방송통신정책연구 11-진흥-가-11

IP 응용서비스상의 통신제한조치 기술동향 및 해외사례 연구

(Study on lawful interception policy and technology of IP applications)

김성혜/정영식/박소영

2011. 12

연구기관 : 한국전자통신연구원

방송통신위원회
KOREA COMMUNICATIONS COMMISSION

이 보고서는 2011년도 방송통신위원회 방송통신발전기금 방송통신정책연구사업의 연구결과로서 보고서의 내용은 연구자의 견해이며, 방송통신위원회의 공식입장과 다를 수 있습니다.

제 출 문

방송통신위원회 위원장 귀하

본 보고서를 『**IP응용서비스상의 통신제한조치 기술동향 및 해외사례 연구**』의 연구결과보고서로 제출합니다.

2011년 12월

연구기관 : 한국전자통신연구원
총괄책임자 : 김성혜(한국전자통신연구원)
참여연구원 : 정영식(한국전자통신연구원)
참여연구원 : 박소영(한국전자통신연구원)

목 차

제 출 문 ····· 1

제 1 장 서 론 ····· 16

제 1 절 연구의 필요성 및 목적 ····· 16

1. 연구의 필요성 및 목적 ····· 16

2. 연구의 방법 ····· 16

제 2 장 통신제한조치 연구 ····· 9

제 1 절 국내외 유무선 IP 응용서비스 감청제도 수립현황 분석 ····· 19

1. 통신비밀보호법 개정안 관련 조항 분석(법안중심) ····· 19

가. 이한성 의원 발의 통신비밀 보호법 일부개정안 분석 ····· 19

나. 최문순의원 발의 통신비밀보호법 개정안 분석 ····· 23

라. 변재일 의원 발의 법안 분석 ····· 30

마. 이학재 의원 발의 법안 분석 ····· 36

바. 박준선의원 발의 법안 분석 ····· 39

사. 김태원 의원발의 법안 분석 ····· 41

아. 정옥임 의원 발의 법안 분석 ····· 41

2. 미국의 아동보호법 관련 제도 수립 현황 및 관련 통비 이슈 분석 ····· 42

가. 인터넷 포르노로부터의 아동보호법 ····· 42

나. 무선 사업자에 대한 면제 허용 ····· 43

다. 유지(Retention)“ 대 ″보존(preservation)“ ····· 43

라. 인터넷 포르노로부터 아동보호법 관련 기사 번역 전문 ····· 44

마. 인터넷 포르노로부터 아동보호법 관련 기사 원문 ····· 47

3. 인터넷 서비스 감청 국제표준화 현황 ····· 50

가. 감청 표준화 추진 배경 ····· 50

나. 감청 표준화 추진 개요 ····· 52

다. 미국의 인터넷 서비스 감청 표준화 현황 ····· 53

라. 유럽연합(EU)의 인터넷 서비스 감청 표준화 현황 ····· 55
제 2 절스마트폰 응용서비스 통신비밀 기술 동향 분석 ····· 60
1. 스마트폰의 위치정보 활용 현황 및 문제점 분석 ····· 60
가. 위치정보 관련 현황 ····· 60
2. 데이터 압축 앱 응용 현황 및 통비 관련 이슈 분석 ····· 63
가. 3G 데이터 트래픽 감소 서비스(ONAVO 서비스) ····· 63
나. 아이폰 압축 앱(오페라 터보) 분석 ····· 66
다. 오페라와 Onavo 비교 ····· 67
라. 오페라 서비스 사용자에 대한 통비 이슈 ····· 68
3. 스마트폰 도청 보도에 대한 기술적 분석 ····· 68
제 3 절 유무선 환경에서 SNS, 메신저, VoIP 서비스 감청방안 및 통신비밀 보호방안 연구 ····· 72
1. 인터넷상 개인정보보호방안 시행시 통신수사 관련 영향 분석 ····· 72
가. 인터넷상 개인정보 보호방안 개념 ····· 72
나. 주민등록번호가 저장되어 있지 않을 경우의 통신수사 방안 ····· 73
2. SNS서비스, 모바일 메신저의 통신비밀 관련 고려사항 분석 ····· 73
가. 카카오톡 사업자가 보관하는 통신자료, 통신사실확인자료 내역 및 메시지 보관[삭제] 방법 ····· 73
나. 모바일 메신저에 대한 외국의 수사기법 및 사례 ····· 73
3. SSL 개요 및 해킹 ····· 76
가. SSL(Secure Socket Layer) 개요 ····· 76
나. 가짜 AP(Access Point)를 이용한 SSL의 해킹 ····· 82
4. 통신수단별 감청 방안 ····· 83
가. SNS의 감청 방안 ····· 83
나. 일반유선전화의 감청 방안 ····· 88
다. 인터넷 서비스의 감청 방안 ····· 89
라. 이동전화(음성)의 감청 방안 ····· 93
마. VOIP[Voice over IP]의 감청 방안 ····· 96

5. DPI(Deep Packet Inspection)에 의한 감청 ····· 98
가. DPI 개요 ····· 98
나. DPI(Deep Packet Inspection) 수행 단계 및 개념 ····· 99
다. DPI의 일반 동작 절차 ····· 100
라. DPI의 세부 동작 단계 사례 ····· 101
6. 최근의 유무선 감청의 주요 도전 요소 들 ····· 102

제 3 장 통신비밀자료제공 통계분석업무 개선 연구 ····· 4

제 1 절 국내 통신비밀자료제공 보고 규정 ····· 104
1. 통신비밀자료 제공 절차 ····· 104
가. 범죄 수사를 위한 통신사실확인자료의 제공 ····· 104
나. 국가안보를 위한 통신사실확인자료의 제공 ····· 105
2. 통신비밀자료 제공 집계 ····· 106
가. 통신사실확인자료 제공 집계 규정 ····· 106
나. 통신제한조치 협조 집계 규정 ····· 110
다. 통신자료 제공 집계 규정 ····· 115
제 2 절 통신비밀자료제공 통계도구 보완기능 개발 ····· 118
1. 개요 ····· 118
2. 통신비밀현황입력 툴(클라이언트 프로그램) 메뉴 설명 ····· 119
가. 통신사업자 정보의 등록 ····· 119
나. 데이터의 입력 ····· 121
다. 보고서의 생성 ····· 123
3. 통신비밀통계분석 툴(서버 프로그램) 메뉴 설명 ····· 124
가. 기본정보 ····· 124
나. 현황보고서 ····· 125

제 4 장 결 론 ····· 137

참 고 문 헌 ····· 139

표 목 차

<표 2-1> 이한성 의원 대표발의안 (감청협조설비 구축 의무화) ····· 10·2
<표 2-2> 이한성 의원 대표발의안 요약 (감청협조설비 구축 의무화) ····· 12·2
<표 2-3> 최순문의원 개정안 요약 ····· 14 2
<표 2-4> 이정현 의원 발의법안 요약 ····· 15 2
<표 2-5> 이정현 의원 발의법안 관련 해외 사례 요약 ····· 15 2
<표 2-6> 통신제한조치 관련 개정안 요약 ····· 17 2
<표 2-7> 통신제한조치의 기간에 대한 해외사례 ····· 17 2
<표 2-8> 통신제한조치 대상자의 감청내용 열람 관련 해외사례 ····· 19 2
<표 2-9> 감청내용 폐기에 관한 개정안 요약 ····· 19 2
<표 2-10>감청내용 폐기에 관한 국외 사례 ····· 20 3
<표 2-11> 통신제한조치 요건에 대한 해외 사례 ····· 21 3
<표 2-12> 통신제한조치의 기간에 대한 해외사례 ····· 22 3
<표 2-13> 긴급감청 신청기한 등의 해외사례 ····· 24 3
<표 2-14> 통신사실확인자료 제공절차 강화 법안 요약 ····· 25 3
<표 2-15> 전자유편 감청에 대한 해외사례 ····· 28 3
<표 2-16> 감청기간 연장에 대한 해외사례 ····· 30 4
<표 2-17> 표준 준수 의무에 대한 법 규정 ····· 31 5

그 림 목 차

[그림 1-1] 연구개발 추진체계 ····· 81
[그림 2-1] onavo 서비스의 기술적 개념 ····· 46
[그림 2-2] 이메일 서비스 감청 개념도 ····· 57
[그림 2-3] SSL의 계층적 위치 ····· 87
[그림 2-4] 데이터 압축 및 암호화 구조도 ····· 97
[그림 2-5] 암호화 순서도 ····· 08
[그림 2-6] 중간자공격의 개념 ····· 38
[그림 2-11] 트위터를 이용한 메시지 전달 구조 ····· 68
[그림 2-12] 카카오톡을 이용한 메시지 전달 구조 ····· 78
[그림 2-7] 유선전화 감청 흐름도 ····· 98
[그림 2-8] 이메일 감청 흐름도 ····· 09
[그림 2-9] 메신저 서비스 흐름도 (서버경유) ····· 19
[그림 2-10] 패킷감청 방식 ····· 29
[그림 2-13] 이동전화 감청 흐름도 ····· 49
[그림 2-14] 패킷복제방식 감청 흐름도 ····· 69
[그림 3-1] 범죄 수사를 위한 통신사실확인자료 제공 절차 ····· 04
[그림 3-2] 국가안보를 위한 통신사실확인자료 제공 절차 ····· 06
[그림 3-3] 통신비밀현황입력 툴(클라이언트 프로그램) 메뉴 구성도 ····· 81
[그림 3-4] 통신비밀통계분석 툴(서버 프로그램) 메뉴 구성도 ····· 91
[그림 3-5] 통비통계보고 툴 초기 화면 ····· 10
[그림 3-6] 통신사실확인자료 제공현황보고(지역별) 입력 화면 ····· 21
[그림 3-7] 보고서 생성 화면 ····· 14
[그림 3-8] 기본정보 메뉴의 서브메뉴인 데이터병합 실행화면 ····· 25
[그림 3-9] 제공업체현황 실행 화면 ····· 26

[그림 3-10] 통신사실확인자료 제공현황 보고서 실행화면(지역별-업체별) ·····72
[그림 3-11) 통신사실확인자료 제공현황 보고서 실행화면(지역별-역무별) ·····82
[그림 3-12] 통신사실확인자료 제공현황 보고서 실행화면(지역별-지역별) ·····82
[그림 3-14] 통신사실확인자료 제공현황 보고서 실행화면(업체별-종류별) ·····93
[그림 3-15] 통신감청 협조현황 보고서 실행 화면(업체) ·····11
[그림 3-16] 통신감청 협조현황 보고서 실행 화면(항목) ·····11
[그림 3-17] 통신감청 협조현황 보고서 실행 화면(허가서) ·····12
[그림 3-18] 통신감청 협조현황 보고서 실행 화면(전화번호/ID) ·····33
[그림 3-19] 통신자료 제공현황-업체별 ·····41
[그림 3-20] 통신자료 제공현황-지역별 ·····41
[그림 3-21] 예외규정에 의한 통신사실확인 및 통신자료 제공현황 보고-업체별 ·····52
[그림 3-22] 예외규정에 의한 통신사실확인 및 통신자료 제공현황 보고-지역별 ·····53

요 약 문

1. 제 목

IP 응용서비스상의 통신제한조치 기술동향 및 해외사례 연구

2. 연구 목적 및 필요성

스마트폰 활성화와 함께 이용자가 급증하고 있는 SNS(Social Networking Service), mVoIP 등 유·무선 환경에서의 IP 응용서비스에 대한 통신제한조치의 필요성이 증가하고 있다. 즉, 인터넷회선의 감청, 전기통신사업자에게 감청협조설비 구축의무 부과, 전자우편 감청 등의 통신제한조치의 시행의 필요성이 증가하고 있다. 이러한 추세에 맞추어 전기통신서비스에 대한 통신제한조치 집행 및 통신비밀자료 제공 등을 규제하는 현행 통신비밀보호제도를 개정하기 위하여 다수의 통신비밀보호법 일부 개정법률안이 국회에 발의되어 있다. 개정법률안은 인터넷회선의 감청, 전기통신사업자에의 감청협조설비 구축 의무 부과, 전자우편 감청 등과 같은 통신제한조치 제도 시행에 관한 규정과, 위치정보의 통신비밀자료로의 활용, 통신사실확인자료 및 통신자료의 통합 규제 등과 같은 통신비밀자료 제공 제도의 시행에 관한 규정을 신설 또는 개정하고자 하고 있다. 이와 같은 법률 개정안의 추이를 파악할 필요성이 있다. 또한 이와 관련하여 통신비밀보호제도 수립에 활용하기 위하여 유·무선 IP응용서비스상의 통신제한조치 기술동향을 파악하고, 해외사례의 연구가 요구된다.

이에 본 과제에서는 통신비밀보호법 개정 이슈들에 대하여 검토하고 국내외 IP응용서비스 감청제도 수립현황, 스마트폰 응용서비스 통신비밀 기술동향, 유무선 환경에서 SNS, 메신저, VoIP 서비스 감청방안 및 통신비밀 보호방안을 연구한다.

특히, 통신비밀자료제공 통계 분석 업무의 효율성 및 정확성 향상을 위한 분석프로그램을 업그레이드 하여 실제로 적용하고 이에 따른 보완사항을 검토하고 성능을 개선한다.

3. 연구의 구성 및 범위

본 과제의 연구 범위는 다음과 같다.

o 유·무선 IP 응용서비스상의 통신제한조치 기술동향 분석 및 해외사례 연구

- 국외 유·무선 IP 응용서비스 감청제도 수립 현황 분석
- 스마트폰 응용서비스 통신비밀 기술 동향 분석
- 유·무선 환경에서 SNS, 메신저, VoIP 서비스 감청방안 및 통신비밀보호방안 연구

o 통신비밀자료제공 통계 분석업무 개선

- 통계분석프로그램 기능 보완 및 개발
- 표준화된 프로그램의 통계분석업무 적용을 통해 관련 업무 개선 추진

4. 연구 내용 및 결과

본 과제의 연구 내용 및 결과를 정리하면 다음과 같다.

o 국내외 유·무선 IP 응용서비스 감청제도 수립 현황 분석

- 국회의 통신비밀보호법 개정 발의안을 중심으로 한 국내/국제 제도 수립 현황 분석
- 미국의 아동보호법 관련 제도 수립 현황 및 통비 이슈 분석
- 인터넷 서비스 감청 국제 표준화 현황 분석

o 스마트폰 응용 서비스 통신비밀 기술 동향 분석

- 스마트폰 위치정보 활용 현황 및 문제점 분석
- 데이터 압축 앱 응용 현황 및 통비 관련 이슈 분석
- 유·무선 환경에서 SNS, 메신저, VoIP 서비스 감청방안 및 통신비밀보호방안 분석

o 통신비밀자료제공 통계 분석업무 개선

- 통계분석프로그램 기능 보완 및 개발 완료
- 통계분석 도구 사용 가이드 개발
- 개발 도구의 통계분석업무 적용을 통한 업무 개선방안 분석

5. 정책적 활용 내용

IP 응용서비스상의 통신제한조치 기술동향 및 해외사례 연구 결과는, 통신비밀보호법 개정과 관련한 국내 통신비밀제도 수립 및 시행을 위한 기반 자료로 활용될 수 있다. 특히, 인터넷회선 감청, 전기통신사업자의 감청협조설비 구축, 위치정보의 통신비밀자료로의 활용, 전자우편의 감청, 통신비밀자료의 규제 등에 관한 정책 수립 및 이슈 검토에 당 연구결과가 활용될 수 있을 것으로 예상된다.

또한, 반기별로 전기통신사업자가 수사기관에 제공한 통신비밀자료 통계자료를 방송통신위원회에 보고하고, 방송통신위원회에서 이를 통계처리를 할 때, 당 과제에서 개발한 통신비밀자료제공 통계보고 툴을 활용하게 될 것으로 예상된다.

6. 기대효과

통신비밀보호법 개정과 관련하여 유무선 IP 응용서비스상의 통신제한조치 기술동향 분석 및 해외사례 연구를 통하여, 법률 개정 과정에서는 연구결과를 활용하여 국회 및 관계 부처의 관련 이슈 검토 시 신속하게 참고자료로 활용될 수 있으며, 궁극적으로 통신비밀보호법 개정에 따른 하위법률의 개정 및 제도 시행에 기여할 수 있을 것으로 기대된다.

또한, 당 과제에서 개발한 통신비밀자료제공 통계보고 툴은 통일된 포맷과 자동화된 입력 방식을 제공하고 있어, 통신비밀 통계 자료의 보고 및 취합 과정에서 정확성과 효율성을 높일 수 있을 것으로 기대된다.

SUMMARY

1. Title

Study on lawful interception policy and technology of IP applications

2. Objective and Importance of Research

The study on the lawful interception on SNS(Social Networking Service), mVOIP, and smart phone application is needed as with the increase of the SNS and smart phone users. In other words, there is an increase in the needs for conducting lawful interception on IP Internet line, assigning duty of constructing facilities for lawful interception to the Telcos and carriers, and law interception of e-mail. In accordance to this trends, multiple amendment on communication secrecy protection laws are initiated by the lawmakers to reform the current communication secrecy protection law in regulating the execution of the lawful interception and obligation of providing communication secrecy data.

The communication secrecy protection bills consists of regulation related to enforcing lawful interception such as on lawful interception on Internet line, assigning duty of constructing facilities for lawful interception to the Telcos and carriers, and law interception of e-mail and of obligation of providing communication secrecy data such as adding location information to the communication secrecy data and integrating communication secrecy data with communication data. Furthermore, analysis of the changes of the oversea's lawful interception regulation and understanding the technical trends of lawful interception on wired/wireless IP application service are needed in performing research to the lawful interception policies.

This project studies issues of reforming the communication secrecy protection law, of current status of the domestics and foreign lawful interception system, and of lawful interception technologies on smart phone, SNS, Messenger, VoIP service. This project also upgrade the current communication secrecy data statistics program to apply current lawful interception environments.

3. Contents and Scope of the Research

The scope of the scope of this project is follows.

- o Analysis of technologies of domestics and foreign lawful interception for wired/wireless IP application services
  - − analysis of a domestics and foreign lawful interception system for wired/wireless IP application services
  - − analysis of communication secrecy technology trends for application services of smart phone
  - − research in method of lawful interception and communication secrecy on SNS, messengers, and VoIP services in wired/wireless environment

- o Upgrade to the statistical report tool for collecting communication secrecy data
  - − functional upgrade to the statistical report tool for collecting communication secrecy data
  - − applying standardized statistical report tool for collecting communication secrecy data

4. Research Results

The result of this project is summarized as follows.

o Analysis of a domestics and foreign lawful interception system for wired/wireless IP application services

- analysis of a domestics and foreign lawful interception system based on issues of the communication secrecy protection bills currently pending in the national assembly
- analysis of children protection law and issues of lawful interception of US
- analysis of the international standardization status on lawful interception for Internet service

o analysis of technical trends of lawful interception for smart phone applications

- analysis of the problem and current status of location information features of smart phone
- analysis of issues related to lawful interception of data compression applications of smart phone
- analysis of lawful interception of SNS, messenger, VoIP and the method to protect communication secrecy in wired or wireless environment

o Upgrade to the statistical report tool for collecting communication secrecy data

- upgrading statistical report tool for collecting communication secrecy data
- development of statistical report tool usage guide
- applying standardized statistical report tool in collecting communication secrecy data

5. Policy Suggestions for Practical Use

The result of this projet can be used as a reference material in enforcing lawful interception and can be used as base material for establishment of the revised lawful interception system.

