 좁게 규정하는 것이 지금까지는 법현실과 잘 조화를 이루고 있었다. 그러나 기술의 발달로 인해 평범한 일반 시민들도 정보통신서비스를 개인적인 목적으로 극히 소규모로 제공할 수 있게 되었고, 그 대표적인 것이 지금 문제가 되고 있는 사설 AP를 통해 WiFi신호를 제공하는 것을 들 수 있다.

그러므로 정보통신망법의 정보통신서비스 제공자의 개념정의에 사설 무선랜 보유자도 해당되는 것으로 볼 것인가의 문제가 발생한다. 그러나 사설 AP제공자는 영리의 목적으로 정보의 제공을 매개하는 것이라기 보다는 개인적 목적으로 무선랜 네트워크를 제공하는 것이므로 정보통신서비스 제공자라고 보기는 어렵다. 그렇다고 한다면 정보통신망법 제45조 이하의 정보통신망의 안정성 확보에 관한 규정은 모든 사설 무선랜 AP보유자에게는 적용되기 어렵다고 해석할 수 밖에 없다. 즉 정보통신망법 제45조 1항의 "정보통신서비스 제공자는 정보통신서비스의 제공에

196) 특히 규제 관련 내용을 포함하는 대표적인 조항인 제44조, 제44조의2, 제45조는 실질적인 규제 대상을 정보통신서비스 제공자에 국한하고 있다.

사용되는 정보통신망의 안정성 및 정보의 신뢰성을 확보하기 위한 보호조치를 하여야 한다.“는 것을 근거로 하여 당장 무선랜 AP보유자에 대한 접속인증조치의 의무화는 불가능하다고 봐야 할 것이다.

영국 디지털경제법 제정 과정에서 논란을 가져왔던, 도서관, 카페, 극장 등 AP보유자 개인이 사용할 목적이 아니라 일반 대중들의 접속제공을 전제로 하나 다만 영리목적이 결여되어 있는 경우에 까지 개인용도의 AP와 동일하게 다루는 것은 적절하지 않다. 그러나 현행 정보통신망법의 개념정의가 그대로 유지되는 한 이들에 대해 안전성과 신뢰성 확보를 위한 조치를 의무화하기는 어렵다는 문제가 발생된다.

(3) 개선방안

민간 부문 무선랜 보안을 위한 정책으로 사설 AP보유자에 대해 접속인증 등 보안조치를 취할 일반적인 의무를 부과하는 것은 적절하지 않다고 이미 밝힌 바 있다. 만약 AP보유자가 개인이라면 위와 같이 보안조치를 의무화 하지 않는 것이 적절할 것이고, AP보유자가 기간통신사업자와 같은 정보통신서비스 제공자라면 스스로 영업상 필요한 보안조치를 자율적으로 마련하겠지만, 영국에서 문제가 되었던 것처럼 대학, 도서관, 커피숍과 같은 어느 정도 규모가 있는 민간 주체라면 정보통신서비스 제공자에 해당되지 않는다고 하여 개인처럼 보안조치를 취할 의무를 전혀 부과하지 아니한 것도 바람직하다고 보기는 어렵다.

현행 정보통신망법을 그대로 유지하는 한, 정보통신서비스 제공자의 개념정의가 비교적 명확하므로 영국 디지털경제법에 제정논의과정에서와 같은 논란이 우리 사회에서 일어나지는 않을 것이다.

그러나 정보통신서비스를 제공하는 주체가 기술변화에 따라 매우 다양해지고 있는 현실을 감안한다면, 정보통신망법의 정보통신서비스 제공자의 개념을 수정하거나 또는 해당 조문에서 수범자를 정보통신서비스 제공자뿐만 아니라 “개인적인 용도를 넘어 일반 대중을 상대로 정보통신서비스를 제공하는 자”도 포함시킬 수 있는 개정을 검토할 필요가 있을

것이다. 다만 이와 같이 범위를 확대하면, 영국 디지털경제법 논의과정과 같은 논란이 예상되고 따라서 무선랜 활성화에 어느 정도 부정적으로 작용할 것이라 생각된다.