The result of this project can be used to develop policy on lawful interception of Internet-based services, construction of lawful interception cooperation facility, using location information to the communication secrecy data, lawful interception of e-mail, and restriction of data of lawful interception.

6. Expectations

The result of this project can be used as a reference in reviewing the issues are related to lawful interception and can contribute in enforcing of a lawful interception system and in reforming of rules and regulation of the communication secrecy protection law according to the amendment of the communication secrecy protection law.

The statistical report tool for collecting communication secrecy data developed by this project will provide unified format and automated input method in collecting communication secrecy data. It can enhance the accuracy and efficiency of conducting statistical analysis on the communication secrecy data report.

CONTENTS

Chapter 1. Introduction

Chapter 2. Study on the Lawful Interception

Chapter 3. Study on the Upgrade of Statistical analysis of Communication secrecy data

Chapter 4. Conclusion

References

제 1 장 서 론

제 1 절 연구의 필요성 및 목적

1. 연구의 필요성 및 목적

스마트폰 활성화와 함께 이용자가 급증하고 있는 SNS(Social Networking Service), mVoIP 등 유·무선 환경에서의 IP 응용서비스에 대한 통신제한조치 기술동향과 해외사례를 연구하여 국내 통신비밀보호제도 수립에 활용할 필요성이 있다.

- 스마트폰 이용자 수는 2010년 1월 103만 명에서 2010년 11월 625만 명으로 크게 증가하였으며, 이에 따라 스마트폰 환경에서의 통신제한조치 및 통신비밀보호에 관한 이슈가 부각되고 있다.

통신비밀자료제공 통계 분석 업무의 효율성 및 정확성 향상을 위한 분석프로그램을 실제로 적용하고 이에 따른 보완사항을 검토 및 조치할 필요가 있다.

이와 같은 필요성에 따라 아래와 같은 연구의 목적을 가지고 연구를 추진하였다.

o 유·무선 IP 응용서비스상의 통신제한조치 기술동향 분석 및 해외사례 연구

- 국외 유·무선 IP 응용서비스 감청제도 수립 현황 분석
- 스마트폰 응용서비스 통신비밀 기술 동향 분석
- 유·무선 환경에서 SNS, 메신저, VoIP 서비스 감청방안 및 통신비밀보호방안 연구

o 통신비밀자료제공 통계 분석업무 개선

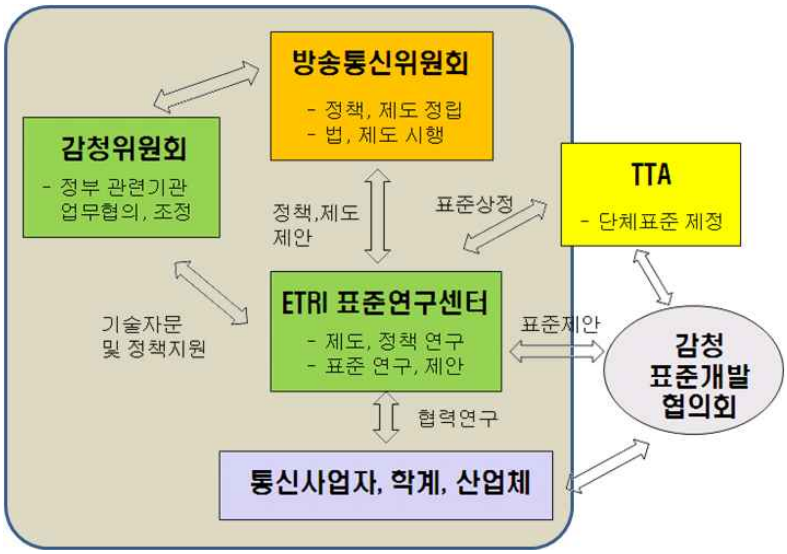
- 통계분석프로그램 기능 보완 및 개발
- 표준화된 프로그램의 통계분석업무 적용을 통해 관련 업무 개선 추진

2. 연구의 방법

국외 전기통신서비스 감청 및 통신비밀보호 제도 수립 및 시행 사례 분석을 바탕으로, 방송통신위원회, 전기통신사업자, 수사기관 등 관련 주체와의 협의를 통하여 국내 감청 제도 시행을 위한 방안을 수립하고 이를 통신비밀보호 관련 제도 수립 시 참고하였다.

전기통신서비스 감청 제도 정립 및 시행을 효율적으로 추진하기 위해 아래와 같은 추진체계를 구성하여 관련 기관이 상호 협력할 수 있도록 추진하였다.

[그림 1-1] 연구개발 추진체계



- 학계, 산업계 등과의 협력을 통하여 통신비밀보호 제도 수립 검토에 필요한 기술적 이슈 및 법률적 사항 검토하였다.

전기통신사업자 및 방송통신위원회와의 협력을 통하여 통신비밀자료 제공에 대한 통계자료 제출, 집계 및 분석에 관한 애로사항을 파악하고 이를 해결하기 위한 툴의 개발 및 적용하였다.

제 2 장 통신제한조치 연구

제 1 절 국내외 유무선 IP 응용서비스 감청제도 수립현황 분석

1. 통신비밀보호법 개정안 관련 조항 분석(법안중심)

현행 통신비밀보호법에서는 전기통신사업자에게 수사기관의 감청 집행에 협조하도록 규정하고 있으나, 감청 집행을 협조하기 위한 구체적인 요구사항 및 기술 조치에 관해서는 정하고 있지 않다. 따라서 단순한 협조만으로 감청이 가능한 유선전화서비스 및 이메일 서비스에 대해서만 주로 감청이 집행되고 있다. 그러나 이동전화 및 인터넷전화의 사용이 일반화되어 이들 서비스에 대한 감청 필요성이 제기되고 있으며, 미국, 캐나다, 독일, 영국, 프랑스, 네덜란드, 호주 등의 국가에서는 이동전화 및 인터넷전화 등의 서비스에 대한 감청을 집행하고 있다.

가. 이한성 의원 발의 통신비밀 보호법 일부개정안 분석

이한성 의원 대표로 발의된 통신비밀보호법 일부개정법률안(2008.10.30, 의안번호 1650)은 전기통신사업자에게 감청협조설비 구축의무를 부과하는 것을 주요 골자로 하고 있다. 더불어, 전기통신사업자의 감청협조설비 구축과 관련하여 감청협조설비 보안성 확보, 설비구축비용 보전, 기능 요구사항의 정의 등에 관한 사항들을 규정하고자 하고 있다.

<표 2-1> 이한성 의원 대표발의안 (감청협조설비 구축 의무화)

현 행	개 정 안
제15조의2(전기통신사업자의 협조의무) ①전기통신사업자는 검사·사법경찰관 또는 정보수사기관의 장이 이 법에 따라 집행하는 통신제한조치 및 통신사실 확인자료제공의 요청에 협조하여야 한다.	제15조의2(전기통신사업자등의 협조의무) ①전기통신사업자등은----------. ② 전화서비스를 제공하는 전기통신사업자, 그 밖에 대통령령으로 정하는 전기통신사업자는 이 법에 따른 검사·사법경찰관 또는 정보수사기관의 장의 통신제한조치 집행에 필요한 장비·시설·기술 및 기능을 갖추어야 한다.
②제1항의 규정에 따라 통신제한조치의 집행을 위하여 전기통신사업자가 협조할 사항, 통신사실 확인자료의 보관기간 그 밖에 전기통신사업자의 협조에 관하여 필요한 사항은 대통령령으로 정한다.	③ 제2항에 따른 장비·시설·기술 및 기능은 대통령령으로 정하는 기준·방법 및 절차에 적합하여야 한다.
<신 설>	④ 제2항에 따른 장비·시설·기술 및 기능의 구비에 소요되는 비용은 대통령령으로 정하는 바에 따라 국가가 그 전부 또는 일부를 부담한다.
<신 설>	⑤ 전기통신사업자는 제2항에 따른 장비 등을 운용함에 있어 권한 없는 자의 접근 방지, 접근기록의 관리 등 대통령령으로 정하는 바에 따른 보호조치를 취하여야 한다.
<신 설>	⑥ 전기통신사업자는 1년의 범위 안에서 대통령령으로 정하는 기간 동안 통신사실확인자료를 보관하여야 한다. 다만, 통신사실확인자료 중 위치정보에 대하여는 그러하지 아니하다.
<신 설>	⑦ 제1항부터 제6항까지에 규정된 사항 외에 통신제한조치의 집행 및 통신사실 확인자료 제공의 요청에 관하여 전기통신사업자등이 협조할 사항은 대통령령

<신 설>	으로 정한다. 제15조의3(이행강제금) ① 방송통신위원장은 제15조의2제2항을 위반하여 통신제한조치의 집행에 필요한 장비·시설·기술 및 기능을 갖추지 아니한 전기통신사업자에 대하여 1년 이내의 기간을 정하여 통신제한조치의 집행에 필요한 장비·시설·기술 및 기능의 구비의무를 이행할 것을 명할 수 있다. ② 방송통신위원장은 제1항에 따른 이행명령을 받은 전기통신사업자가 시정기간 내에 당해 시정명령을 이행하지 아니한 경우에는 10억원 이하의 범위 안에서 대통령령으로 정하는 금액의 이행강제금을 부과할 수 있다. ③ 제2항에 따른 이행강제금은 최초의 이행명령이 있은 날을 기준으로 하여 1년에 1회씩 그 이행명령이 이행될 때까지 반복하여 부과·징수할 수 있다. ④ 방송통신위원장은 제1항에 따른 이행명령을 받은 자가 이를 이행하는 경우에는 새로운 이행강제금의 부과를 중지하되, 이미 부과된 이행강제금은 징수하여야 한다. ⑤ 방송통신위원장은 제2항에 따른 이행강제금 부과처분을 받은 자가 이행강제금을 기한 내에 납부하지 아니하는 때에는 국세 체납처분의 예에 따라 징수한다. ⑥ 이행강제금의 부과·징수 등에 관하여 필요한 사항은 대통령령으로 정한다.

위 법률개정안에서는 전화서비스를 제공하는 전기통신사업자 등에게 감청에 필요한 장비 등의 구비의무를 부과하고자 한다(안 제15조의2제2

항). 다만 전기통신사업자 네트워크 및 관리시설 내부에 감청 설비가 구축됨에 따른 감청 오남용을 방지하기 위하여, 장비 등을 운용함에 있어 권한 없는 자의 접근 방비, 접근기록의 관리 등 보호조치를 취하도록 하고 있다(안 제15조의2제5항 신설). 기 설치된 전기통신 네트워크 장비에 감청 기능을 추가하거나 별도의 감청 설비를 구축하기 위해서는 적지 않은 비용이 소요될 것으로 예상되는데, 이와 같이 감청협조를 위한 장비 등의 구비에 소요되는 비용은 국가가 전부 또는 일부를 부담하도록 하고 있다(안 제15조의2제4항 신설). 법률개정안의 시행과 관련하여, 감청기술 표준 개발, 감청설비의 개발, 시험 및 도입 등에 소요되는 시간을 고려하여, 이동전화사업자는 이 법 시행 후 2년 내에, 그 밖의 전기통신사업자는 4년 내에 장비 등을 구비해야 하며, 정당한 사유가 있는 경우 방송통신위원장에게 신청하여 기간을 연장할 수 있도록 하고 있다(부칙 신설). 이 때, 방송통신위원장은 신청에 대하여 정당한 이유가 있을 경우 기간을 연장할 수 있으며, 법무부장관 등 관계 기관의 장과 미리 협의하도록 하고 있다. 위 개정안의 내용을 간략하게 표로 정리하면 다음과 같다.

<표 2-2> 이한성 의원 대표발의안 요약 (감청협조설비 구축 의무화)

	현행	개정안
감청협조설비 구축의무	o 협조의무 내용 대통령령 위임	o 전기통신사업자에게 감청협조설비 구축 의무 부과 (안 제15조의2제2항)
감청설비 능력요구사항	-	o 대통령령으로 정하는 능력요구사항 준수 (안 제15조의2제3항 신설)
감청설비 오남용 방지	-	o 감청협조설비 보호조치 요구 (안 제15조의2제5항 신설)
설비구축비용	-	o 국가가 전부 또는 일부 부담 (안 제15조의2제4항 신설)

이행강제금	-	o 1년에 1회 10억원 이하 (안 제15조의3 제2항 및 제3항 신설)
협조설비구축 유예기간	-	o 이동전화사업자/기타전기통신사업자: 각각 법 시행 후 2년/4년 이내 (부칙 제4조제1항~제3항 신설)
신고 포상금	-	o 국가기관 또는 통신기관의 불법감청 신고 시 포상금 지급 (안 제15조의4 신설)

나. 최문순의원 발의 통신비밀보호법 개정안 분석

o 본 법안은 전기통신사업법 상의 “통신자료”에 대한 내용을 통신비밀보호법으로 옮겨 규정하고자 하며, 법원, 검사 또는 수사관서의 장, 정보수사기관의 장은 재판, 수사, 형의 집행 또는 국가안전보장에 대한 위해를 방지하기 위한 정보 수집을 위하여 필요한 경우 전기통신사업자에게 통신자료제공을 요청할 수 있도록 함 (안 제13조의5 신설)

※ 현행 전기통신사업법 제54조제3항 이관

o 검사수사기관의 장은 공소를 제기하거나, 공소의 제기 또는 입건을 하지 아니하는 처분을 한 날부터 30일 이내에, 정보수사기관의 장은 통신자료제공을 받은 날부터 30일 이내에 대상 가입자에게 통신자료제공을 받은 사실을 알리도록 함 (안 제13조의6 신설)

o 통신사실확인자료 제공 및 통신자료 제공에 관한 통지를 하지 아니한 자는 3년 이하의 징역 혹은 1천만 원 이하의 벌금에 처하도록 함 (안 제17조제2항제3호)

<표 2-3> 최순문의원 개정안 요약

	현행	개정안
통신자료 제공 규정	o 전기통신사업법에서 규제	o통신비밀보호법에서 규제
통신자료 제공 통지	o 통지규정 없음	o 수사기관이 30일 이내에 통지 o 통지하지 않을 경우 처벌

다. 이정현 의원 발의 법안 분석

1) 통신자료 규제 관련 법안

o 법안의 주요 내용

- 전기통신사업법 상의 “통신자료”를 통신비밀보호법의 규율대상으로 이관하여, 통신사실확인자료와 동일하게 규정하고자 한다.
- 전기통신사업법 상의 “통신자료”를 통신비밀보호법에서 “가입자정보”로 정의하고, 통신사실확인자료와 가입자정보를 묶어서 “통신자료”로 정의한다. (안 제2조 및 제13조)
- 검사 또는 사법경찰관은 수사 또는 형의 집행을 위하여 필요한 경우 법원의 허가를 받아 전기통신사업자에게 가입자정보의 제공을 요청할 수 있도록 한다(안 제13조)
- 정보수사기관의 장은 국가안전보장에 대한 위해를 방지하기 위하여 정보수집이 필요한 경우 고등법원 수석부장판사의 허가 또는 대통령의 승인을 받아 전기통신사업자에게 가입자정보의 제공을 요청할 수 있도록 한다 (안 제13조의4)
- 검사사법경찰관은 공소를 제기하거나, 공소의 제기 또는 입건을

하지 아니하는 처분을 한 날부터 30일 이내에, 정보수사기관의 장은 가입자정보를 받은 날부터 30일 이내에 대상 가입자에게 가입자정보를 제공받은 사실을 서면 통지하도록 한다 (안 제13조의3 및 제13조의4)

<표 2-4> 이정현 의원 발의법안 요약

	현행	개정안
통신자료 규제	o 전기통신사업법 규제	o 통신비밀보호법 규제 o “가입자 정보”로 명칭 변경
통신자료 요청 근거	o 수사기관의 장 등이 전기통신사업자에 요청서 제출	o 검사/사법경찰관: 법원의 허가 o 정보수사기관의 장: 고등법원 수석부장판사 허가/대통령 승인
통신자료 제공 통지	o 통지규정 없음	o 30일 이내에 수사기관 등이 서면통지

o 해외사례

<표 2-5> 이정현 의원 발의법안 관련 해외 사례 요약

국가명	근거법령	규정	비고
미국	ECPA	o 가입자정보 및 통신서비스 이용정보 통합 규정	o DP 대상에 이름, 주소, 전화번호 및 서비스 이용정보 포함
유럽	EU Directive 2006/24/EC	o 가입자정보 및 통신서비스 이용정보 통합 규정	o Directive에서 보관하도록 하는 데이터가 이름, 주소, 전화번호, 서비스 이용 시간 등의 서비스 이용정보 포함

독일	-	-	o 연방헌법재판소에서 통신사실확인자료 보관 의무의 위헌성을 인정하여 효력정지 가처분 명령을 내린 상태
일본	-	-	o 관련 규정 없는 것으로 파악됨

미국, 유럽 등에서는 통신자료와 통신사실확인자료를 통합하여 규제하고 있는 것으로 파악됨

- 미국의 DP 제도에서 보관 대상인 데이터는 이름, 주소, 전화연결 기록, 서비스 시간, 이용한 서비스의 종류 등 통신자료와 통신사실확인자료를 모두 포함

  ※ 통신자료 및 통신사실확인자료 외에 서비스 비용 지불 방법 (신용카드 번호 및 은행 계좌번호) 정보 또한 DP의 대상에 해당됨

- 유럽의 DR Directive에서 정하고 있는 보관 데이터는 통신 발신지, 통신 착신지, 통신 시간, 통신종류, 이동통신장비의 위치 등을 식별하기 위한 데이터로 통신자료와 통신사실확인자료 모두 포함

2) 통신제한조치의 기간 및 연장 규정

본 법안은 통신제한조치의 기간을 단축하고 그 연장횟수를 제한한다. (안 제6조제7항 및 제7조제2항)

<표 2-6> 통신제한조치 관련 개정안 요약

	현행	개정안
통신제한조치 기간, 연장 청구기간 및 횟수	o 기간: 2개월 o 연장 청구기간: 2개월 o 연장 청구횟수: 규정 없음	o 기간: 1개월 o 연장 청구기간: 1개월 o 연장 청구횟수: 2회
국가안보를 위한 통신제한조치	o 기간: 4개월 o 연장 청구기간: 4개월 o 연장 청구횟수: 규정 없음	o 기간: 2개월 o 연장 청구기간: 2개월 o 연장 청구횟수: 규정 없음

o 통신제한조치의 기간연장에 대한 관계기관 입장

- 시민단체: 감청기간 연장에 대한 횟수를 제한하는 것은 매우 시급한 일이며, 법률 개정에 찬성함
- 시민단체: 감청기간은 기본 10일 및 최대 30일까지 연장 가능한 수준의 규정이 적절한 것으로 생각됨

o 해외사례

<표 2-7> 통신제한조치의 기간에 대한 해외사례

국가명	근거법령	감청기간	연장기간	비고
미국	종합범죄방지 및 가로안전법 (수사)	o 최대 30일	o 최대 30일	제2518조 제5항
	대외정보감시법 (안보)	o 내국인 포함: 최대 90일 o 외국인: 최대 1년	o 내국인 포함: 최대 90일 o 외국인: 최대 1년	제1805조
영국	수사권규율법	o 3개월	o 3개월 o 국가의 안보와 경제 번영 보장을 위한 경우 6개월 연장 가능	제9조 제6항