영국 디지털경제법에 관한 논란에서는 통신부(Ofcom)의 regulatory code에서 "40만 이상의 가입자를 가진 고정형 ISP"만을 무선랜 보안조치를 의무화하는 대상으로 제한함으로써 구체적 타당성을 확보하는 것도 이와 유사한 대응이라고 생각된다.

나. 공공무선랜 보안을 위한 법적 근거

공공 부문 무선랜에서의 중요한 현실적 과제 중 하나는 접속인증이 적용되면서도 전국적인 범위에서 단일한 인증절차가 적용될 수 있도록 하는 것이다. 특히 지방자치단체에 의해 개별적으로 추진되는 공공 부문 무선랜 사업에서 국가적 범위의 단일인증체계를 갖추도록 정책을 추진하는 것이 요구된다고 할 것이다. 이에 대한 법적 근거는 별도의 입법이 아니라 국가정보화기본법이나 전자정부법 등 기존의 관련성 있는 법률을 개정하여 포괄적인 법적 근거가 되는 조항을 신설하고 이를 구체화하는 하위 법령을 마련하는 방법을 채택하는 것이 좋을 것이다.

다. 각종 하위 규범의 정비

(1) 공공장소 무선랜에 대한 보안 점검

개인이 가정에 설치한 AP와 달리 공공장소에서 불특정 다수인을 대상으로 WiFi를 공급하는 경우에는 이를 통해 저작권을 침해하는 파일공유나 해킹 시도와 같은 위법한 행위의 출발점이 될 우려가 매우 높다. 따라서 이에 대한 보안을 확보하는 것이 중요하다. 그러나 현재 공공장소에서 제공되는 무선랜에 대한 보안점검을 할 수 있는 법적 근거가 명확하게 마련되어 있지는 않다. 그러므로 이에 대한 입법적 해결방안

을 모색하는 것도 무선랜 보안을 위한 하나의 대책이 될 수 있을 것이다.

민간 부문의 공공장소 무선랜은 이른바 Hot-spot이라고 하며, 대부분은 기간통신사업자에 의해 제공되는 경우가 대부분이다. 정보통신서비스 제공자에 해당되는 경우에는 무선랜에 대한 보안점검을 실시하지 않아도, 정보통신망법 제45조 제1항의 보안관련 기본 조항에 의해 정보통신망의 안정성과 신뢰성을 확보하기 위한 보호조치를 하여야 할 명시적 의무가 존재하므로 이에 따라 보안점검을 자발적으로 실시할 수 밖에 없을 것이다. 이들 정보통신서비스 제공자에 대해서는 정보통신망법 제 46조 제 2항에서 보호조치의 구체적 내용을 정한 정보보호조치 및 안전진단의 방법·절차·수수료에 관한 지침(이하 정보보호지침)을 정하여 고시하고 정보통신서비스 제공자에 대하여 이를 지키도록 권고하고 있다. 이 정보보호지침에서 정보통신서비스 제공자 스스로 무선랜에 대한 보안점검을 자율적으로 하도록 규정하는 것을 고려해볼 필요가 있다.

또 다른 법적 근거로서는 정보통신망법 제46조의3 제1항은 이 조문에서 정한 기준에 해당하는 자는 안전진단 수행기관으로부터 자신의 정보통신망 또는 집적정보통신시설에 대하여 매년 정보보호지침에 따른 정보보호 안전진단을 받도록 의무화하고 있다. 이 안전진단 수행기관으로부터 받는 정보보호 안전진단에 무선랜 보안 안전점검을 포함시키는 것도 하나의 방법이 될 것이다.

문제는 대학, 도서관, 카페와 같은 정보통신서비스 제공자는 아니지만 불특정 다수가 이용할 수 있는 WiFi의 경우에도 보안점검이 필요할 수도 있을 것이다. 그러나 이들은 정보통신서비스 제공자가 아니므로 위와 같은 무선랜 보안 안전점검 대상에 포함되지 않는다. 또 안전점검의 대상이라 하더라도 자율적으로 점검을 시행할 것이라고 기대하는 것도 현실적으로 어렵다. 그러므로 정보통신서비스 제공자 아닌 공공장소 무선랜 공급자에 대한 보안점검을 시행할 수 있는 방안이 모색될 필요가 있다.