프랑스	전기·전자통신의 비밀에 관한 법률	o 4개월	o 4개월	제100-2조
일본	통신방수법	o 최대 10일 (제5조제1항)	o 최대 10일 (제7조제1항) o 감청 기간은 총 30일을 초과하지 못함 (제7조제1항)	-
독일	서신, 우편 및 전기통신 비밀 제한에 관한 법률	o 3개월	o 매회 최대 3개월 o 기간연장 횟수에 관한 규정은 없는 것으로 파악됨	제10조 제5항

- 미국, 영국, 프랑스, 일본 등에서는 총 연장기간에 대한 제한을 두고 있으며, 연장기간은 주로 초기 감청기간과 비슷한 수준으로 정하고 있음

- 독일에서는 감청 연장 기간을 1회당 3개월로 제한하고 있으며, 기간 연장 횟수에 관한 별도의 규정은 없는 것으로 파악됨

3) 통신제한조치 대상자의 감청내용 열람

o 법안 주요 내용

- 통신제한조치 대상자가 집행 사실을 알게 된 경우에는 대통령령으로 정하는 바에 따라 검사·사법경찰관 또는 정보수사기관의 장에게 해당 통신제한조치로 알게 된 내용의 열람 또는 복사를 요청할 수 있도록 함 (안 제9조의2제7항 신설)

o 해외사례

<표 2-8> 통신제한조치 대상자의 감청내용 열람 관련 해외사례

국가명	근거법령	규정	비고
미국	-	o 현재까지 관련규정 파악된 바 없음	-
영국	-	o 현재까지 관련규정 파악된 바 없음	-
프랑스	-	o 현재까지 관련규정 파악된 바 없음	-
독일	-	o 현재까지 관련규정 파악된 바 없음	-
일본	통신방수법	o 감청내용 청취, 열람 및 복제 신청 가능	o 정당한 이유가 있을 경우 판사가 허가

4) 통신제한조치로 취득한 내용의 폐기관련 법안

o 법안 주요 내용

- 통신제한조치 집행으로 취득된 우편물 또는 전기통신의 내용 중 통신제한조치허가서 또는 긴급감청서에 기재되지 않은 내용 등이 포함되어 있거나 범죄수사·소추의 목적 등에 더 이상 필요하지 않을 경우 이를 폐기하도록 함 (안 제12조제2항 신설)
- 그 경위 및 결과의 요지를 조서로 작성하도록 함 (안 제12조제3항 신설)
- 제12조제2항 또는 제3항을 위반한 경우 3년 이하의 징역 또는 1천만원 이하의 벌금에 처함 (안 제17조제2항제4호 신설)

<표 2-9> 감청내용 폐기에 관한 개정안 요약

	현행	개정안
감청내용 폐기	o 규정 없음	o 허가서 등에 기재되지 않은 내용 o 범죄수사 등에 더 이상 필요하지 않을 경우

o 해외사례

<표 2-10>감청내용 폐기에 관한 국외 사례

국가명	근거법령		감청내용 폐기 규정	비고
미국	종합범죄방지 및 가로안전법		o 판사 명령 하에서만 폐기 가능 o 10년 이상 보존	o 허가받지 않은 감청 내용에 대한 규정 없음
	대외정보감시법		o 우연히 취득된 무선통신내용	-
영국	수사권규율법		o 현재까지 관련규정 파악된 바 없음	o 감청내용 사본은 더 이상 필요하지 않을 경우 즉시 폐기해야 함
프랑스	전기·전자 통신의 비밀에 관한 법률	일반	o 공소시효 기간 경과 후, 수사기관의 청구에 의하여 폐기	o 폐기에 대한 보고서 작성
		국가안보	o 녹음 10일 경과 후 수상의 지시에 따라 폐기	o 폐기에 대한 보고서 작성
일본	통신방수법		o 다음 중 더 늦은 날까지 보관 - 제출일로부터 5년경과 - 사건 종결일로부터 6개월경과	o 보관기간 연장 가능

라. 변재일 의원 발의 법안 분석

1) 통신제한조치 요건 규정

o 법안 주요 내용

통신제한조치의 허가에 있어서 청구이유가 제5조제1항의 허가요건을 모두 충족하고 있고 다른 방법으로는 그 범죄의 실행을 저지하

거나 범인의 체포 또는 증거의 수집이 어렵다는 구체적인 증거가 포함된 소명자료를 첨부하도록 함 (안 제6조제4항)

o 해외사례

<표 2-11> 통신제한조치 요건에 대한 해외 사례

국가명	근거법령	규정	비고
미국	종합범죄방지 및 가로안전법	o 범죄의 실행 또는 범죄를 실행하기 위한 계획에 대한 증거를 제시할 수 있거나 제시하였을 경우 감청 허용 o 감청 신청서에 “다른 수사 절차가 시도되어 실패한 적이 있는지 여부와 그러한 걸차가 시도되더라도 성공하기 어렵다든지 또는 너무 위험한 것으로 판단하는 이유에 관한 충분하고 완전한 기술”을 포함하도록 하고 있음[1]	
영국	수사권규율법	o 소속장관이 감청영장을 발부 할 때 다음을 고려하도록 하고 있음 - 국가안보, 중대한 범죄의 예방 및 탐지 등을 위하여 영장이 필요하고, 감청의 그 목적 달성에의 적합성 - 영장에 따라 수집되어야 할 필요가 있다고 생각되는 정보가 다른 합법적 방법으로 수집될 수 있는지의 여부 o 감청 신청서에 감청 외의 방법으로 정보 취득이 어려운 사유를 별도로 명시하도록 하는 규정은 파악되지 않음	
프랑스	전기·전자통신의 비밀에 관한 법률	o 감청 신청서에 감청 외의 방법으로 정보 취득이 어려운 사유를 별도로 명시하도록 하는 규정은 없는 것으로 파악됨	
일본	통신방수법	o 다른 방법에 의하여서는 범인을 특별히 지정하거나 범행의 상황 또는 내용을 밝히는 것이 현저히 곤란할 때에는	제3조 제1항

		판사가 발부하는 감청영장에 의하여 감청할 수 있음 o 감청 신청서에 감청 외의 방법으로 정보 취득이 어려운 사유를 별도로 명시하도록 하는 규정은 파악되지 않음	
독일	서신, 우편 및 전기통신 비밀 제한에 관한 법률	o 감청처분은 사실관계 확인이 다른 방법으로는 불가능하거나 매우 곤란할 경우에만 할 수 있도록 규정 o 사실관계 확인이 다른 방법으로는 불가능하거나 매우 곤란할 것임을 신청서에 설명해야 함	

2) 통신제한조치 기간 단축

o 법안 주요 내용

– 통신제한조치의 기간을 최대 2개월에서 1개월로, 연장 청구 기간을 최대 2개월에서 1개월로, 국가안보를 위한 통신제한조치의 기간을 최대 4개월에서 2개월로 각각 단축함 (안 제6조 및 제7조)

o 해외사례 (이정현 의원안에서와 동일)

1) 이 밖에도 동법 제2518호 “유선통신, 대화 또는 전자통신의 감청 절차”에서는 감청 신청서에 포함되어야 하는 정보에 관하여 규정하고 있다.

<표 2-12> 통신제한조치의 기간에 대한 해외사례

국가명	근거법령	감청기간	연장기간	비고
미국	종합범죄방지 및 가로안전법 (수사)	o 최대 30일	o 최대 30일	제2518조 제5항
	대외정보감시법 (안보)	o 내국인 포함: 최대 90일 o 외국인: 최대 1년	o 내국인 포함: 최대 90일 o 외국인: 최대 1년	제1805조

국가명	근거법령	감청기간	연장기간	비고
영국	수사권규율법	o 3개월	o 3개월 o 국가의 안보와 경제 번영 보장을 위한 경우 6개월 연장 가능	제9조 제6항
프랑스	전기·전자통신의 비밀에 관한 법률	o 4개월	o 4개월	제100-2조
일본	통신방수법	o 최대 10일 (제5조제1항)	o 최대 10일 (제7조제1항) o 감청 기간은 총 30일을 초과하지 못함 (제7조제1항)	-
독일	서신, 우편 및 전기통신 비밀제한에 관한 법률	o 3개월	o 매회 최대 3개월 o 기간연장 횟수에 관한 규정은 없는 것으로 파악됨	제10조 제5항

3) 긴급통신제한조치 법원 허가 취득 시간 규정

o 법안 주요 내용

- 긴급통신제한조치 중 지체 없이 법원의 허가를 받도록 하는 것을 24시간 이내로 명시하고, 긴급통신제한조치 가능 시간을 36시간을 24시간으로 축소 (안 제8조제2항)

o 관계기관 입장

o 법무부

- 긴급통신제한조치가 36시간 내에 종료되어 법원의 허가가 필요 없는 경우에도 검사의 승인을 받도록 되어 있고, 긴급통신제한조치 대장 관리가 이루어지고 있으므로 남용 우려가 없음
- 실제로 수사기관에 의해서 이루어지는 긴급통신제한조치 집행 건수는 2006년 12건, 2007년 15건, 2008년 4건에 불과함 (국정원 건수 제외)

o 야당, 시민단체

- 시민단체: 현재 36시간까지 법원의 허가 없이 감청할 수 있도록 하는 긴급감청 제도는 수사기관의 편의를 위해 국민의 기본권을 제한하는 제도로서 삭제되어야 함

o 해외사례

<표 2-13> 긴급감청 신청기한 등의 해외사례

국가명	근거법령	긴급감청 신청기한	긴급감청 종료 요건
미국	종합범죄방지 및 가로안전법	o 48시간 내 신청	o 목적한 통신 감청 o 명령신청 기각
	대외정보감시법	o 법무장관 승인 하에 긴급감청 가능 o 72시간 내 판사 신청	o 목적한 통신 감청, o 명령신청 기각, o 72시간, 중 가장 빠른 시기
영국	-	o 관련규정 파악된 바 없음	-
프랑스	-	o 관련규정 파악된 바 없음	-

독일	서신, 우편 및 전기통신 비밀 제한에 관한 법률	o 의회 감독기구 위원장 또는 대리인의 동의하에 긴급감청 가능 o 지체 없이 의회 감독기구의 동의 추완 필요	o 2주 후
일본	-	o 관련규정 파악된 바 없음	-

4) 통신사실확인자료 제공 절차 강화 법안

o 주요 내용

통신사실확인자료 제공의 남발을 막기 위해 절차를 강화함 (안 제13조제2항)

- 범죄수사를 위한 통신사실확인자료 요청의 경우 각 피의자별로 하도록 하였으며 다수의 가입자에 대해서 요청하는 경우 1건의 허가 요청서에 의하지 못하도록 함
- 통신사실확인자료 제공요청의 경우 예외 없이 법원의 허가를 먼저 얻은 후 하도록 함
- 통신사실확인자료 제공을 한 기관 및 중앙행정기관 등은 상임위원회 등의 요구가 있는 경우 국회에 확인자료제공현황보고서를 제출하도록 함 (안 제15조제5항 신설)

<표 2-14> 통신사실확인자료 제공절차 강화 법안 요약

	현행	개정안
요청사유 기재	o 요청사유 기재 (제13조제2항)	o 각 피의자별 또는 내사자별로 요청사유 기재 o 각 가입자당 1건의 허가요청서
긴급요청	o 긴급요청 가능 (제13조제2항)	o 허가 없는 긴급요청 불가(긴급요청 관련 내용 삭제)

o 관계기관 입장

o 야당, 시민단체

- 시민단체: 통신사실확인자료의 경우 "필요한 경우" 요청할 수 있도록 하여 오남용 소지가 높으므로, "피의자가 죄를 범하였다고 의심할 만한 상당한 이유가 있고, 수사 또는 형의 집행을 위하여 필요한 경우"로 명확히 명시해야 함
- 시민단체: 법원에 허가를 요청할 때 해당 피의자의 범죄혐의를 소명할 자료 등을 상세히 제출하도록 해야 함

마. 이학재 의원 발의 법안 분석

o 법안 주요 내용

- 현행 통신비밀보호법은 송·수신이 완료된 전자우편에 대한 압수·수색과 관련한 규정을 두고 있지 않아, 형사소송법상의 압수·수색에 관한 규정에 의해 집행되고 있음

- 송·수신이 완료된 전자우편을 통신비밀보호법 상 “전기통신”에 포함시켜 포털회사 등의 서버에 저장되어 있는 개인의 전자우편에 대한 보호수준을 강화하고자 함
- 전기통신의 정의에 송·수신이 완료된 전자우편을 포함시킴 (안 제2조제3호)
- 송·수신이 완료된 전자우편에 대한 수사 등에 관하여는 형사소송법에 우선하여 적용하도록 함 (안 제4조의2 신설)
- 송·수신이 완료된 전자우편에 대한 긴급통신제한조치(E-mail 감청)을 한 경우 법원의 허가를 받지 못하거나 대통령의 승인을 받지 못하면 이를 즉시 폐기하도록 함(안 제8조제2항 및 제9항)

o 관계기관 입장

o 야당, 시민단체

- 시민단체: 개정 방향에는 찬성하나, 다음과 같은 보완이 필요한 것으로 의견을 밝힘
  · 전기통신의 범위에 송수신이 완료된 이메일 뿐 아니라, 휴대폰 문자메시지, 음성사서함, 비공개 게시판의 게시물 등 현대적 매체에 의한 통신 결과물을 포함시킬 필요가 있음
  · 통지주체와 시기, 통지유예제도 등 통비법 상의 통지제도의 문제점을 개선해야만 이 개정안의 취지를 살릴 수 있음
  · 통신제한조치로 취득한 이메일이 범죄혐의와 관련이 없으면 수사기관이 이를 즉시 폐기할 것과, 폐기하였음을 정보주체에 통지할 것을 의무화함으로서 사생활 침해를 최소화할 필요가 있음.

o 해외사례

<표 2-15> 전자유편 감청에 대한 해외사례

국가명	근거법령	관련 규정	비고
미국	종합범죄방지 및 가로안전법	o 전자우편을 전자통신[2]의 일부로 해석 ➔ 통신제한조치의 일환으로 규제	-
영국	수사권규율법	o 전자우편을 공공전기통신서비스[3]의 일부로 해석 ➔ 통신제한조치의 일환으로 규제	-
프랑스	전기·전자통신의 비밀에 관한 법률	o 전자우편을 전기통신[4]의 일부로 해석 ➔ 통신제한조치의 일환으로 규제	-
일본	통신방수법	(법의 해석이 어려움)[5]	-
독일	서신, 우편 및 전기통신 비밀제한에 관한 법률	o 전자우편을 전기통신서비스[6]의 일부로 해석 ➔ 통신제한조치의 일환으로 규제	-

2) "전자통신"이란 주간 또는 해외 거래에 영향을 미치는 유선, 무선, 전자기, 광전자 또는 광학시스템에 의하여 전체적으로 또는 부분적으로 전송되는 모든 종류의 부호, 신호, 문언, 영상, 음향, 데이터 또는 정보 전달을 의미

3) "공공전기통신서비스"란 영국의 하나 이상의 지역에서 특정한 구역 또는 대중에게 제공되는 전기통신시스템을 의미한다. 이 때 "전기통신시스템"이란 전기 또는 전자기 에너지의 사용을 포함하는 수단에 의하여 통신의 전송을 용이하게 할 목적으로 존재하는 시스템을 의미한다.

4) Telecommunications: any form of transmission, emission or reception of signs, signals, text, images, sound or other information, by wire, optical fiber, radio or other electromagnetic means

5) "통신"이라 함은 전화 기타 전기통신으로서 그 전송로의 전부 또는 일부가 유선(유선 이외의 방식으로 전파 기타 전자파를 송수신하기 위한 전기적 설비에 부속되는 유선을 제외한다)인 것 또는 그 전송로에 교환기 설비가 있는 것을 말한다.

미국, 영국, 독일, 프랑스 등의 경우 전자우편을 전자통신의 한 종류로 보고 그에 대한 압수수색을 통신제한조치의 일환으로 규제하고 있음[7)]

바. 박준선의원 발의 법안 분석

o 법안 주요 내용

- 2010년 12월 28일 헌법재판소는 통신비밀보호법 제6조 제7항 단서 중 '통신제한조치기간의 연장' 관련하여 총연장기간 또는 총연장횟수의 제한 없이 통신제한조치기간을 연장할 수 있도록 규정한 것에 대해 헌법불합치 결정을 하였음(2011. 12. 31.까지 개정 안될 경우 효력 상실).

- 본 법안은 통신제한조치의 총 연장기간을 1년으로 제한하여 수사상 통신제한조치의 필요성과 통신의 비밀 등 국민의 기본권이 적절히 조화를 이루도록 하려는 것임

o 관계기관 입장

- 시민단체: 감청기간 연장에 대한 횟수를 제한하는 것은 매우 시급한 일이며, 법률 개정에 찬성함
- 시민단체: 감청기간은 기본 10일 및 최대 30일까지 연장 가능한 수준의 규정이 적절한 것으로 생각됨

---

6) Telecommunications service means services normally provided for remuneration consisting in, or having as their principal feature, the conveyance of signals by means of telecommunications networks, and includes transmission services in networks used for broadcasting

7) 김성천 교수 (중앙대) 작성 자료 참고

o 해외사례

– 미국, 영국, 프랑스, 일본 등에서는 총 연장기간에 대한 제한을 두고 있으며, 연장기간은 주로 초기 감청기간과 비슷한 수준으로 정하고 있음

o 독일에서는 감청 연장 기간을 1회당 3개월로 제한하고 있으며, 기간연장 횟수에 관한 별도의 규정은 없는 것으로 파악됨

<표 2-16> 감청기간 연장에 대한 해외사례

국가명	근거법령	감청기간	연장기간	비고
미국	종합범죄방지 및 가로안전법 (수사)	o 최대 30일	o 최대 30일	제2518조 제5항
	대외정보감시법 (안보)	o 내국인 포함: 최대 90일 o 외국인: 최대 1년	o 내국인 포함: 최대 90일 o 외국인: 최대 1년	제1805조
영국	수사권규율법	o 3개월	o 3개월 o 국가의 안보와 경제 번영 보장을 위한 경우 6개월 연장 가능	제9조 제6항
프랑스	전기·전자통신의 비밀에 관한 법률	o 4개월	o 4개월	제100-2조
일본	통신방수법	o 최대 10일 (제5조제1항)	o 최대 10일 (제7조제1항) o 감청 기간은 총 30일을 초과하지 못함 (제7조제1항)	-

독일	서신, 우편 및 전기통신 비밀 제한에 관한 법률	o 3개월	o 매회 최대 3개월 o 기간연장 횟수에 관한 규정은 없는 것으로 파악됨	제10조 제5항

사. 김태원 의원발의 법안 분석

o 법안 주요 내용

- 자살위험자 행방 조사를 위한 통신사실 확인자료 제공의 절차 규정을 통신비밀 보호법 제13조5항에 신설함
- 제13조의5(자살위험자 행방 조사를 위한 통신사실 확인자료제공의 절차 등)

① 검사 또는 사법경찰관은 배우자, 2촌 이내의 친족 또는 「민법」 제928조에 따른 후견인으로부터 자살위험자(「자살예방 및 생명존중문화 조성을 위한 법률」 제4조의 자살위험자를 의미한다)로 가출·실종 신고된 사람의 행방을 조사하는 데에 있어 그 신고자의 요청에 따라 필요한 경우 전기통신사업자에게 통신사실 확인자료제공을 요청할 수 있다.