그 입법적 해결방법으로 기존의 고시를 개정하는 것으로 만으로는 불가능한 이유는 고시의 법적 근거가 되는 정보통신망법에서 정보통신

서비스 제공자만을 수범대상으로 정하고 있으므로, 정보통신서비스 제공자 아닌 민간 공공장소 무선랜 공급자를 고시에 포함시킬 수 없다.

따라서 정보통신망법 제45조 제1항을 개정하여 “또한 영리의 목적 없이 전기통신사업자의 전기통신역무를 이용하여 정보의 제공을 매개하는 자도 동일한 보호조치를 하여야 한다.” 는 내용을 추가하는 것이 필요하다. 그리고 이에 따라 정보보호지침에 이러한 비영리 무선랜 공급자에 대한 안전진단 등 구체적인 조치사항을 포함시켜야 할 것이다.

(2) 무선설비규칙에 무선랜 보안설정 관련 사항 포함

전술한 바와 같이 민간 부문 무선랜 보안을 위한 가장 효과적인 정책수단은 AP제조자에 대해서 무선랜 보안을 위한 기능을 AP에 포함시키고, 이용자가 AP에 보안을 설정하고자 하는 경우에는 매우 쉽게 설정할 수 있게 지원하도록 의무화하는 것이다. 물론 AP제조자에게 어느 정도로 강한 의무를 부과할 것인가는 법현실과 조화를 이루는 내용으로 정책적으로 신중하게 검토되어져야 할 것이지만, 적어도 무선랜 보안을 위한 기능을 포함시키고 보안설정에 대한 상세한 안내를 이용자에게 제공하도록 하는 정도라면 AP제조자가 수용하기에 적절한 수준이 될 것이라 생각한다.

이를 위해 전파법 제45조에 따른 무선설비규칙 제98조 제7항 제1호에 무선랜 보안과 관련된 사항을 포함시키는 것도 입법적인 해결대책이 될 것이다. 즉 “해당 무선랜 설비는 보안취약성이 있으므로 반드시 보안 설정 후 사용하십시오”라는 문구를 동 설비의 외부의 잘보이는 곳에 표시할 것“, ”해당 무선랜 설비제조자는 보안설정 방법 등 보안을 위해 필요한 사항을설명서나 홈페이지 게시 등의 방법으로 사용자에게 충분하고 알기쉽게 고지할 것“을 추가하는 것이 적절할 것이다. 다만 무선설비규칙 제98조 제7항은 블루투스도 대상이므로 이를 명확히 할 필요가 있으며, 5GHz 대역의 무선랜이 존재하는 것도 고려하여 제98조 제5항에도 관련 내용을 포함시켜야 할 것이다.

(3) ISMS 심사기준에 무선랜 추가

정보통신망법 제47조 제2항에 따른 '정보보호관리인증 등에 관한 고시(ISMS 심사기준)'에 무선랜 보안조치 항목을 포함시켜서 인증심사의 기준으로 설정하는 것도 무선랜 보안을 위한 하나의 방법으로 고려해 볼 수 있다. 이렇게 되면 정보보호관리인증을 득하기 위해서는 무선랜 보안조치를 확실하게 갖추게 될 것이므로, 간접적으로 무선랜 보안을 유도하는 정책수단이 될 것이다.

ISMS 심사기준 제11조 별표6에 11.7에 통제목적은 "무선랜 보안", 통제사항은 "무선랜"으로 하여 "무선랜 사용시에 사업정보, 개인정보 등 정보를 보호하기 위하여 사용자인증, 암호화, 무선인터넷 공유기의 보안설정 등 필요한 보안정책을 수립하여야 한다"고 통제내용을 신설하는 것이 바람직 할 것이다.