② 제13조는 통신사실 확인자료제공의 절차에 관하여 이를 준용한다.

③ 검사 또는 사법경찰관은 통신사실 확인자료제공을 받은 사건에 관하여 조사를 종결한 때에는 그 처분을 한 날부터 30일 이내에 그 대상이 된 전기통신의 가입자에게 통신사실 확인자료제공을 받은 사실과 제공요청기관 및 그 기간 등을 서면으로 통지하여야 한다. 다만, 그 가입자가 생존하지 아니한 경우에는 그러하지 아니하다.

아. 정옥임 의원 발의 법안 분석

o 법안 주요 내용

- 증권선물위원회로 하여금 금융범죄수사를 위한 통신사실 확인자료 수집 청구를 허용하도록 하여 불공정거래 등 범죄에 효과적으로 대처하도록 하려는 것임(안 제13조의5 신설 및 제13조의6 개정).
- 제13조의5(불공정거래수사를 위한 통신사실 확인자료제공의 절차 등) ①증권선물위원회는 「자본시장과 금융투자업에 관한 법률」 제427조의 조사를 위하여 정보수집이 필요한 경우 전기통신사업자에게 통신사실 확인자료제공을 요청할 수 있다.

  ②제7조 내지 제9조 및 제9조의2제3항·제4항·제6항의 규정은 제1항의 규정에 의한 통신사실 확인자료제공의 절차 등에 관하여 이를 준용한다. 이 경우 “통신제한조치”는 “통신사실 확인자료제공 요청”으로 본다.

  ③제13조제3항 및 제5항의 규정은 통신사실확인자료의 폐기 및 관련 자료의 비치에 관하여 이를 준용한다.

2. 미국의 아동보호법 관련 제도 수립 현황 및 관련 통비 이슈 분석

가. 인터넷 포르노로부터의 아동보호법

인터넷 포르노로부터의 아동보호법(Protecting Children From Internet Pornographers Act of 2011)”은 스미스 법안 이라고 불리는데, 인터넷의 포르노물로부터 아동을 보호하기 위하여 제정되었다.(2011년 6월28일 최종수정된 법률) 이 법률은 온라인 아동 포르노 유통자 들과 이용자들에 대한 수사를 위해 ISP 들의 도움이 현실적으로 필요하며, ISP 들이

가입자 들의 기록(통신기록)을 유지(Retain)할 필요성이 있기 때문에 이의 강제를 위해 법이 제정되었다. 물론, 이때 저장된 로그데이터는 다른 유형의 범죄를 조사하는데도 사용 될 수 있다. 이 법률은 ISP 들이 고객에게 서비스를 제공하기 위해 고객에게 임시로 할당되는 네트워크 주소를 최소 18개월간 유지(retain)할 것을 요구하고 있으며, 주소 정보가 무선 통신에 의해 전송되지 않는 경우 데이터 유지를 규정하고 있다. 이 법안은 집행 기관이 범죄를 찾아내고 기소하기 위해 필요한 도구를 제공하게 될 것으로 판단된다.

나. 무선 사업자에 대한 면제 허용

아동보호법은 무선 서비스 제공사업자 들은 인터넷 회사들로 하여금 고객 데이터의 로그를 요구하는 새로운 법안에 명시되어 있는 광범위한 요구사항 들을 준수할 필요가 없다고 CNET이 보도하였다. 이는 무선 사업자 들의 네트워크는 IP 주소를 복수의 이용자 또는 계정에 할당하도록 설계되어 있으므로, 법 집행 기관이 요구하는 유형의 데이터를 유지하기가 기술적으로 가능하지 않기 때문에 법안에 대해 면제한다는 익명의 의견이 있었다. 이는, 무선 사업자 들의 로비에 의한 결과로 보이며, 본 규제를 준수해야 할 대상인 케이블 및 DSL 제공자 들로 부터 강한 반대가 있을 것으로 보여진다. 미국 법무부에서는 이러한 무선사업자에 대한 면제를 허용하는 것에 대하여 반대 의견 표명하였으며, 법무부는 수사를 위해 무선 인터넷 사업자 들도 고객에 대한 로그 데이터를 유지하여야 한다고 요구하고 있다. 무선사업자에 대한 면제허용은 데이터 유지(Retention)에 대한 논의와 함께 향후 논란이 예상되고 있다.

다. 유지(Retention)“ 대 "보존(preservation)“

1996년에 전자통신 트랜젝션 기록법(Electronic Communication Transactional Records Act)이라고 부르는 연방법이 데이터 보존(Preservation)을 법규화 하고 있으며, ISP 들은 네트워크 모니터링, 사기 예방, 요금 분쟁 등과 같은 비즈니스 목적을 위해 더 이상 요구되지 않는 모든 가입자 로그 파일 들을 삭제하고 있다. 그러나 전자통신트랙젝션 기록법에 의하면 ISP 들이 정부 기관의 요청이 있을 경우, ISP가 보유하고 있는 기록 들을 90일간 유지할 것을 요구하고 있다(Preservation)

“아동 보호법 2008“에서는 아동 포르노 전송에 관한 실제 정보를 얻는 ISP 들은 이러한 사실이나 상황 정보를 보고할 것을 요구하고 있으며, 이러한 요구사항을 고의적으로 준수하지 않는 기업은 처음 위반에 대해 15만 달러의 벌금을, 그리고 후속 위반에 대해서는 각 위반에 대해 30만 달러 까지의 벌금이 부과될 수 있다.

유럽연합은 Data Retention을 제도화하여 시행하고 있으나, 미국은 아직 Data Preservation 제도만이 시행되고 있는 상황인 것으로 파악되고 있다.

라. 인터넷 포르노로부터 아동보호법 관련 기사 번역 전문

무선 서비스 제공사업자 들은 인터넷 회사들로 하여금 고객 데이터의 로그를 요구하는 새로운 법안에 명시되어 있는 광범위한 요구사항 들을 준수할 필요가 없다.

CNET은 몇 주 전에 한 기사에서 무선 통신사업자들에 대한 이러한 면제를 처음으로 보고하였다. 이 법안은 하원 법사위원회 위원장인 미국 공화당의 라마 스미스(공화당, 텍사스)와 데비 와서맨 슐츠(민주당)에 의해 오늘 발표되었다.

이는 새로운 정부의 명령을 준수하고 싶어 하지 않는 무선 사업자들의 로비의 결과로 보인다. 그러나 이러한 면제는 이미 미국 법무부의 분노를 자아냈으며, 규제를 준수해야 할 케이블 및 DSL 제공자들로 부터의 강한 반대가 있을 것으로 보인다. 무선무역협회인 CTIA는 오늘 코멘트 요청에 응하지 않았지만, 이전에 대변인을 통해 이 법안과 관련해 위원회와 협력할 것이라고 밝힌 바 있다.

수사관 들이 온라인 아동 포르노 유통자들과 이용자들을 식별하기 위해 ISP 들의 도움을 필요로 한다고 스미스는 오늘 성명에서 말했다. 이 법안은 법 집행 관계자 들이 아동 성 착취에 대항해 싸울 수 있도록 도와주기 위해 전화 회사에 의한 기록 유지와 유사하게 ISP 들이 가입자들의 기록(통신기록)을 유지할 것을 요구한다. 그렇지만 로그 데이터는 어떤 유형의 범죄를 조사하는데 사용될 수 있다.

익명을 요구한 하원 법사위원회의 공화당 보좌관은 무선 사업자들의 네트워크는 IP 주소를 복수의 이용자 또는 계정에 할당하도록 설계되어 있으므로, 법 집행 기관이 요구하는 유형의 데이터를 유지하기가 기술적으로 가능하지 않기 때문에 법안에 대해 면제되었다고 말했다.

인터넷 포르노로부터의 아동보호법이라고 부르는 스미스 법안은 무선 통신에 의해 주소가 전송되지 않는다면 ISP 들이 서비스가 제공되는 계정에 임시로 할당된 네트워크 주소를 최소 18개월간 유지할 것을 요구한다. 이 법안은 또한 연방 법률에 생식기를 음란하게 노출하는 것으로써 정의된, 아동 포르노 소유자 들에 대한 처벌을 강화하고 있다.

모바일 면제는 2005년에 법무부가 이슈를 제기한 이래로 부글부글 끓

고 있는 데이터 유지(Retention) 요구사항에 대한 논쟁에 새로운 논란을 가져오고 있다. 제안은 2006년에 미국 의회에서 공식적으로 표면화 되었고, 부시 행정부의 법무장관인 알베르토 곤잘레스는 논의되어야 할 이슈라고 언급했으며, 마침내 FBI의 로버드 뮬러 국장이 실행하게 되었다.

금년 이달 초에 범죄 부문 법무 부차관보인 제이슨 웨인스타인은 무선 사업자 들이 이러한 정보를 저장하지 않을 경우 법 집행기관 들이 필수적인 증거를 수집하는 것을 불가능하게 할 수 있으므로 무선 사업자들도 포함되어야 할 것을 경고하였다.

스미스 법안의 정의는 고객에게 유선 접속을 제공하는 커피숍, 호텔, 대학, 학교, 사업장 등과 전통적인 광대역 서비스사업자 들을 정리할 수 있게 한다.

스미스는 2007년에 무선에 대한 면제 없이 사이버 범죄 방지 조치의 필요성을 요청하는 광범위하게 유사한 법안을 도입한 바 있다. 오늘 소개된 법안은 법집행 기관에 범죄를 찾아내고 기소하기 위해 필요한 도구를 제공하게 될 것이라고 성명서에서 밝혔다.

"유지(Retention)“ 대 "보존(preservation)“

현재, ISP 들은 네트워크 모니터링, 사기 예방, 요금 분쟁 등과 같은 비즈니스 목적을 위해 더 이상 요구되지 않는 모든 로그 파일들을 전통적으로 삭제해 왔다. 그러나, 조사를 수행하는 경찰에 의한 요청이 있을 경우에는 이러한 일반 규칙을 변경하여 데이터 보존(Preservation)이라고 부르는 기능을 제공하고 있다.

1996년에 전자통신 트랜젝션 기록법이라고 부르는 연방법이 데이터 보존을 법규화 했다. 이 법은 ISP 들이 정부 기관의 요청이 있을 경우,

ISP가 보유하고 있는 기록 들을 90일간 유지할 것을 요구한다.

인터넷 주소 들이 상대적으로 부족한 정보자원이므로 ISP 들은 컴퓨터가 사용되는 시점에 풀에서 주소를 고객들에게 할당하는 경향이 있다. (DHCP와 PPP over Ethernet이는 두 가지 표준기술들이 사용되고 있음)

또한, "아동 보호법 2008"이라고 부르는 기존 법률에서는 아동 포르노 전송에 관한 실제 정보를 얻는 ISP 들은 이러한 사실이나 상황 정보를 보고할 것을 요구하고 있다. 이러한 요구사항을 고의적으로 준수하지 않는 기업은 처음 위반에 대해 15만 달러의 벌금을, 그리고 후속 위반에 대해서는 각 위반에 대해 30만 달러 까지의 벌금이 부과될 수 있다.

무선 사업자는 인터넷 기업이 그들의 고객 데이터를 로그할 것을 강제화 하는 새로운 법안의 광범위한 요구사항을 준수할 필요가 없다.

마. 인터넷 포르노로부터 아동보호법 관련 기사 원문

Wireless providers won't have to comply with extensive requirements in a new bill that would force Internet companies to log data about their customers.

CNET was the first to report this exemption for wireless carriers in an article a few weeks ago. That legislation was publicly announced today by U.S. Reps. Lamar Smith (R-Texas), the head of the House Judiciary Committee, and Debbie Wasserman Schultz (D-Fla.).

That appears to be the result of lobbying from wireless providers, which don't want to have to comply with any new governmental mandates. But the exemption has already drawn the ire of the U.S.

Justice Department, and is likely to attract strong opposition from cable and DSL providers who would be the ones singled out for regulation.

CTIA, the wireless trade association, did not respond to a request for comment today. Previously it said through a spokesman only that "we are committed to working with the committee on the legislation."

"Investigators need the assistance of Internet Service Providers to identify users and distributors of online child pornography," Smith said in a statement today. "This bill requires ISPs to retain subscriber records, similar to records retained by telephone companies, to aid law enforcement officials in their fight against child sexual exploitation." The logged data, however, could be used to investigate any type of crime.

A Republican aide to the House Judiciary committee, who did not want to be identified, said the bill exempts wireless providers because their networks are designed in such a way that IP addresses are assigned to multiple users or accounts and they are "not technologically capable of retaining the type of data that law enforcement needs because that's not how their system works.“

Smith's bill, called the Protecting Children From Internet Pornographers Act of 2011, requires Internet providers to "retain for a period of at least 18 months the temporarily assigned network addresses the service assigns to each account, unless that address is transmitted by radio communication." It also enhances penalties for possession of child pornography, which is defined in federal law as the "lascivious" exhibition of the genitals.

The mobile exemption represents a new twist in the debate over data

retention requirements, which has been simmering since the Justice Department pushed the topic in 2005, a development that was first reported by CNET. Proposals publicly surfaced in the U.S. Congress the following year, and Bush administration Attorney General Alberto Gonzales said it was an issue that "must be addressed." So, eventually, did FBI director Robert Mueller.

In January, CNET reported that the Obama Justice Department was following suit. Earlier this month, Jason Weinstein, the deputy assistant attorney general for the criminal division, warned that wireless providers must be included because "when this information is not stored, it may be impossible for law enforcement to collect essential evidence."

The definitions in Smith's bill could sweep in coffee shops that offer wired connections to their customers, as well as hotels, universities, schools, and businesses that offer wired network connections, plus traditional broadband providers.

Smith introduced a broadly similar bill in 2007, without the wireless exemption, calling it a necessary anti-cybercrime measure. "The legislation introduced today will give law enforcement the tools it needs to find and prosecute criminals," he said in a statement at the time.

"Retention" vs. "preservation"

At the moment, Internet service providers typically discard any log file that's no longer required for business reasons such as network monitoring, fraud prevention, or billing disputes. Companies do, however, alter that general rule when contacted by police performing

an investigation--a practice called data preservation.

A 1996 federal law called the Electronic Communication Transactional Records Act regulates data preservation. It requires Internet providers to retain any "record" in their possession for 90 days "upon the request of a governmental entity.“

Because Internet addresses remain a relatively scarce commodity, ISPs tend to allocate them to customers from a pool based on whether a computer is in use at the time. (Two standard techniques used are the Dynamic Host Configuration Protocol and Point-to-Point Protocol over Ethernet.)

In addition, an existing law called the Protect Our Children Act of 2008 requires any Internet provider who "obtains actual knowledge" of possible child pornography transmissions to "make a report of such facts or circumstances." Companies that knowingly fail to comply can be fined up to $150,000 for the first offense and up to $300,000 for each subsequent offense. Wireless providers won't have to comply with extensive requirements in a new bill that would force Internet companies to log data about their customers.

3. 인터넷 서비스 감청 국제표준화 현황

가. 감청 표준화 추진 배경

미국 및 유럽연합의 주요 국가(영국, 독일, 네덜란드 등), 호주 등 많은 국가에서는 전기통신 서비스에 대한 합법적 감청을 법제화 하고 있으며, 통상, 감청 시행에 대한 근거와 감청 범위 등 감청을 위한 상위 수

준의 요구사항 들이 법에 명시되고 있다. 실제 전기통신 서비스에 대한 감청 집행을 위해서는 법에서 명시하는 수준 보다 훨씬 자세한 기술적인 사항 들이 규정되어야 한다. 외국 법들의 사례를 보면 모두 감청기술에 대한 세부 요구사항과 감청 집행 방법 등은 관련 표준을 제정하여 이를 준수하도록 법에서 명시하고 있다. 특히, 감청 협조설비 제공 의무가 있는 통신사업자는 해당 표준에 따른 설비를 구축, 운용시 법에서 규정하는 요건을 만족하는 것으로 인정하며, 미국 CALEA의 제107조 Safe Harbor에서 표준 준수의무를 명시하고 있다.

※ 미국의 경우, 세부 기능 요소와 전송될 통화식별정보에 대한 요구 항목에 대해서는 모두 표준범위에 포함한다.

독일 전기통신법(Telekommunikationsgesetz) 제10조 [감청조치의 기술적 구현]에서 국제표준 준수의무를 명시하고, 국제표준을 벗어날 경우 근거를 제시하도록 하였다.

호주 전기통신법(Telecommunications Act 1997) 의 제15편 정보수사기관의 협력 부문에서 국제표준 또는 호주표준 준수 의무를 명시하고 있다.