2. 법해석학적 정비 방안

가. 정보통신망법 제48조 제2항

현행 정보통신망법 제48조 2항의 "누구든지 정당한 접근권한 없이 또는 허용된 접근권한을 넘어 정보통신망에 침입하여서는 아니 된다"는 규정은 유선 네트워크의 해킹을 염두에 두고 제정된 규정이다. 이러한 규정은 거의 대부분의 국가들도 가지고 있는 매우 보편적인 규정이다. 이러한 규정이 과연 무선랜 특히 개방된 무선랜에도 그대로 적용될 것인가는 전세계적으로 논란이 되고 있는 법적 과제이다. 특히 "정당한 접근권한"이 무엇을 의미하는가? 개방된 무선랜에 접속하는 것이 정당한 접근권한이 있는 것으로 다룰 것인지 아니면 정당한 접근권한이 없는 것으로 다룰 것인지는 해석론상으로 매우 어려운 문제이다.

접속인증이 필요한 무선랜과 달리 개방된 무선랜에는 기술적으로는

누구나 접속이 가능하므로 누가 “정당한 접근권한”을 갖는가는 기술적인 관점이 아니라 규범적인 관점에서 판단하여야 할 것이다. 누구나 접근 가능한 상황에서 정당한 접근권한이 있는가를 판단하기 위해서는 접속제공자의 주관적 의사를 기준으로 할 수 밖에 없을 것이다. 예를 들어 저작권으로 보호되는 음악파일의 경우에 누구나 기술적으로 복제가능하지만 이에 대해 정당한 권한이 있는가는 규범적으로 판단하게 되며, 이러한 규범적 판단의 기준은 ‘저작권자가 이용자에게 저작물을 이용할 수 있게 하는 의사를 갖고 있느냐’의 여부로 결정될 것이다.

저작권의 경우에는 저작물의 이용에 대해 저작권자와 이용자간의 계약관계로 정당한 접근권한이 주어지는 것이 일반적이지만, 개방된 무선랜의 경우에는 계약관계가 존재하지 아니하므로 일방적으로 개방하는 무선랜 제공자의 주관적 의사에 따라 결정될 수 밖에 없을 것이다.

앞서 살펴본 바와 같이 민간 부문 무선랜의 경우에는 AP보유자가 자신의 AP를 타인도 정당한 방법으로 무해하게 합법적으로 사용하는 한도에서는 자유롭게 이용하도록 하겠다는 묵시적인 의사를 갖고 있는 것으로 이론구성하였다. 이러한 묵시적 의사에 따른 이용인 경우에는 임의의 이용자는 정당한 접근권한을 갖고 개방된 무선랜에 접속한 것으로 해석되어야 할 것이다. 이러한 법해석학적 이론구성을 통해 민간 부문의 무선랜을 개방할 수 있는 법적 근거와 이를 정당한 방법으로 무해하게 제3자가 이용하는 것이 합법적인 것으로 허용되어야 하는 법적 근거가 마련될 수 있을 것이다.

나. 공동불법행위에 관한 법이론적 검토

전술한 바와 같이 P2P에 의한 저작권 침해에 대한 기존의 판례는 일관되게 P2P운영자의 방조에 의한 공동불법행위 책임을 인정하여 왔다. 이러한 법논리를 형식적으로 개방된 사설 AP를 통한 불법행위에 적용하면 무선 AP제공자에게 방조에 의한 공동불법행위책임을 지워야 하는 문제가 생긴다. 그러므로 법이론적으로 개방 무선랜을 통해 위법행위

가 이루어지더라도 개방된 상태로 무선랜을 제공한 자에게 불법행위책임을 부담시키지 않을 법논리를 검토할 필요가 있을 것이다.

민간 부문의 개방된 무선랜에 제3자가 접속하여 불법복제나 해킹과 같은 타인의 권리를 침해하는 위법한 행위를 한 경우에도 무선랜 제공자는 제3자의 가해행위에 기여한 것으로 해석되어서는 아니 된다.

첫 번째 타인의 불법행위에 대해 과실에 의한 방조가 가능하지만, 과실에 의한 방조가 성립하기 위한 "과실의 내용은 불법행위에 도움을 주지 않아야 할 주의의무가 있음을 전제로 하여 이 의무에 위반하는 것을 말한다"는 것이 판례의 확고한 태도이다.[197] 따라서 무선랜 보유자에게 접속인증조치를 설정할 의무를 부과하지 아니하고 정당한 방법으로 무해하게 합법적으로 사용하는 것을 허용한다는 묵시적 의사가 있는 것으로 해석한다면, 무선랜 보유자에게는 접속인증을 통해 타인의 불법행위를 방지해야 할 주의의무 자체가 없으므로 과실 자체가 성립되지 않는다고 보아야 할 것이다.

둘째로 개방된 AP보유자는 제3자의 불법행위(불법복제나 해킹 등)에 도움을 준 것이 아니라, 오로지 불법행위가 가능할 수 있는 환경을 무차별적으로 제공한 것에 불과하므로 아예 주의의무 위반 자체가 성립되지 않는다. 예를 들어 누구에게나 먹을 수 있도록 자신의 우물을 개방하여 주변 사람들에게 식수를 공급해 온 자에게, 누군가가 그 우물에 독극물을 투입하여 주민들의 건강을 침해한 경우에 우물 소유자에게 그 위법행위에 도움을 주었다고 볼 수는 없는 것이다. 오히려 우물의 소유권을 위법하게 침해한 것으로 보는 것이 더 적절한 법적용이라고 볼 것이다. 따라서 개방된 AP보유자는 접속자의 불법행위에 기여한 자라기보다는 접속자에 의해 자신의 무선랜에 대한 권리를 침해받는 또 다른 피해자라고 보는 것이 법리상 타당하다고 생각된다. 왜냐하면 무선랜을 공개하는 전제에는 정당한 방법으로 무해하게 합법적으로 사용하는 경우에만 이용하도록 허용한 것이나 이를 접속자가 위반하여 위법한 행위를

197) 대법원 2000.4.11. 선고 99다41749 판결.

추가적으로 한 것이므로, AP보유자의 권리가 침해된 것으로 보아야지 AP보유자가 접속자의 공동불법행위자라고 보는 것은 타당하지 않다.

그러므로 개방 AP보유자는 설령 임의의 제3자가 그 무선랜을 이용하여 위법한 행위를 하더라도, 그 불법행위에 대해 구체적인 위험을 인식하고 있는 경우가 아니라면, 그 불법행위에 대한 방조에 의한 불법행위라고 해석되어서는 아니된다. 또 개방 AP와 연결되어 인터넷을 접속할 수 있도록 해준 ISP 역시 공동불법행위책임을 부담하지 않을 것이다.

제 6 장 결 론

무선랜은 사용의 편리함과 낮은 설치 및 유지비용으로 인해 점차 많은 분야에서 널리 활용되고 있다. 특히 스마트폰이 도입된 이후 일반 국민들의 무선랜을 통해 인터넷에 접속하고자 하는 수요가 폭발하여 사회적인 관심대상으로 부각되었다. 하지만 무선랜은 동시에 무선 통신의 특성상 존재하게 되는 다수의 보안 취약점을 가지고 있으며 이런 문제점을 해결하기 위해 다양한 보안관련 기술이 개발 및 적용되고 있다. 그럼에도 불구하고 무선랜 제공자나 이용자의 보안에 대한 인식은 극히 저조한 상태에 머물러 있는 반면, 앞으로 지하철, 할인마트, 주유소 등 일상 생활의 여러 분야에서 무선랜 사용이 증가할 것으로 예상되는 만큼 무선랜 보안은 더욱 중요한 이슈로 다뤄지게 될 것으로 예상되고 있다.