<표 2-17> 표준 준수 의무에 대한 법 규정

국가	표준 준수 의무	표준 부재 시 규정
미국	- CALEA 107조 Safe Harbor에 Attorney General이 산업표준 및 CALEA capability 요구사항을 실행시킬 수 있는 industry-wide한 표준을 지정할 수 있는 산업체 협의회 및	- 표준의 부재시에도 103조와 106조의

	표준기구와 협의하도록 함 - 또한, 제정된 표준의 적용에 대하여 통신사업자가 산업체 협의회나 표준기구 또는 FCC에 의해 정해진 103조(감청설비 능력요구사항 지원) 및 106조(장비제조자와 전기통신서비스 공급자의 협력)에 부합하는 관련 공공 기술 요구 사항 및 관련 표준이 존재하는 경우, 그 표준 및 기술 요구사항 준수를 명시함	의무가 경감하는 것이 아님을 명시
독일	- 전기통신법(Telekommunikationsgesetz) 제10조 [감청조치의 기술적 구현]에서 국제표준 준수의무를 명시하고, 국제표준을 벗어날 경우 근거를 제시하도록 함 - 국제표준외의 예외사항은 “연방통신망중개소”가 해당기관과 협의하도록 함	- 새로운 기술적 발전이 기술지침에 반영되지 않았을 경우, 협조의무자는 자신의 감청설비의 구성에 대하여 ‘연방통신망 중개소’와 협의하도록 하고 있음
호주	- 전기통신법 (Telecommunications Act 1997)에 국제 표준 또는 그 결정이 기초하고 있는 국제 표준의 관련부분을 명기하도록 함 - 국제표준이나 호주 표준의 관련부분의 적용을 용이하게 하기 위하여 필요한 수정만을 가한 국제 표준의 일부 또는 전부의 적용, 채택, 또는 편입에 의한 감청 능력 또는 특별협조능력 구비를 명시함	

나. 감청 표준화 추진 개요

o 미국은 CALEA를 통해 가장 먼저 감청 관련 기술표준을 제정, 적용하고 있음

- 미국내 표준단체인 ATIS, TIA 등에서 유무선 통신, 인터넷 서비스 등에 대한 감청 기술표준 제정

o 유럽연합 차원에서 감청 기술표준이 제정되어 유럽 내 국가뿐 아니라 유럽 이외의 국가에서도 채택, 적용되고 있음

- ETSI(European Telecommunications Standards Institute)에서 전기통신 전 분야에 대한 감청 관련 표준 개발
- 3GPP(3G Partnership Project)에서 3G 이동통신에 대한 감청 관련 표준 개발

o 최근, 국제전기통신 표준을 제정하는 ITU-T에서는 패킷검사(DPI) 관련 국제표준을 개발하고 있음

※ ITU-T(International Telecommunications Union
- Telecommunications Standardization Sector)

다. 미국의 인터넷 서비스 감청 표준화 현황

o 미국은 가장 먼저 감청 관련 법 체계를 수립하면서 표준 기반의 감청 집행 체계를 시행하고 있으며, 전기통신 서비스별로 다양한 감청 관련 표준을 제정, 적용하고 있음

o ATIS-1000678 (2006): Lawfully Authorized Electronic Surveillance

(LAES) for Voice over Packet Technologies in Wireline Telecommunications Networks (Version 2)

- 유선통신 네트워크에서 패켓 기술을 이용한 음성 서비스에 대한 감청을 지원하기 위한 표준 (T1.678-2004의 개정 표준)
- 감청 지원을 위한 유선통신 네트워크의 능력과, 감청된 정보(통신식별정보와 통신내용) 전달을 위한 통신사업자와 수사기관 간 인터페이스 및 프로토콜을 정의함

o ATIS-1000013 (2007): LAES For Internet Access and Services
- 인터넷 엑세스 및 제공되는 서비스 들에 대한 감청을 지원하기 위한 표준
- 감청된 정보(통신식별정보와 통신내용) 전달을 위한 인터넷접속 제공사업자와 수사기관 간 인터페이스를 정의
  ※ 인터넷접속 제공사업자는 초고속인터넷사업자, 케이블사업자, WiFi 사업자 등이 해당됨

o ATIS-0700005 (2007): Technical Requirements for LAES for 3GPP IMS-based VoIP and other Multimedia Services
- 3세대 이동통신망에서 IMS 기반의 인터넷전화(VoIP)와 다른 멀티미디어 서비스에 대한 감청을 지원하기 위한 표준
  ※ IMS(IP Multimedia Subsystem)은 3G 이동통신망에서 IP 기반으로 음성을 포함한 다양한 멀티미디어 서비스를 지원하기 위해 개발된 시스템
- 감청된 정보(통신식별정보와 통신내용) 전달을 위한 이동통신 사업자와 수사기관간 인터페이스를 정의

라. 유럽연합(EU)의 인터넷 서비스 감청 표준화 현황

o ETSI TR 102 528 V1.1.1 (2006): LI; Interception domain Architecture for IP networks
- IP 네트워크에 대한 감청을 지원하기 위한 네트워크 운영자 및 통신서비스 제공사업자의 상위 수준의 참조 구조를 정의
- 이 문서는 기존에 이동통신망에서 패켓서비스 도메인에 대한 감청 표준인 TS 133 106 및 TS 133 107에서 정의된 사항과 별개로 IP 네트워크에 대한 사항을 정의

o ETSI TS 102 232-1 V2.6.1 (2011): LI; Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 1: Handover specification for IP delivery
- ETSI는 IP 기반 인터넷 서비스 유형별로 감청을 지원하기 위한 세부 사항 들을 ETSI IS 102 232-x 시리즈 표준으로 각각 정의하고 있음
- Part 1은 인터넷 서비스에 대한 감청된 정보(통신식별정보와 통신내용)를 인터넷 서비스제공 사업자로 부터 수사기관으로 전달하기 위한 인터페이스와 전송 프로토콜 등을 정의
  ※ 기존 전기통신 서비스에 대한 일반적인 감청 인터페이스에, 인터넷 서비스에 대한 감청정보 전달을 위해 추가적으로 요구되는 사항을 정의

o ETSI TS 102 232-2 V2.5.1 (2010): Part 2: Service-specific details for E-mail services

- E-mail 서비스 감청을 위한 수사기관 요구사항과, 인터넷 서비스 제공사업자로 부터 전달될 이메일 감청정보(통신식별정보와 통신내용)에 대한 세부 사항을 정의

o ETSI TS 102 232-3 V2.2.1 (2009): Part 3: Service-specific details for internet access services
- 인터넷 액세스 서비스에 대해 감청 대상자 식별정보와 IP 주소 정보를 바인딩하는 절차 관련 요구사항과, 수사기관에 전달되어야 할 감청정보에 대한 세부 사항을 정의

o ETSI TS 102 232-4 V2.3.1 (2010): Part 4: Service-specific details for Layer 2 services
- Layer 2(MAC 계층) 세션 정보에 접근할 수 있으나 Layer 3(IP 계층) 정보를 가질 필요는 없는 엑세스 네트워크 제공사업자가 감청을 지원하기 위한 표준
- L2 계층에서 감청을 위한 요구사항과, 감청 구조 및 정보 흐름, 그리고 L2 계층에서 수집되는 정보를 수사기관에 전달하기 위한 프로토콜 등에 대해 정의

o ETSI TS 102 232-5 V2.5.1 (2010): Part 5: Service-specific details for IP Multimedia Services
- SIP, RTP, H.323 표준 프로토콜 등을 이용하여 제공되는 IP 멀티미디어 서비스의 감청을 위한 세부 요구사항과 프로토콜 등을 정의
  ※ SIP(Session Initiation Protocol)과 RTP(Real Time Transport Protocol)는 인터넷 표준개발 단체인 IETF에서 개발된 멀티미디어 세션 설정 및 오디오/비디오 정보의 실시간 전달 프로토

콜이며, H.323은 ITU-T에서 개발된 멀티미디어 응용 서비스 제공을 위한 표준기술임

o ETSI TS 102 232-6 V2.3.1 (2008): Part 6: Service-specific details for PSTN/ISDN services
- 이 표준의 제1부(TS 102 232-1)에 정의된 패킷 기반 기법을 이용하여 감청된 PSTN/ISDN 서비스에 대한 감청정보를 수사기관에 전달하기 위한 세부 사항을 정의

o ETSI TS 102 232-7 V2.2.1 (2011): Part 7: Service-specific details for Mobile Services
- 이동통신망에 대한 감청 인터페이스를 정의하고 있는 3GPP TS 33.108과 ANSI/J-STD-025-B 표준에 정의된 바에 따라 감청된 정보를, 이 표준의 제1부(TS 102 232-1)에 정의된 방식에 따라 지원하기 위한 추가적인 사항을 정의
※ 3GPP TS 33.108과 ANSI/J-STD-025-B 표준에 정의된 사항에 대한 수정이나 변경 없이 그대로 적용됨

마. 패켓검사(DPI: Deep Packet Inspection) 기술 표준화 현황

1) 패켓 검사(DPI) 기술 표준화 개요

o 다양한 종류의 응용 트래픽이 혼재되어 전송되는 패켓 기반 네트워크에서 (DPI: Deep Packet Inspection) 기술은 통신사업자로 하여금 이들 복잡한 트래픽을 효율적으로 처리하여 망 성능을 높일 수 있도

록 하는 주요 기술로 적용되고 있다.

o 현재, 통신사업자에 의해 적용되는 DPI 기술은 통신망을 통해 전송되는 패켓의 헤더 정보를 분석하여 응용 서비스의 종류(email, VoIP, 메신저 등)나 송수신 목적지(IP 주소 정보 등)를 구분하여 해당 트래픽을 효율적으로 처리할 수 있도록 하는 기술이다.

- 실제 통신을 위한 사용자 정보(음성 또는 데이터)는 패켓 헤더가 아니라 헤더 뒤에 따라 오는 추가적인 패켓인 페이로드 부분에 기록되므로 패켓 헤더에 대한 검사로는 통신 내용이 검출되지 않는다.

o ITU-T Study Group 13에서는 2009년부터 전기통신망의 효율적 운영과 트래픽 유형에 따른 효율적 서비스 제공을 위해 패켓검사(DPI) 기술의 적용을 위한 세부 표준화 작업을 추진하고 있다.

2) ITU-T의 패켓 검사 관련 표준화 현황

o Draft Recommendation ITU-T Y.dpireq: Requirements for Deep Packet Inspection in NGN

- 이 권고안은 NGN 통신망 환경에서 패켓검사(DPI: Deep Packet Inspection) 기능을 수행하는 기능요소와 이들 기능요소에 대한 인터페이스에 대한 요구사항, 그리고 네트워크 관점에서의 DPI에 대한 기능 요구사항을 정의
- 또한, DPI 기술이 사용될 수 있는 다양한 유스케이스와 패켓 검사를 위한 규칙 적용 사례 등에 대해 권고 부록에 기술
- 이 문서에 정의된 요구사항 들은 NGN 통신망 이외의 다른 통신

망 환경에 적용될 수도 있음

※ 2011년 10월경 ITU-T 권고로 승인될 예정임

o Draft ITU-T Recommendation Y.dpifr: Framework for Deep Packet Inspection

- 이 권고초안은 전기통신망에서 DPI 기술 적용을 위한 세부 구조와 동작 방식, 주요 기능 요소별 동작방안 등에 대해 정의
- 2011년 5월 현재, 아직 초기 단계의 표준 문서로 표준화 작업 그룹 내에서 DPI 기능 제공을 위한 세부 프레임워크에 대한 논의가 활발하게 추진되고 있음

제 2 절 스마트폰 응용서비스 통신비밀 기술 동향 분석

1. 스마트폰의 위치정보 활용 현황 및 문제점 분석

가. 위치정보 관련 현황

1) 아이폰의 위치정보 관련 현황

o 위치정보 저장방법

아이폰의 GPS 또는 기지국을 이용한 사용자의 위치정보는 아이폰 내의 “consolidated.db"라는 파일에 자동으로 저장된다. 이는 앨러스데어 앨런과 피트 위든이란 두 명의 프로그램머가 4월20일 미국 샌프란시스코에서 열린 위치기술 전문가 회의에서 아이폰과 아이패드에 사용자 위치정보가 기록되고 있다고 공개한 후에 널리 알려지게 되었다.

consolidated.db 파일에는 사용자의 위치, 시간, 와이파이망 정보 등의 위치정보가 1초단위로 암호화 되지 않은 상태로 저장되고 있으며. 본 파일은 사용자가 삭제할 수 없다. 앨런에 따르면 저장된 정보는 아이튠즈에 동기화 될 때 자동으로 사용자 컴퓨터에 남게 되며, 이와 같은 기능은 작년 6월에 업데이트된 ios4.0 버전부터 생긴 것이다.

o 전송방법

기지국 및 와이파이 액세스 포인트 정보를 자동으로 수집해서 12시간마다 암호화된 상태로 와이파이 인터넷 연결을 통해서 전송된다.

※ 애플은 2010년6월 미국 국회의원 에드워드 마키와 조 바튼에게

애플이 사용자로부터 어떤 위치정보를 수집하고 있는지에 대한 상세한 내용을 기록한 서한을 보냈는데, 이 서한에서 위와 같이 밝힘.

위와 같이 와이파이망을 통한 위치정보 전송은 아이폰이 도입될 때 위치정보약관에 해당내용이 있다.

※ 해당약관(일부): 위치정보, 아이폰과 같이 GPS기능이 부과된 Apple 제품은 주기적으로 GPS로부터 이동통신 및 WiFi기지국에 대한 위치정보를 기록합니다. 이러한 정보는 익명의 형식으로 수집되고, 고객이나 고객의 아이폰을 특정하지 않으며, 아이폰에 축적된후 주기적으로 애플 서버로 전송되어 저장되고 apple의 위치기술의 정확도와 성능을 향상시키는데 사용됩니다. 고객에게는 이동통신망 데이터 이용료가 과금되지 않도록 하기 위하여 이런 정보는 고객이 WiFi망에 연결되어 있을 때만 보내집니다.

o 활용방법

iPhoneTracker라는 프로그램을 이용하면, consolidated.db 파일을 읽어서 지도상에 그 위치의 궤적을 볼 수 있으며, 미국에서는 범죄수사에 이미 아이폰/아이패드에 저장된 위치정보를 활용하고 있다. Apple은 미국에서는 공식적으로는 위치정보만 저장, 전송하고 위치기반서비스를 제공하고 이를 개선하는데 이 정보를 사용하고 있음을 밝히고 있으며, 위치정보수집에 동의하지 않으면 사용자는 일부 애플리케시션을 사용할 수 없게 된다.

2) 안드로이드 폰의 위치정보 관련 현황

o 위치정보 저장방법

“cache"방식으로 저장되며, 일정시간(48시간)이 지나면 정보를 삭제하여 정보의 축적을 방지하며, 사용자가 삭제가능하다.

※ 갤럭시 s의 경우 시간순으로 50개의 위치정보만을 기록함.

위치정보의 저장시 암호화하여 저장하며, PC 등과 연결시 동기화는 되지 않고, 몇 초 단위로 사용자 데이터를 수집하고 구글에 전송하는데, 이 데이터에는 GPS 위치, 와이파이(Wi-Fi) 핫스팟, 기기의 ID 등이 포함되며, 사용자 설정에 의해 기능을 켤수도 있도 끌 수도 있다.

o 전송방법

보안전문가 세이미 캠커가 조사한 결과, 대만 HTC사(社)의 한 안드로이드폰의 경우 휴대폰의 위치와 근처 와이파이망의 이름, 위치, 신호강도 등의 정보를 수 초마다 저장해뒀다가 이 데이터를 와이파이 망을 이용하여 시간당 몇 차례씩 구글에 전송하는 것으로 나타났다.

o 활용방법

위치정보응용서비스(google map 등)에 활용하며 사용자는 위치정보제공에 동의하지 않더라도 위치기반 서비스를 받을 수는 있으며, 이 경우 위치정보의 정밀도는 떨어지게 된다.

3) 스마트폰의 위치정보 이용 관련 문제점

o 아이폰의 위치정보 활용관련 문제점

사용자의 위치정보가 암호화되지 않은 상태로 스마트폰에 저장되어 위치정보의 유출위험이 있으며, 사용자가 위치정보를 삭제할 수 없다. 어떠한 종류의 위치정보가 폰에 저장되고 전송되는지에 대한

애플의 공식적인 발표가 없으므로, 위치정보 이외의 개인정보의 저장 및 전송 가능성이 있다.

o 안드로이드 폰의 위치정보 활용 관련 문제점

어떠한 종류의 위치정보가 폰에 저장되고 전송되는지에 대한 구글의 공식적인 발표가 없으므로, 위치정보 이외의 개인정보의 저장 및 전송 가능성이 있다.

2. 데이터 압축 앱 응용 현황 및 통비 관련 이슈 분석

가. 3G 데이터 트래픽 감소 서비스(ONAVO 서비스)

1) Onavo 서비스의 기본 개념

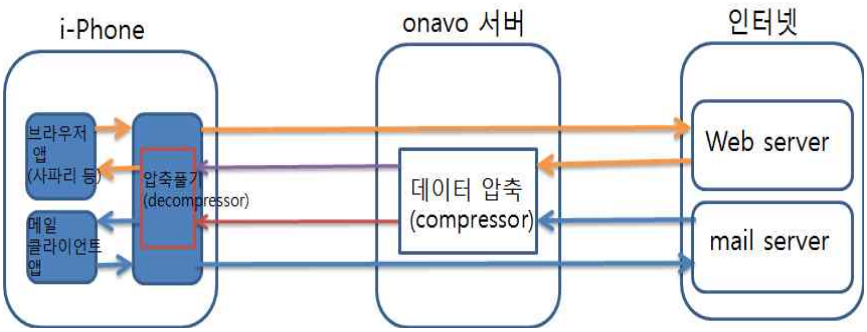
I-Phone의 무료앱인 onavo는 3G 데이터 통신시에 HTTP 프로토콜로 다운로드 되는 트래픽에 대하여 압축(compression)과 압축을 푸는(decompression) 과정을 자사의 서버와 앱을 통하여 제공하여 3G데이터 트래픽을 줄여주는 앱이다. 현재는 무료이나 향후 유료화가 계획되어 있다.

2) 적용대상

3G 데이터 통신중에만 작동되며 현재는 download되는 HTTP 트랙픽, 마이크로소프트의 익스체인지 메일 다운로드에 대하여만 작동한다. SSL와 같은 보안트랙픽, VoIP, YouTube, SKype와 같은 실시간 스트리밍서비스에 대하여는 onavo의 데이터 트래픽 감소기능이 작동되지 않는다.

3) onavo의 3G 데이터 트래픽 감소의 기술적 방법

[그림 2-1] onavo 서비스의 기술적 개념



I-Phone 사용자는 onavo 앱을 다운하고, onavo에 회원으로 가입한 후에 모든 3G 트랙픽은 onavo서버로 redirecting된다는 것에 동의해야 onavo 서비스를 사용할 수 있으며, 위 절차가 끝나면 onavo 앱은 아이폰에서 백그라운드로 항상 동작한다.(사용자는 onavo에 의한 데이터 트래픽 감소 기능을 끌 수 있다.)

아이폰 사용자가 http프로토콜을 이용하여 웹을 액세스 하면, 아이폰에서 나가는 데이터 트래픽은 모두 onavo 서버로 redirecting 되고 onavo서버에서 웹을 액세스하고 이때 다운되는 트래픽을 압축하여 아이폰으로 전송하고 아이폰의 onavo앱은 onavo 서버에서 오는 압축된 데이터를 풀어서 아이폰의 브라우저에 전달한다. 결국, 사용자와 onavo 서버 사이에는 압축된 데이터가 전송되므로 데이터 전송량이 줄어들게 된다. 압축 알고리즘은 공개되어 있지 않으나, HTTP 프로토콜로 다운로드되는 영상이 원래의 영상보다 화질이 떨어진다는 onavo측의 설명에 따르면, 영상에 대해서는 손실부호화, 텍스트에 대해서는 무손실부호화 방법을 사용하고 있는 것으로 추정된다.

※ 웹상에 게제된 사진들은 대부분 jpg, gif 등으로 영상압축을 한 사진이기 때문에 무손실부호화로는 거의 데이터 압축 효과를 얻

을 수 없기 때문임

※ onavo는 Amazon Web service hosting을 사용하여 서버를 운영하고 있음.

4) onavo 서비스의 보안

onavo 서비스는 별도 데이터에 대한 별도의 보안 프로토콜을 제공하지 않고, 모든 데이터 트래픽이 onavo 서버로 redirecting 되므로 사용자의 데이터가 유출될 가능성이 있다.

5) ONAVO 서비스의 국내 현황

o 실제 사용 결과

onavo앱이 데이터 트래픽을 감소시키는 무료 앱이라는 이유료 이를 아이폰에 설치한 가입자의 사용기에 따르면, 속도가 느리고, 사진이 깨어져 수신되는 경우가 많고, 아이폰에서 지울 경우 완전히 지워지지 않는 단점이 있어서 별로 추천하지 않는다. 느린 속도는, 모든 데이터 트래픽이 미국에 있는 onavo의 서버를 통하여야 하고, onavo서버에서 데이터 압축 및 풀기를 해야 하기 때문인 것으로 추정되고 있다.