해외의 무선랜 보안 관련 정책이나 법규를 살펴보면, 영국의 디지털경제법의 제정과정에서 대학, 도서관, 카페와 같이 전통적으로는 인터넷 가입자가 대중을 상대로 한 무선랜 공급자로서 활동하는 만큼 이들에 대해서도 무선랜 보안조치를 ISP들처럼 의무화하여야 하는 것은 아닌가 하는 논란이 제기된 바 있었다. 그러나 법제정과정에서 가입자 40만명 이상의 고정형 ISP에 대해서만 저작권 침해와 관련한 보안조치를 강화시키는 선으로 후퇴함으로써 무선랜 제공자에 대한 일반적인 보안조치 의무를 부과하지는 아니하였다. 그 외에 미국 캘리포니아주 사업 및 직업법에서 AP제작자에게 이용자에 대한 보안의 위험성을 고지할 의무와 보안설정의 방법을 설명할 의무를 부과한 바 있다. 또 미국 뉴욕주의 Westchester 카운티에서 인터넷 카페 등에서 이용자의 보안조치를 위한 안내표지를 붙이는 조례를 제정한 바 있다. 그러나 이외에 무선랜 자체를 대상으로 마련된 법률은 찾아보기 어렵고, 주로 전통적인 해킹을 금지하기 위한 법규에 의해 개방 무선랜의 임의접속을 처벌할 수 있는가의 논란이 제기되고 있을 뿐이다. 이러한 점에서 해외의 무선랜 보안 관련

법률에서 우리가 직접적으로 취할 만한 시사점을 찾기는 어렵다. 다만 영국의 디지털경제법 제정과정에서의 논란이 발생한 것처럼, 카페나 레스토랑 등 대중을 상대로 한 무선랜에 대한 통제가 보안상으로는 필요하다고 할지라도, 일반 대중들의 동의를 얻는 것은 현실적으로 어렵고 이는 무선랜의 활성화에 막대한 영향을 줄 것이라는 교훈을 남겼다.

무선랜 보안 침해에 관한 사례를 살펴보면, 국내에서는 아직 무선랜에 관한 침해사례가 보고된 바 없으며, 무선랜의 취약성을 지적한 보고사례만 존재할 뿐이다. 해외의 사례를 살펴보면, 개방된 무선랜에 접속한 그 자체에 대해서 미국과 영국에서 유죄를 선고한 지역 하급심 판례가 소수 있을 뿐이라 유의미한 시사점을 제공하지는 못한다. 개방된 무선랜에 제3자가 접속하여 위법한 행위를 한 경우 AP보유자의 책임에 대해서 독일 연방대법원의 판결이 최근 내려진 바 있다. 이 판례는 AP보유자에게 보안조치를 설정할 일반적인 주의의무를 인정하였다는 점에서는 매우 획기적인 것이지만, 이에 대한 비판도 상당히 존재한다는 점에서 우리 나라에서 그대로 수용하는 것은 바람직 하지 않다고 생각된다. 최근 논란이 되고 있는 구글의 WiFi를 통한 정보수집 사건은 WiFi의 보안이 얼마나 중요한 것인가를 보여주는 대표적인 사례라고 할 수 있다.

무선랜 보안과 관련하여 우리나라가 취할 정책방향으로는 무선랜 제공 주체에 따라 민간 부문과 공공 부문으로 나누어 살펴본다. 먼저 민간 부문의 무선랜에 대해서는 사적자치의 원칙을 적용하여, 무선랜 보안은 자율적으로 시행하는 것을 기본으로 한다. 따라서 사설 AP보유자가 자신의 AP를 개방된 상태로 공개하는 것을 허용하고, 개방 AP에 임의의 제3자가 접속하여 이용하는 것도 적법한 것으로 허용한다. 다만 개방 AP보유자는 '제3자가 정당한 방법으로 접속하여 무해하게 합법적으로 사용하는 것만을 허용한다는 묵시적 의사'가 있는 것으로 간주하고, 이용자도 묵시적 의사에 합치하는 이용만이 합법적인 것으로 허용될 뿐 이러한 묵시적 의사에 반하는 접속이용에 대해서는 책임을 지워야 할 것이다. 또 제3자가 AP보유자의 묵시적 의사에 반하여 저작권침해나 해킹 등의 위법행위를 한 경우에도 AP보유자는 또 다른 피해자로서 공동불법행위자

책임을 지지 않는다고 할 것이다. 민간 부문의 무선랜 보안을 위해서 가장 중요한 것은 AP제작자에 대해서 AP보유자가 보안설정을 원하는 경우에 용이하게 보안설정을 할 수 있도록 정책적인 수단을 마련하는 것이라 생각된다. 따라서 AP제작자에게 보안기능을 AP에 반드시 내장시키고 보안설정 방법을 이용자에게 이해하기 쉽게 알려주며 경우에 따라서는 공장출하시 보안설정이 된 상태로 출하할 의무를 부과하는 것도 고려해 볼 수 있다.

공공 부문의 무선랜 보안을 위해서는 공공성, 비례성, 균질성의 원칙을 준수하여야 한다. 공공 부문의 무선랜은 공공성에 따라서 반드시 접속인증을 요구하도록 하고, 접속인증의 방법은 사용자인증으로서 공인인증서를 이용한 방법이 적절한 방법 중 하나라고 생각된다. 또 접속인증절차는 균질성에 따라 전국적으로 공통된 방법을 사용하는 것이 바람직할 것이다. 유명관광지나 박물관, 경기장 등의 예외적인 경우에는 개방 무선랜을 설치하되, 보안의 취약성을 감안하여 공간적 제한과 시간적 제한 그리고 정보의 제한을 두어야 할 것이다. 또한 공공 부문의 무선랜에는 접속인증 뿐만 아니라 데이터 암호화도 반드시 도입하여, 기술적으로 적절한 수준의 데이터 암호화를 통한 보안의 유지가 이루어져야 할 것이다.

무선랜 보안을 위해서 입법적으로는 정보통신망법 제2조 제3호의 정보통신서비스 제공자의 개념정의를 수정하거나 또는 보안의무의 주체에 대중을 상대로 하는 적절한 규모의 비영리 무선랜 제공자를 포함시키는 시도가 요구된다. 또 공공 부문의 무선랜에 대해 보안설정을 의무화하는 법적 근거를 국가정보화기본법에 포함시키고, 보안 관련 하위 법규를 무선랜 보안을 고려하여 정비하는 방안도 요구된다. 그리고 각국에서 논란이 되고 있는 개방 AP에 임의로 접속하는 그 자체가 “정당한 접근권한” 없이 정보통신망에 접속하는 것으로 보아야 하는가에 대한 법해석론과 개방 AP보유자가 임의의 접속자의 불법행위에 대한 책임으로부터 자유로울 수 있는 범위와 그 법이론적 근거도 적절히 마련되어야 한다.

참 고 문 헌

- 국내 문헌 -

[1] 김준호, 민법강의(신정8판), 법문사, 2008

- 외국 문헌 -

[2] Rovert V. Hale Ⅱ, Esq., *Current Developments in WiFi Liability and Regulation*, Hottest Issues in Cyberspace Law Cyberspace Committee, Business Law Section State Bar of California (2006)

[3] BenjaminKern,Whacking, *Joyriding, and War-Driving: Roaming Use of WiFi and the Law*, 21 Santa Clara Computer & High Tech. L.J. 101, 138 (2004)

[4] Sophos, *Security threat report: 2009*, 11 (2009).

[5] 'Air Tight Networks사'의 세계 7개 금융가 대상 무선랜 취약성 조사 결과. Financial Districts Wireless Vulnerability Study(2009).

[6] T.D. Fischer Group, Riverbend Properties, the Wausau/ Central Wisconsin Convention & Visitors Bureau, and Straight Shot Express Rovert V. Hale Ⅱ, Esq., *Current Developments in WiFi Liability and Regulation*, Hottest Issues in Cyberspace Law Cyberspace Committee, Business Law Section State Bar of California (2006)

[7] Kevin Poulsen, "*Crazy-Long Hacker Sentence Upheld*", Wired, 2007. 11. 06.