6) ONAVO 서비스 사용자에 대한 감청

onavo는 음성호에 대한 압축을 제공하지 않으므로 음성에 대해서는 일반적인 감청이 가능하나, 데이터 호(웹 접근, 다운로드 등)에 대한 감청은 압축과 관련된 고려가 필요하다.

o 데이터 호에 대한 감청방법

onavo 서비스 가입자의 폰에서 웹으로 나가는 데이터는 압축되지

않으므로 일반적인 데이터 감청방법을 사용할 수 있으며, 다운로드되는 http 프로토콜에 의한 데이터는 폰까지는 압축된 형태로 전달되고, onavo 앱에서 이를 풀기 때문에, 감청을 위해서는 onavo 서비스에서 사용하는 압축알고리즘을 알아야 한다. 다운로드되는 익스체이저 메일은 압축되어 폰까지는 압축된 형태로 전달되고, 앱에서 이를 풀어서 익스체인저 메일 클라이언트에게 전달하기 때문에 감청을 위해서는 onavo 서비스에서 사용하는 압축알고리즘을 알아야 한다. 아이폰에서 발송되는 익스체이저 메일은 압축되지 않고 일반메일과 동일하기 때문에 onavo 서비스 가입자에 대한 특별한 감청방법은 필요치 않다. onavo 서비스 가입자가 송수신하는 모든 데이터는 onavo 서버로 가게 되므로 onavo 서버에 대한 감청을 통하여 가입자에 대한 감청이 가능하다.

나. 아이폰 압축 앱(오페라 터보) 분석

1) 오페라 개념

o 오페라 소프트웨어 (Opera Software ASA): 노르웨이 소프트웨어 기업으로 웹브리우져인 오페라 계열을 개발함

o 오페라: 다양한 기능을 가지는 웹브라우져로 다른 웹브라우져에 비해 작고 가벼우며, 페이지 렌더링(화면 출력) 속도가 매우 빠름. 사용하기 위해서는 가입절차가 필요없음.

o 오페라 터보: 네트워크 연결이 느리거나 불안정한 환경에서 오페라 터보 기능을 활성화시키면, 오페라 웹페이지에서 요청한 자료들이 오페라 터보 서버로 우선 전송된 후에 서버에서 압축된 데이터를 오페라 웹브라우져 사용자에게 전송하는 형태임.

– 오페라 터보 기능은 PC용 오페라, 오페라 모바일, 오페라 미니에

모두 사용 가능함

- 오페라 터보 기능은 사용자가 직접 판단하여 네트워크 상태가 좋지 않을 경우 활성화하여 사용함
- 오페라 터보 기능은 네트워크 연결 종류(3G, WiFi 등) 무관하게 동작함

o 오페라 모바일: 스마트폰과 PDA 용으로 개발된 웹브라우져로 오페라 모바일 버전 9.7부터 오페라 터보 기능이 추가되며, 안드로이드 운영체제, BREW, 윈도 모바일, 심비안/S60 등 지원

o 오페라 미니: 휴대폰, 스마트폰, PDA용으로 설계된 웹브라우져로 무료로 제공되는 앱임.

※ 오페라 미니와 오페라 모바일은 모두 모바일용 단말용이며 오페라 모바일에서는 직접 렌더링하고 오페라 미니에서는 서버에서 렌더링함. 화질과 기능적인 면에서 오페라 모바일이 더 우수함.

다. 오페라와 Onavo 비교

o 오페라는 웹브라우져 기능으로 웹서핑을 위해 사용되며, Onavo는 주로 웹서핑과 이메일에 사용되지만 특정 애플리케이션에 국한되지 않음

o 오페라터보와 Onavo는 서버를 경유하여 압축하는 개념은 동일함. (이미지에 대해서는 손실 부호화, 텍스트에 대해서는 무손실 부호화 적용)

o Onavo는 3G에서만 동작하며, 오페라터보는 3G뿐만 아니라 붐비는 WiFi나 테더링된 스마트폰에서도 동작함

라. 오페라 서비스 사용자에 대한 통비 이슈

o 오페라는 웹브라우져 기능으로 감청되는 내용은 서비스 이용자가 웹 서핑한 내용만 해당됨.
o 오페라는 웹브라우져 응용으로 사용자 가입 절차가 없어 압축서버(오페라 터보 서버)에서의 사용자를 확인할 수 있는 정보가 없음
o 오페라 터보 서버에서 출력된 압축된 데이터에 대해서는 압축 알고리즘을 알아야 함

3. 스마트폰 도청 보도에 대한 기술적 분석

1) MBC 보도 내용 개요

o 2011년 6월 7일 MBC 뉴스데스크에서 MBC 단독 보도로 안드로이드 기반 스마트폰 도청 관련 언론 보도가 있었음

o 안드로이드 기반 스마트폰을 이용하여 주변의 대화 내용을 도청하는 사례 시연
- 도청 시연에 안드로이드 기반 갤럭시S와 옵티머스 스마트폰 사용
- 해커가 게임으로 위장하여 인터넷에 올려 둔 악성 프로그램을 게임인 줄 알고 다운로드 받아 작동시키면 스마트폰이 감염되어 도청기 역할 수행

o 안드로이드 폰에 저장되어 있는 정보를 빼내는 사례 시연
- 안드로이드 폰에 새로운 게임에 접속해 보라는 문자 메시지 도착 시, 문자 메시지에 링크되어 있는 게임을 내려 받아 실행시키면 스마트폰이 악성코드에 감염
- 감염된 스마트폰에 저장된 전화번호 목록, 사진, 이메일, 문서 들

이 해커의 노트북으로 전송될 수 있음
- 감염된 스마트폰의 위치 정보도 확인 가능
- 감염된 수많은 스마트폰을 이용하여 분산서비스 거부(DDoS) 공격을 함으로써 특정 웹 사이트를 마비시킬 수 있음
- 스마트폰 해킹을 통해 계좌에서 돈을 빼가는 것도 가능할 것

2) 스마트폰 상에서의 응용 프로그램 개발 환경

o 스마트폰은 PC와 동일한 기능을 제공하므로 응용 프로그램이 스마트폰의 내부 장치 들(마이크, 스피커, 메모리 등)을 엑세스 하거나, 제어 하는 것이 가능함

o 안드로이드 등의 스마트폰 운영체제는 제3자에 의한 응용 프로그램 개발이 가능하도록 API(응용프로그램 인터페이스)가 공개되어 제공됨
- 개발자는 이들 API를 이용하여 스마트폰 내 각종 장치를 엑세스할 수 있게 되며, 이러한 기능을 이용하여 다양한 응용 프로그램을 개발하게 됨

3) 스마트폰에서의 해킹 방법

o 악성 프로그램이 스마트폰 내부 마이크 기능을 동작시킬 경우 주변의 대화 내용을 녹음할 수 있고, 녹음된 내용을 외부 해커에게 전송하도록 할 경우 원격지에서 대화 내용을 청취 가능함

o 스마트폰에 앱을 설치하여 스마트폰의 각종 장치들을 제어하는 해킹 공격이 가능함
- 스마트폰 내부의 저장장치에 접근하여 전화번호 목록, 사진, 이메

일 등의 데이터를 수집하여 원격지 해커에게 전송 가능
- 스마트폰 내부의 GPS 기능을 제어하여 현재의 위치정보를 원격지 해커에게 전송 가능

o 감염된 수많은 스마트폰에 대해 해커가 원격지에서 특정 명령을 실행시켜 분산서비스 거부(DDoS) 공격을 하도록 함으로써 특정 웹 사이트를 마비시킬 수 있음

4) 스마트폰에서의 악성코드에 의한 해킹 대응 방법

o 악성 코드가 들어 있는 프로그램을 설치하지 않도록 주의해야 함
- 대부분 블랙마켓에서 유통되는 악성코드가 원인이므로 주의가 필요하며, 공식 싸이트에서 앱을 다운로드 받는 것이 안전함
- 공식시장에서는 앱에 대한 검증과 점검이 빨리 이루어져 문제의 악성 프로그램에 대한 차단이 이루어지나, 블랙마켓에서는 악성코드에 대한 필터링이 어려움
- 응용 프로그램 다운로드 보다 이메일이나 메시지를 통해 유포되는 악성 프로그램이 더 큰 문제이며, 메시지 등을 통해 전달되는 의심스러운 앱은 가능한한 설치하지 않는 것이 바람직함

o 스마트폰에 보안 프로그램인 “백신“을 미리 설치하여 악성 코드 설치 시도시 이를 차단할 수 있도록 대비할 필요가 있음

o 스마트폰의 환경설정 기능을 이용하여 출처를 알 수 없는 응용 프로그램 설치를 차단시키는 방안 사용
- 통상, 스마트폰의 환경 설정 메뉴에는 사용자 들이 프로그램을 다운로드 받아 설치하는 것을 제어할 수 있는 기능을 제공함

- 이러한 기능을 이용하여 출처가 불분명한 응용 프로그램의 설치를 차단시킴으로써 해킹 위협에 대응 가능

제 3 절 유무선 환경에서 SNS, 메신저, VoIP 서비스 감청방안 및 통신비밀 보호방안 연구

1. 인터넷상 개인정보보호방안 시행시 통신수사 관련 영향 분석

가. 인터넷상 개인정보 보호방안 개념

현재 인터넷 통신서비스를 제공하는 대부분의 업체들은 가입시에 성명, 주민등록번호, 주소 등의 개인정보를 요구하고 있으며, 이들 정보를 서버에 저장하여 관리하고 있다. 최근에 이들 저장된 개인정보가 해킹으로 대량으로 유출되는 사고가 발생하였고, SK컴즈는 개인정보유출을 원천적으로 차단하기 위하여 통신서비스 가입자의 주민등록번호를 수집하지 않을 계획을 갖고 있다. SK컴즈는 실제로 2011년8월31일부터 주민등록번호를 수집하지 않고 있으며, 기존에 수집된 가입자 주민등록번호도 2011년8월31일부로 DBMS(Database Management System: 데이터베이스 관리시스템)에서 파기하였다. 이러한 SK컴즈의 움직임은 주민번호가 포함된 개인정보는 악용될 경우, 신용카드부정발급 등의 범죄에 사용될 수 있고, 만약 그러한 범죄로 인한 개인의 피해가 발생한 경우, SK컴즈는 개인정보의 관리자로서 그 책임을 져야 하기 때문에 이를 방지하는 차원으로 해석될 수 있다. SK컴즈는 결과적으로 주민번호를 포함하지 않은 개인정보만을 관리하게 됨으로써, 해킹등에 의한 개인정보 유출시에도 심각한 개인의 피해를 원천예방하는 효과를 갖는다. 주민번호를 포함되지 않은 개인정보는 유출되어도 부정하게 사용될 가능성이 크게 줄어들게 되므로 많은 기업들이 SK컴즈의 예를 따를 가능성이 있다.

나. 주민등록번호가 저장되어 있지 않을 경우의 통신수사 방안

인터넷 서비스 제공회사에 회원들의 주민등록번호가 저장되어 있지 않을 경우에는 해킹에 의한 개인정보 유출위험이 줄어들고, 유출되었을 경우의 피해도 줄어들 것이나 범죄수사를 위한 감청 등의 경우에는 주민등록번호 등의 개인식별정보가 없으면 감청의 실시가 어려워질 수 있다. 이를 방지하기 위하여 인터넷통신서비스 제공자는 회원 가입시에 가입자의 이름과 실명확인번호(CI)를 반드시 저장하여야 한다. 통신자료를 요청하는 국가기관에서는 인터넷통신서비스 가입자의 이름과 주민등록번호, 또는 주민등록번호만을 기입하여 통신자료 및 감청을 요청할 수 있으며, 이 경우에 국가기관이 주민등록번호로 감청을 요청하면, 인터넷통신서비스 제공자는 요청받은 주민등록번호를 신용평가사에 제출하여 실명확인번호(CI)값을 받아서 저장해둔 실명확인값과 비교하여 개인을 확인할 수 있게 된다. 이 경우에 주민등록번호로 CI값을 조회 가능하지만 사용자 ID나 CI값 등으로 주민등록번호를 조회할 수는 없다.

2. SNS서비스, 모바일 메신저의 통신비밀 관련 고려사항 분석

가. 카카오톡 사업자가 보관하는 통신자료, 통신사실확인자료 내역 및 메시지 보관[삭제] 방법

카카오톡은 회원아이디, 가입/탈퇴 일시, 대화내역, 접속기록(상대방 전화번호, 통신일시)을 최대 1개월치를 저장하여 국가기관의 감청요청에 대응하고 있으며, 현재 1개월치를 저장하고 있지만 서버용량 부족으로 인하여 저장기간을 단축시키는 방안을 고려중이다.

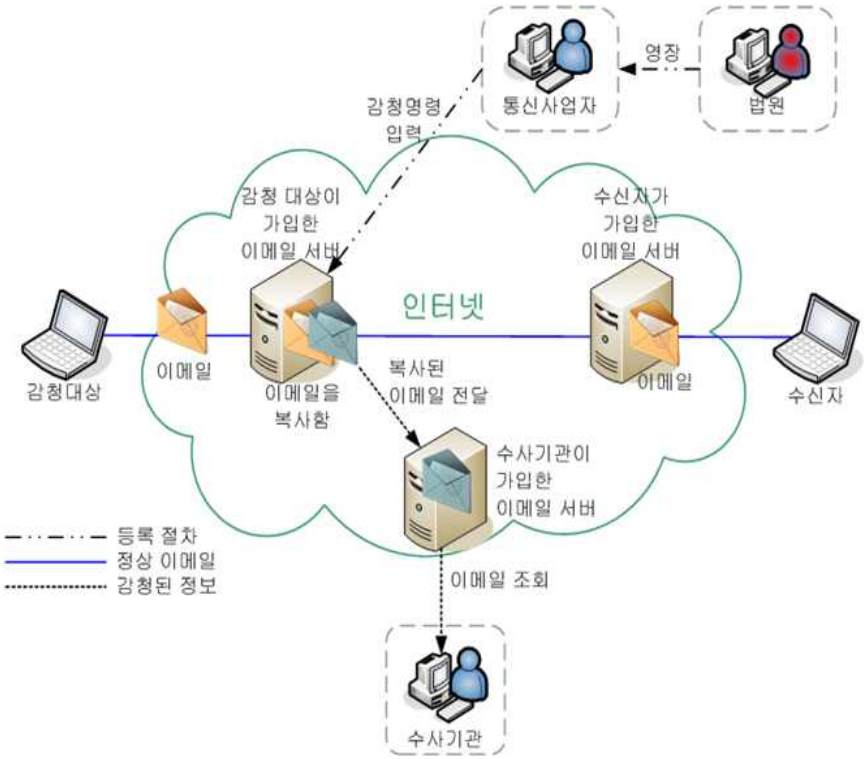
나. 모바일 메신저에 대한 외국의 수사기법 및 사례

1) BlackBerry messenger(BBM) 서비스 감청

아랍에미리트(UAE) 통신 당국은 블랙베리를 통해 주고받는 이용자 데이터에 대한 감청 및 검색이 어렵다는 이유로 블랙베리 메신저, 이메일 등의 메시징 서비스를 중단시키겠다고 밝혔는데, 이는 블랙베리를 통해 전달되는 메시징 서비스 데이터가 제조사인 캐나다 RIM 사의 서버를 직접 경유하여 암호화가 이루어지기 때문이었고, UAE 당국은 내국인은 물론 외국인 방문자들에게도 이 조치를 적용하겠다고 공표한 것으로 알려졌었다. 비슷한 이유로, 사우디아라비아, 쿠웨이트, 인도, 파키스탄 등의 국가에서 블랙베리의 주요 서비스를 중단하도록 하거나, 이를 검토하고 있는 것으로 파악되었다. 8월 10일, RIM 사가 사우디아라비아 정부에 블랙베리 서비스 이용자에 대한 PIN(personal identification number) 및 사용자 코드를 제공하기로 함에 따라, 서비스 중단에 대한 결정은 철회되었다. 이에 따라, 사우디아라비아 정부는 블랙베리의 메시징 서비스를 처리하는 RIM 서버에 접근할 수 있으며, 통신 암호화에 이용된 사용자 코드를 이용하여 암호화된 통신 내용을 해독할 수 있게 되었다.

이메일 등과 같은 메시징 서비스에 대한 감청은 일반적으로 서비스 제공업자가 서버에 저장된 통신 내용(메시지)의 사본을 수사기관에 제공함으로써 이루어지게 된다.

[그림 2-2] 이메일 서비스 감청 개념도



RIM 사가 사우디 정부로 하여금 블랙베리 메신저 제공 서버에 접근할 수 있도록 함에 따라, 위 그림과 비슷한 형태로 블랙베리 메시징 서비스를 감청하는 것이 하나의 가능성이 될 수 있다. 사우디아라비아를 비롯한 중동 국가와는 달리, 미국 및 유럽 일부 국가들은 블랙베리 트래픽을 감청하기 위한 법원 영장을 요청할 수 있었던 것으로 알려졌다. RIM사는 자사의 모바일 메신저인 BBM서비스에 대한 감청을 2010년1월31일까지 가능하게 하는 것에 대하여 인도 정부와 합의하였다. 인도와 합의전에 RIM 사는 공식적으로 BBM은 자사의 보안구조는 대칭키

방식으로, 한 고객이 자신의 보안키를 또 다른 고객이 그들 자신의 암호화키를 가지고, 마스터 암호화키를 RIM사가 보관하지 않고, 백도어도 없기 때문에 암호화된 고객의 정보는 당사자가 아니면 누구도 읽을 수 없다고 했었다. 인도 정부와 합의된 BBM의 감청은 cloud computing 방법을 이용하여 제공된다. 인도 정부와 합의한 내용 중에는 감청을 용이하게 하기 위하여 BBM 서버를 인도 내에 두는 것도 포함되어 있다.

3. SSL 개요 및 해킹

가. SSL(Secure Socket Layer) 개요

1) SSL의 주요 목표

SSL 프로토콜은 인터넷 상에서 비밀 통신을 제공하기 위하여 제안되었으며, 도청과 위조로부터 안전하게 데이터를 전송하기 위하여 TCP/IP 계층과 응용프로그램계층 사이에 위치한다. 이러한 SSL의 주요 특징은 다음과 같다.

o 암호학적 보안

- SSL은 두 통신 개체 사이의 보안 연결을 설정하는데 사용된다.

o 상호 운용성

- 독립된 프로그래머가 SSL을 이용하여 서로의 코드에 대한 지식 없이 암호학적 인수들을 성공적으로 교환할 수 있는 응용 프로그램을 만들 수 있어야 한다.

o 확장성

- SSL은 필요에 따라 새로운 공개키와 많은 암호화 기법을 사용할 수 있는 구조를 제공함. 따라서 새로운 약점이 노출될 수 있는 프로토콜을 새롭게 설계할 필요가 없고 완전히 새로운 보안 라이브러리를 작성할 필요가 없다.

2) SSL의 보안 서비스

SSL은 상호인증, 무결성을 위한 전자서명, 기밀성을 위한 암호화 등을 제공함으로써 클라이언트와 서버 사이에 안전한 통신을 제공합니다.

o 기밀성 서비스

기밀성 서비스를 제공하기 위해 사용되는 비밀키는 핸드쉐이크 프로토콜에 의해 생성됨. SSL에서는 전자서명과 키 교환을 위해 RSA 또는 DH 알고리즘을 이용할 수 있고, 기밀성을 필요로 하는 다수의 응용 프로그램에 대하여 다양한 암호 알고리즘을 제공할 수 있다.

o 메시지 무결성 서비스

MAC(Message Authentication Code)은 누군가 데이터 전송을 방해할 수 없도록 하거나 재전송 공격에 이용할 수 없도록 무결성 서비스를 제공한다.

o 클라이언트와 서버간의 상호 인증 서비스

SSL은 연결설정 과정에서 서로 간에 신뢰할 수 있도록 클라이언트와 서버가 서로에 대한 인증을 할 수 있는 공개키 인증서를 사용합니다. SSL은 다음과 같은 인증서를 지원한다.

- 임의의 길이의 공개키를 사용하는 RSA 공개키 인증서
- 최대 512 비트 길이의 공개키를 사용하는 RSA 공개키 인증서
- 서명 데이터에만 이용되는 RSA 공개키를 사용하는 Signing-only RSA 인증서
- DSS 인증서
- Diffie-Hellman 인증서

이러한 인증서의 사용은 선택이지만, SSL에서는 클라이언트와 서버 양쪽 모

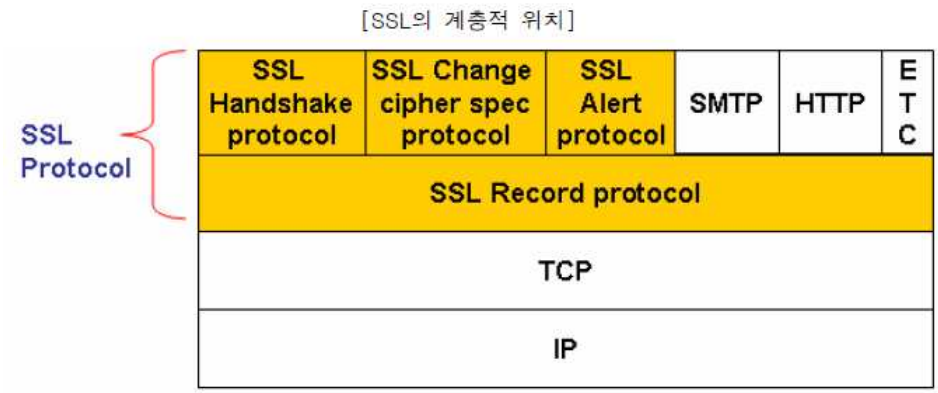
두가 Diffie-Hellman 키 교환 프로토콜을 사용하지 않는 한 서버 인증서를 필요로 한다. 기밀성 서비스를 제공하기 위해 사용되는 비밀키는 핸드쉐이크 프로토콜에 의해 생성된다. SSL에서는 전자서명과 키 교환을 위해 RSA 또는 DH 알고리즘을 이용할 수 있고, 기밀성을 필요로 하는 다수의 응용 프로그램에 대하여 다양한 암호 알고리즘을 제공할 수 있다.

3) SSL의 특징

o 계층적 구조

SSL은 그림과 같이 전송계층과 응용계층 사이에 위치하며, 크게 상위계층인 Control 프로토콜과 하위계층인 Record 프로토콜로 나눌 수 있습니다. Control 프로토콜은 그림과 같이 Handshake Protocol, Change Cipher Spec, Alert Protocol로 구분된다.

[그림 2-3] SSL의 계층적 위치

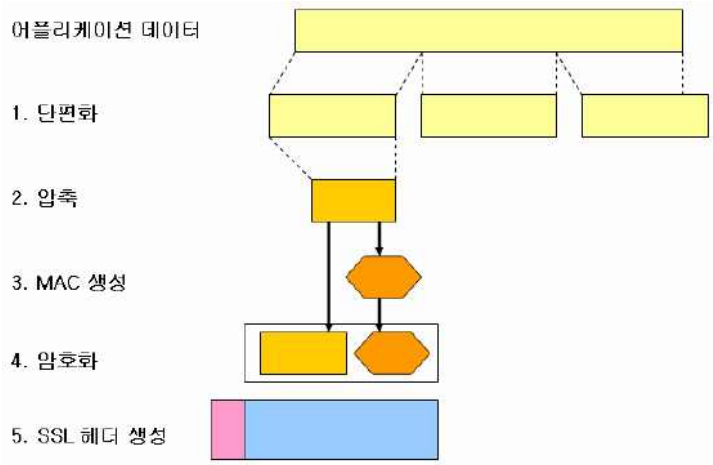


o SSL 패킷 생성 프로세스

Record 계층에서는 전송될 데이터를 보호하기 위해서 다음과 같

은 과정을 거침. 각각의 데이터를 알맞은 크기로 자르고, 선택적으로 압축하고, MAC을 적용하고, 암호화하여 그 결과를 전송한다. 전송된 데이터는 복호화되고 입증되고, 압축이 풀리고, 분할된 데이터가 다시 합쳐져서 상위 계층으로 전송된다.

[그림 2-4] 데이터 압축 및 암호화 구조도



위와 같이 Record 계층에서 데이터를 보호하기 위해서 적용되는 암호알고리즘과 암호키, MAC 알고리즘은 cipher spec에 의해 결정된다. 이는 핸드쉐이크 프로토콜을 통해 전송되고, 이때 데이터 암호키 생성을 위해서 pre-master-key 도 전송된다. 데이터 암호 알고리즘은 공개키 알고리즘보다 계산량이 적은 Block 암호 알고리즘을 사용한다.

o SSL 핸드쉐이킹

SSL의 핸드쉐이킹 과정을 순서대로 설명하면 아래와 같다.

① 클라이언트는 서버에게 클라이언트의 SSL 버전 번호, 암호 설정, 랜덤 생성 데이터 및서버가 SSL을 사용하여 클라이언트와 통신할 때 필요한 기타정보 등을 전송한다.(ClientHello)

② 서버는 클라이언트에게 서버의 SSL 버전 번호, 암호 설정, 랜덤 생성 데이터 및 클라이언트가 서버와 SSL을 사용하여 통신하는데 필요한 기타 정보 등을 전송한다. 서버는 또한 자신의 인증서를 전송하고 클라이언트가 서버의 자원을 요구한다면 클라이언트의 인증서에 대한 요구를 전송한다. (ServerHello)

③ 클라이언트는 서버를 인증하기 위해 서버가 보낸 정보를 사용하고 서버가 인증될 수 없으면 암호화 및 인증된 안전한 연결이 수립될 수 없도록 한다.(Server Certificate, ServerKey Exchange) 서버가 인증되었으면 다음 과정을 수행한다.

[그림 2-5] 암호화 순서도

④ Handshake에서 생성된 모든 데이터를 사용하여 클라이언트는 세션을 위한 premaster secret을 생성하고 이를 서버의 공개키를 사용하여 암호화한 후 서버에게 전송한다.

⑤ 서버가 클라이언트의 인증을 요구하면 클라이언트는 핸드쉐이크(Handshake) 세션에서 유일하게 알려진 데이터를 서명한다. 클라이언트는 서명한 데이터와 클라이언트의 인증서를 암호화된 premaster secret과 함께 전송한다. (ClientCertificate, Client Key Exchange, Certificate Verify)

⑥ 서버가 클라이언트의 인증서를 요청했다면 서버는 클라이언트의 인증을 시도합니다. 클라이언트가 인증되지 않으면 세션은 종료됨. 클라이언트가 인증되었다면 서버는 비밀키를 사용하여 premaster secret을 복호화하고 master secret의 생성을 위한 과정을 수행한다.

⑦ 클라이언트와 서버는 master secret을 사용하여 세션 동안에 교환될 정보의 암호화와 복호화 및 무결성에 사용될 대칭키인 세션키를 생성한다.

⑧ 클라이언트는 서버에게 앞으로의 메시지는 세션키에 의해 암호화 될 것이라는 내용과 암호화와 관련된 파라미터들을 포함하는 메시지 (Change Chipher Spec)를 송신하고 클라이언트 측 핸드쉐이크(Handshake)의 종료를 알리기 위해 Finish 메시지를 보냄. 이때Finish 메시지는 암호화 되어 전송한다.

⑨ 서버는 클라이언트에게 앞으로의 메시지는 세션키에 의해 암호화 될 것이라는 내용과 암호화와 관련된 파라미터들을 포함하는 메시지 (Change Chipher Spec)를 송신하고 서버 측 핸드쉐이크(Handshake)의 종료를 알리기 위해 Finish 메시지를 보냄. 이때 Finish 메시지는 암호화 되어 전송한다.

⑩ SSL 핸드쉐이크가 종료되고 SSL 세션이 시작됨. 클라이언트와 서버는 세션키를 사용하여 데이터의 암호화·복호화 및 송·수신을 하며 데이터의

무결성을 검사한다.(Record프로토콜)

나. 가짜 AP(Access Point)를 이용한 SSL의 해킹

1) 해킹방법

SSL은 기본적으로 서버, 클라이언트 모델로 이해할 수 있으며, SSL은 서버와 클라이언트간에 상호인증에 필요한 데이터 및 인증키 등을 인터넷을 통하여 송수신한다. SSL 해킹은 암호체계를 해킹하는 방법중에 중간자공격기법(man in the middle attack)을 활용하여 이루어지게 된다. SSL 해킹의 방법은 다음과 같다.

- 중간자공격을 하는 자는 가짜 AP를 운영하기 때문에 AP를 통과하는 모든 데이터의 내용을 읽을 수 있다.
- AP에 접속하는 클라이언트 중 일부가 서버쪽에 접근하려고 하면, 자신이 진짜 클라이언트인것처럼 서버에 접속하고 서버로부터 진짜 인증서를 발급받는다.
- 중간자공격을 하는 가짜 클라이언트는 자신이 진짜 클라이언트 인것처럼 서버쪽에 정보를 보내고, 진짜 클라이언트에게는 자신이 진짜 서버에 직접 접속한 것처럼 가짜인증서를 발급하여 속인다.
- 중간자공격자는 발급받은 가짜클라이언트의 진짜인증서를 이용하여 서버와 접속하면서, 진짜 클라이언트가 보내는 모든 정보를 다 볼 수 있다.(해킹 가능함)
- 이때 진짜 클라이언트는 중간자 공격자가 발급한 인증서를 진짜 서버의 인정서로 착각하여 정상적인 통신을 계속하면서 정보를 유출하게 된다.

[그림 2-6] 중간자공격의 개념

이렇게 중간자 해킹을 하는 이유는 중간의 모든 데이터를 볼 수 있다고 하더라도 비대칭 암호체계에서 클라이언트의 암호키를 알 수 없기 때문이며, 중간자해킹이 성공하면 중간자는 클라이언트가 입력하는 모든 정보를 볼 수 있기 때문에, 특정 사이트에 대한 아이디 및 암호를 획득하여 특정 사이트 특정 유저의 정보를 알 수 있고 변경까지도 가능하게 된다.

2) 해킹 방지 방법

AP를 사용하는 모든 사용자(스마트폰 사용자 등)는 신뢰할 수 없는 AP의 사용을 금지하고, 장기적으로는 중간자공격을 막을 수 있는 암호체계의 개발 및 보급이 필요하다.

4. 통신수단별 감청 방안

가. SNS의 감청 방안

* SNS : Social network service, 온라인 커뮤니티

SNS는 기술적으로는 감청이 가능하나, 서버가 외국에 있는 경우 서비스제공자의 협조를 강제하기 어렵고, 트위터상에서 감청대상자의 식별이 쉽지 않아 감청이 어려울 것으로 예상된다.

1) 미국의 SNS 감청 현황

미국에서는 2010년 9월 27일 뉴욕타임지에 2011년 통과를 목

표로 SNS서비스를 포함하는 모든 종류의 IP서비스, 예를 들면 facebook, 암호화된 e-mail, p2p 서비스, Skype 등에 대하여 감청 명령을 내렸을 경우에 감청이 가능하도록 하는 법안을 미법무부와 안보국이 준비하고 있다고 보도되었다.

그 법안은 암호화된 메시지를 intercept하고 이를 복호화(decryption)할 수 있어야 한다는 것도 포함되어 있어서 현재 인터넷에서 사용되는 메신저, 트위터, 페이스북, 등 SNS서비스를 포함하는 모든 종류의 인터넷 서비스는 서비스를 위한 소프트웨어 개발단계에서부터 감청을 고려하여 설계되어야 한다는 것을 내포하고 있다. 이 경우에 BlackBerry를 만든 Research in Motion 사와 같이 인터넷 서비스를 위한 서버가 외국에 있는 경우도 그 적용 대상으로 하고 있다.

CALEA에는 아직 반영되지 않은 것으로 보여 아직 관련 법안은 미의회를 통과되지 않은 것으로 판단된다.

2) SNS의 감청이슈

페이스북과 같은 소셜네트워크 서비스에서 감청 관련 이슈는 다음과 같은 것들이 있음

- 메시징 등의 통신 기능이 페이스북 또는 다른 소셜 네트워크 응용 내에서 이루어짐
- 메시징이나 채팅은 자신 또는 타인의 계정내 담벼락 등에 직접 작성하게 됨
- 소셜 네트워크 데이터 센터나 서버는 다른 국가 영역내에 존재하는 경우가 많음
- 유무선 통신에서의 CDR(Call Detail Record)과 같은 메타데이터가 소셜 네트워크 서비스에서 존재하지 않음
- 소셜 네트워크 서비스에서 감청을 위한 표준 규격이 존재하지 않음

3) SNS 서비스 감청 솔루션

소셜 네트워크 서비스에 대한 감청을 위해서 가능한 솔루션으로는 다음을 고려할 수 있음

- 이메일 등과 같이 소셜 네트워크 메시징 서비스 제공자에게 감청이 가능하도록 기능 구비를 요구하는 방안
- 소셜 네트워크 응용 서비스에서 자신의 계정을 직접 개설하여, 소셜 네트워크를 통해 교환되는 정보를 수집하는 방안
- 소셜 네트워크 응용 서비스에서 친구의 친구로 가입하여, 친구를 통해 간접적으로 정보를 수집하는 방안
- DPI 기술을 적용하여 수동적으로 소셜 네트워크 서비스를 통해 교환되는 정보를 모니터링 하는 방안
  ※ 많은 소셜 네트워크 응용 들이 암호화 기술을 적용하는 사례가 많으므로 DPI 기술을 적용한 감청은 용이하지 않고, 현재는 대부분 소셜 네트워크 서비스에 가입자로 등록하여 정보를 수집하고, 분석하는 방법이 주로 사용되고 있으며, 이러한 기능을 제공하는 관련 솔루션이 개발되어 있는 상태임

4) 트위터(twitter) 의 감청 방안

o twitter는 twitting과 direct messaging 서비스 등을 제공

① twitting : 가입자가 메시지를 작성하면 follower에게 메시지 전달
·트위터 가입자가 twit(메시지)를 남기면 트위터 서버에 저장되었다가, 그 가입자의 follower가 로그인하면 twit이 전달됨(메시지는 암호화되지 않음)

⇨ twitting은 트위터 홈페이지에 공개되어 있으므로 누구나 볼 수 있으나, 감청대상자의 트위터명을 알아야 접속이 가능

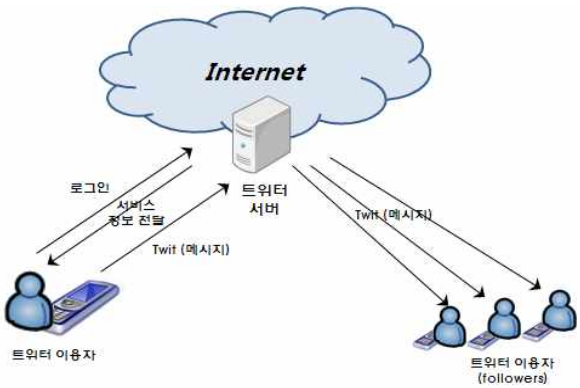
② direct messaging: twitter : 가입자가 다른 가입자에게 1:1 메시지를 보냄

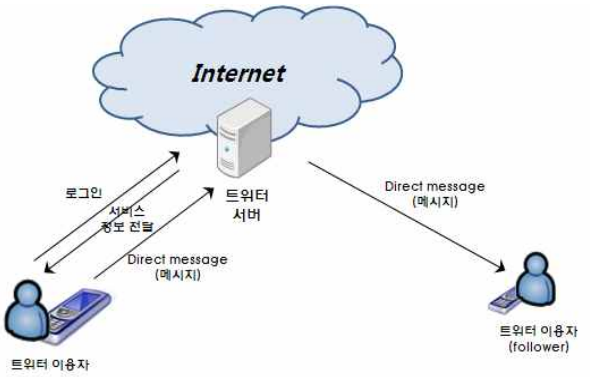
·가입자가 다른 가입자(follower)에게 direct message를 남기면 트위터서버에 저장된 후, follower가 로그인하면 메시지 전달(메시지는 암호화되지 않음)

⇨ 메시지가 암호화되지 않으므로 서비스제공자의 협조를 받을 경우 감청이 어렵지는 않으나, 트위터서버가 외국에 있어 협조를 받기 어려움

또한, 서비스제공자의 협조를 받는다 하더라도, 트위터 등 해외 SNS는 실명확인없이 이메일계정으로 가입하므로, 특히 외국 이메일 계정 사용시에는 감청 대상자를 식별하기 어려울 것으로 예상됨

[그림 2-11] 트위터를 이용한 메시지 전달 구조



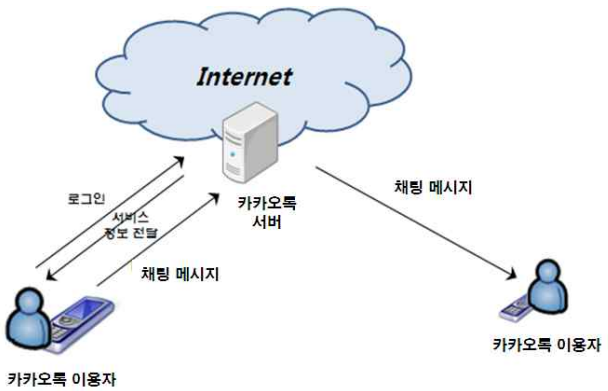


5) 모바일 메신저[카카오톡]의 감청 방안

모바일 메신저 서비스 제공 방식에 따라 기술적 측면에서의 감청 가능성 여부가 달라질 수 있으며, 카카오톡(Kakao Talk) 서비스의 경우 감청에 큰 어려움이 없을 것으로 예상

o 카카오톡 서비스 개요

[그림 2-12] 카카오톡을 이용한 메시지 전달 구조



- 카카오톡 서비스 이용자는 3G 또는 WiFi 네트워크를 통하여 서비스 이용자 간 채팅 메시지 송수신 가능
- 카카오톡 이용자(발신자)가 보낸 메시지는 카카오톡 서버에 저장되었다가, 수신자의 단말과 카카오톡 서버가 연결되면 수신자에게 전달됨
- 비슷한 형태의 메신저 서비스로 네이버톡(Naver Talk), 다음 마이피플(Daum MyPeople), 구글톡(Google Talk) 등의 서비스가 있음

o (고려사항) 메시지 암호화 및 카카오톡 메시지의 서버 경유

- 카카오톡 메시지는 WiFi 네트워크 이용 시 SSL 방식으로 암호화하며, 3G 네트워크 이용 시 암호화 하지 않는 것으로 파악됨
  ※ SSL(secure sockets layer): 인터넷 상거래시 필요한 개인 정보를 보호하기 위한 개인 정보 유지 프로토콜로 전 세계적으로 널리 사용되고 있음
- 암호화 기법 이용(WiFi 접속 시) 또는 3G 네트워크의 이용으로 무선 구간에서의 감청은 용이하지 않을 것으로 예상
  ⇨ 메시지가 카카오톡 서버를 경유하고, 서버에서 메시지 복호화가 기술적으로 가능하므로 사업자의 협조 하에 감청이 가능할 것으로 예상됨

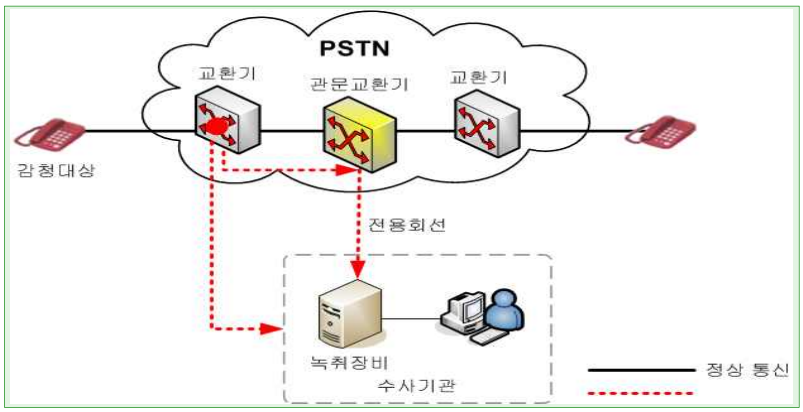
나. 일반유선전화의 감청 방안

일반유선전화는 적절한 감청설비의 설치로 감청시행이 가능하다.