- 인터넷자료 및 기사 -

[1] http://www.jiwire.com/ (2010. 7. 10 방문)

[2] http://www.betanews.net/article/500089 (2010. 7. 14. 방문)

[3] http://www.airtightnetworks.com/(2010. 7. 10. 방문)

[4] http://www.WiFi.org/wifi-protected-setup (2010. 7. 10. 방문)

[5] http://wifinetnews.com/archives/2008/04/russia_requires_WiFi_registration.html (2010. 7. 15. 방문)

[6] http://www.newswireless.net/index.cfm/article/941 (2010. 7. 15. 방문)

[7] http://www.chinatradeinformation.net/china-trade-news/relaxation-of-WiFi-restriction-could-remove-iphone-obstacle.html (2010. 7. 15. 방문)

[8] http://management.silicon.com/government/0,39024677,39150672,00.htm (2010. 7. 17 방문)

[9] http://www.cybercrime.gov/ardolfIndict.pdf (2010. 7. 17 방문)

[10] http://www.informationweek.com/news/software/showArticle.jhtml?articleID=225701522 (2010. 7. 17 방문)

[11] http://pacer.ca4.uscourts.gov/opinion.pdf/054147.U.pdf (2010. 7. 17 방문)

[12] http://www.wired.com/science/discoveries/news/2006/07/71358 (2010. 7. 17 방문)

[13] http://www.nydailynews.com/news/national/2009/08/17/2009-08-17_hacker_alberto_gonzales_charged_with_larged_id_theft_ever_involving_130m_credit_.html (2010. 7. 17 방문)

[14] http://www.boston.com/business/articles/2010/07/07/investor_tjx_settle_suit_over_data_theft/?rss_id=Boston.com+--+Top+business+news (2010. 7. 17 방문)

[15] http://www.theregister.co.uk/2007/08/01/smut_spam_wifi/(2010. 7. 17 방문)

[16] http://www.securityfocus.com/news/8991 (2010. 7. 17 방문)

[17] http://news.softpedia.com/news/German-Officials-Horrified-by-Google-Street-View-WiFi-Snooping-140439.shtml (2010. 7. 17 방문)

[18] http://www.zdnet.co.uk/news/security/2010/06/21/googles-WiFi-net-caught-passwords-says-france-40089304/ (2010. 7. 17 방문)

[19] http://news.cnbnews.com/category/read.html?bcode=119323 (2010. 7. 17 방문)

[20] http://www.guardian.co.uk/technology/2010/may/21/google-street-view-uk-data (2010. 7. 17 방문)

[21] http://www.product-reviews.net/2010/06/22/google-street-view-wifi-data-collection-sparks-uk-investigation (2010. 7. 17 방문)

[22] http://www.zdnetasia.com/google-asia-mum-about-street-view-fate-62201392.htm (2010. 7. 17 방문)

[23] http://www.msnbc.msn.com/id/37107291/ns/technology_and_science-security/ (2010. 7. 17 방문)

[24] http://news.cnet.com/2100-1036_3-6177095.html (2010. 7. 17 방문)

[25] http://webcache.googleusercontent.com/search?q=cache:VArK7JzNMyUJ:www.hackforums.net/archive/index.php/thread-321253.html+hack+wpa+via+fake+ssid&cd=2&hl=en&ct=clnk&gl=us&client=safari (2010. 7. 17 방문)

[26] http://techcrunch.com/2010/07/05/employees-challenged-to-crack-facebook-security-succeed/(2010. 7. 17 방문)

[27] http://www.zdnet.com/blog/soho-networking/WiFi-routers-vulnerable-to-upnp-attack-from-hackers/120 (2010. 7. 17 방문)

[28] http://threatcenter.smobilesystems.com/wp-content/uploads/2009/11/MIMT-Whitepaper031.pdf (2010. 7. 17 방문)

[29] http://www.boannews.com/media/view.asp?idx=18717&kind=1 (2010. 7. 17 방문)

[30] http://www.boannews.com/media/view.asp?idx=18055&kind=1 (2010. 7. 17 방문)

[31] http://www.boannews.com/media/view.asp?idx=20827&kind=1 (2010. 7. 17 방문)

해외 무선랜 보안 법제도 연구

인 쇄 : 2010년 7월

발 행 : 2010년 7월

발행인 : 한국인터넷진흥원 원장

발행처 : 한국인터넷진흥원(KISA, Korea Internet & Security Agency)

서울시 송파구 가락동 79-3 대동빌딩
Tel: (02) 4054-118

인쇄처 : 동광문화사

Tel: (02) 503-5165

<< 비 매 품 >>