① 통신사가 감청 대상 가입자의 유선전화 교환기에 감청회선을 연결

② 해당 가입자가 통화시 통화내용을 전용선을 통해 수사기관으로 전달

[그림 2-7] 유선전화 감청 흐름도



* 교환기 : 가입자 회선을 수용(집선)하는 기능 수행
* 관문교환기 : 교환기간의 데이터 처리(시내↔시외간, 유선↔이동전화 망간의 접속 등)를 수행

다. 인터넷 서비스의 감청 방안

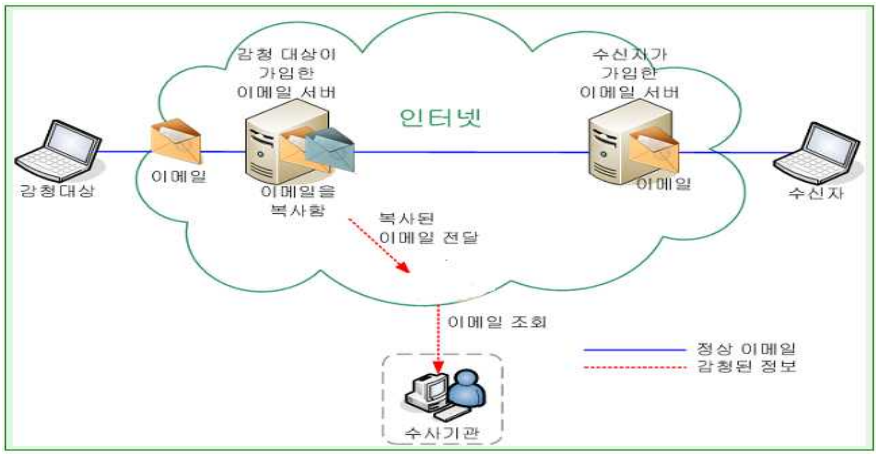
1) 이메일: 감청 시행 가능

① 통신사가 감청대상 가입자에게 송·수신되는 내용이 수사기관에도 자동 전달되도록 서버에 등록

② 감청대상자가 이메일 송수신시 통신사 서버에서 이메일 내용 복사

③ 통신사는 복사한 이메일 내용을 수사기관 담당자 이메일로 전송

[그림 2-8] 이메일 감청 흐름도



2) 비공개 게시판[카페,블로그 등] : 감청 시행 가능

감청대상이 회원으로 가입한 비공개 게시판 내용을 통신사가 CD 등으로 백업하여 수사기관에 제공

3) 메신저: 사실상 감청 불가

* 메신저 : 상대편이 인터넷에 접속해 있는지를 실시간으로 확인할 수 있으며 상호간 메시지를 교환할 수 있는 프로그램 (문자/음성/영상 채팅/파일전송 기능)

o 메시지가 암호화되어 전달되므로 감청이 어려움 (감청 요청사례 없음)

① 사용자가 로그인시 서버에서 사용자 인증

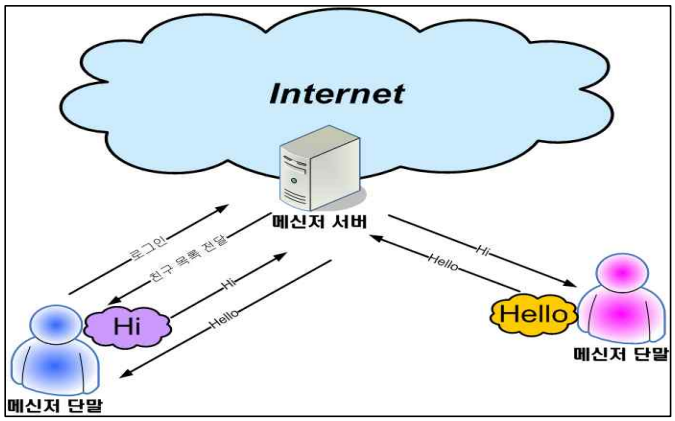
② 로그인한 사용자의 친구목록 및 접속상태 정보를 서버로부터 수신

③ 메시지 교환 (일반적으로 암호화된 상태로 전달)

- 서버 경유하여 메시지를 전달하는 경우에는 서비스 제공사업자 서버를 경유하여 메시지가 전달된다 하더라도, 통상 메시지를 암호화하므로 통신내용은 확인이 불가함

※ 사용자가 메신저 사용 종료시 '대화내용 서버 저장'여부를 묻고 사용자가 승낙시, 암호가 풀린 평문의 대화내용을 서버에 저장 (이 경우 수사기관이 형사소송법에 의한 압수수색영장으로 "송·수신이 완료된 통신내용"제공을 요청시 제공)

[그림 2-9] 메신저 서비스 흐름도 (서버경유)



- 단말간 직접 전달의 경우에는 메시지가 서버를 경유하지 않으므로 메시지를 감청할 수 있는 별도의 설비가 요구되나 구현이 매우 어려우며, 역시 메시지 암호화로 통신내용 확인이 어려움

4) 패킷감청 : 감청 시행 가능

o 패킷감청은 2004년 이전부터 시행되고 있는 것으로 알려져 있으며 수사기관이 감청대상자의 인터넷회선을 흐르는 패킷의 복사본을 통신사에서 일괄 제공받아 인터넷 통신내용을 확인하는 것이다.

- 기술적으로는 감청대상자가 송수신하는 모든 내용(통신내용, 파일 내려받기, 이메일, 게시물 등)을 수사기관이 동일하게 볼 수 있음

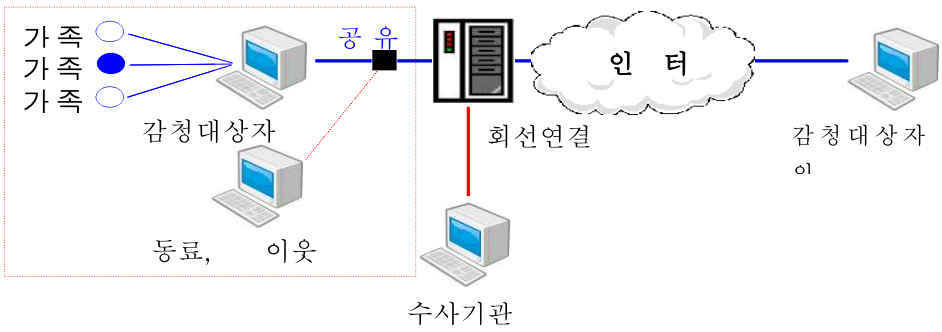
※ 실제 패킷감청은 KT등 인터넷 망사업자를 통해 한정해서 이루어지고 있는 것으로 파악되며, 패킷감청 중 음성통화내용은 암호화되어서 전송되고 있음

o (감청방식)

① 통신사가 감청 대상 가입자의 인터넷 교환기에 감청회선을 연결

② 해당 가입자가 인터넷 사용시 동일한 내용을 수사기관이 확인

[그림 2-10] 패킷감청 방식



o (쟁점사항) 패킷감청은 감청대상자의 인터넷회선을 흐르는 모든 통신내용을 볼 수 있도록 허가를 얻고 있어 너무 포괄적이라는 우려 제기

- 또한, 감청대상자와 인터넷을 공유하는 가족, 동료의 통신내용도 감청 가능

<표 2-> 유형별 감청비교

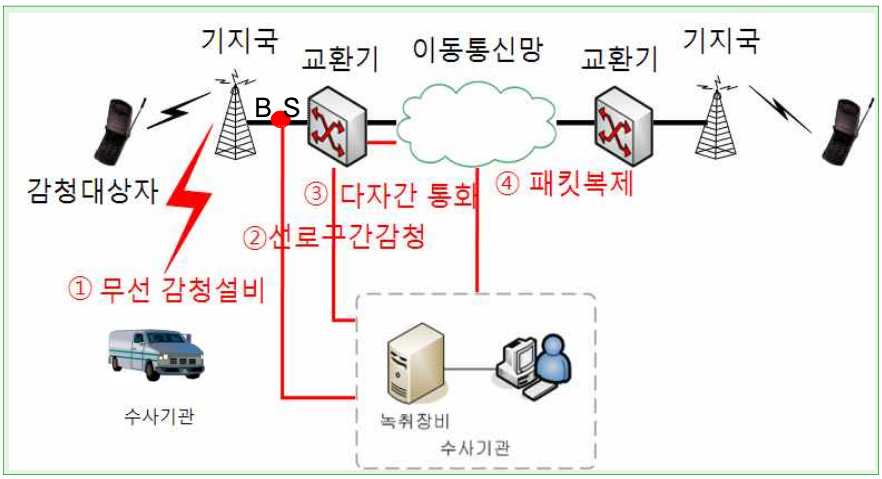
구분	인터넷 패킷감청	전화	이메일
대상자	감청대상자 (회선 공유하는 가족, 동료 가능)	감청대상자 (유선전화는 가족, 동료 가능)	감청 대상자
수집 정보	가입자회선에 대한 모든 통신내용	음성통화	이메일 내용

라. 이동전화(음성)의 감청 방안

이동전화 감청은 다양한 감청방식을 통해 가능하나, 보편적인 방식인 통신사 협조를 통한 감청의 경우 통신사에 별도의 감청설비 구축 필요

- 현재 설비 구축 비용 등의 문제로 감청 설비가 갖추어져 있지 않아 감청이 불가함

[그림 2-13] 이동전화 감청 흐름도



*BSC(Base Station Controller) : 기지국과 교환기 사이에 위치하며 기지국 관리 및 제어(주파수 출력 등)를 담당하는 장치

① (무선구간 감청) 무선 감청설비를 탑재한 차량을 이용하여 감청대상자와 기지국사이의 무선구간에서 통신내용을 획득

- 이동통신망의 기존 이동통신 설비에 대한 변경없이 감청이 가능
- 감청대상자와 동일한 기지국에서만 감청이 가능
  (감청대상자의 위치 파악이 어려울 경우 감청이 어려움)
- 수사기관의 직접 감청이 가능하므로 감청 오남용 우려가 있음

※ '05년 국정원 불법도청사건(세칭 '미림사건')에서 사용된 방법으로 당시 사용한 장비는 모두 폐기되었으며, 그 후 출시되는 이동전화에는 암호기능이 추가되어 동 방식으로 감청은 불가능한 것으로 알려져 있음

② (선로구간 감청) 기지국 제어기(BSC)와 교환기 사이에 감청장비를 설치하여 해당 선로를 통해 전달되는 통신내용을 획득

③ (다자통화방식 감청) 이동전화 교환기에 구현되어 있는 다자통화 기능을 수정하여 감청대상자의 통신내용을 획득

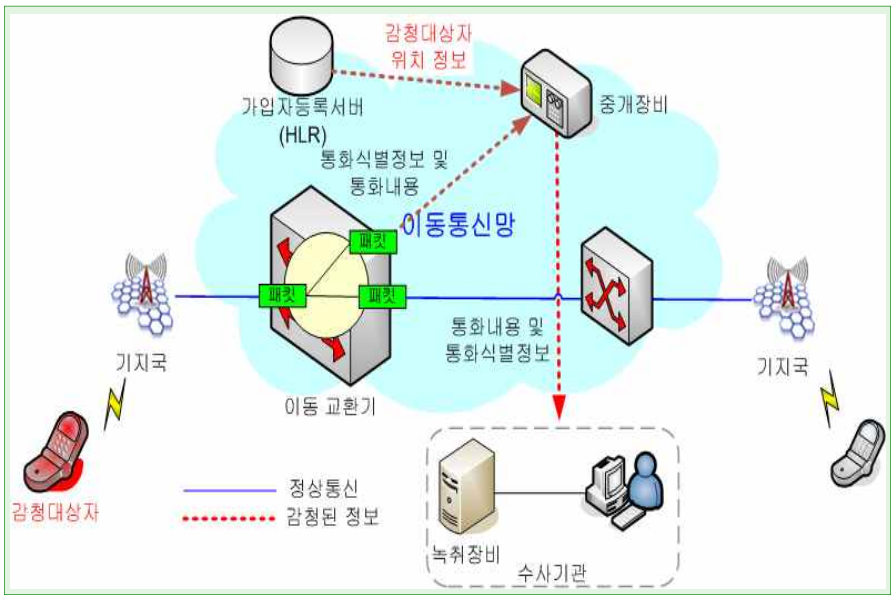
- 즉, 가입자가 상대방과 통화시 수사기관이 다자통화방식으로 당사자간 통신내용을 확인 (기술적으로 6자 통화까지 가능)

※ 동남아, 러시아 등에서 개발 적용한 사례가 있음

④ (패킷복제 감청) 이동전화 교환기에 통신정보를 복제기능을 탑재한 후 감청정보를 수사기관으로 전달

- 국외에서 WCDMA 이동통신서비스 감청을 위한 방식으로 솔루션이 개발되어 적용되고 있음

[그림 2-14] 패킷복제방식 감청 흐름도



※②~④의 경우 감청시 가입자 등록서버(HLR)에서의 가입자 식별 정보와 매칭 하여 감청 대상자의 통신내용만 수사기관에 전달

마. VOIP[Voice over IP]의 감청 방안

o 기술적으로 감청이 가능하나, 이를 위한 감청설비가 구축되지 않아 감청을 시행하지 않고 있음

o VoIP는 인터넷 또는 이동통신망을 통해 서비스가 제공되고 있으며, 감청은 기술적으로 가능하나, 별도의 감청설비가 필요함

- 인터넷망의 SBC*를 통하여 인터넷전화서비스가 제공되는 경우, 통신정보 및 통화내용을 SBC에서 추출

- SBC를 통하지 않고 제공되는 경우(기업용 등), SSW*에서 통신정보

를, 라우터에서 통신내용을 추출

*SBC(Session border controller): 인터넷전화보안장비의 일종으로 DDos등을 방어

*SSW(Soft Switch): 서킷망과 패킷망의 호처리를 제어하는 교환 장비

① 인터넷을 통한 VoIP서비스 감청

(기존 인터넷망을 보유한 통신사업자가 VoIP서비스 제공시 : KT, 온세 등)

·가입자 통화가 인터넷전화사업자의 망을 통해 이루어지므로 인터넷전화사업자를 통해 감청이 가능하나, 별도의 감청설비 필요

(인터넷망을 임차하여 VoIP서비스 제공시 : 무한넷코리아 등)

·유선전화 · 이동전화 · 인터넷망의 접속지점(Gateway)에서 감청이 가능하나, 별도의 감청설비 필요

※망임대사업자를 통한 감청도 기술적으로 가능하나, 이 경우 해당 가입자가 가입한 통신회사가 아니므로 법적 논란 소지

② 이동통신망을 통한 VoIP서비스(mVoIP) 감청

·이동통신사의 교환설비를 통해 패킷서비스 감청이 가능(인터넷패킷감청방식과 동일)하나, 별도의 감청설비 필요

※스카이프 : 별정통신사업자. 자체인터넷망이나 타사업자와의 제휴를 통해 VoIP제공

· 스카이프 가입자간 통화는 자체인터넷망을 이용하고, 이동전화 · 유선전화 · 타사업자의 인터넷전화는 스카이프가 해당 통신사와의 제휴를 통해 통화를 연결

스카이프는 메인서버가 외국(에스토니아)에 있어 국내법이 적용되지 않고, 모든 통화가 메인서버를 거치지는 않아(P2P) 감청이 어려울 것으로 예상

5. DPI(Deep Packet Inspection)에 의한 감청

가. DPI 개요

o DPI(Deep Packet Inspection)이란 어떤 종단점 장비가 아닌 임의의 패켓 네트워크 장비에 의해 패켓 내용을 분석할 수 있도록 하는 동작을 의미하며 일반적인 특징은 다음과 같다.

- L2 Frame이 1010 패턴으로 전송(물리계층)
- DPI는 새로운 기술이 아니고 오래전부터 사용되던 기술임(예, 패켓 분석 도구, 프로토콜 분석 도구 등)
- IP Packet은 “IP Header + TCP/UDP Header + Payload”로 구성되며, IP Packet 구조 만을 분석하는 것을 Simple DPI, 전송되는 데이터(즉, Payload 정보)를 분석하는 것을 Extended DPI라고 부르기도 함

► 확장 DPI를 “Application Decoding”이라고 함

► Simple DPI : 프로토콜과 응용 검출(detection)

► Advanced DPI : 메타데이터 추출 및 프로토콜과 응용 디코딩을 수행

o DPI Applications
- Security : 차세대 Firewalls, SPAM and Virus Filtering
- 트래픽 관리
- LI and Network Intelligence
  ► DPI Probe, Classification

o DPI and Encryption
- 많은 응용에서 적용되는 추세: 스카이프, 구글메일, 페이스북
- 따라서, DPI 탐지가 더욱 복잡해 짐
- 해결책:
  ► 가용한 DPI 정보 사용 (프로토콜, 서브 프로토콜, Endpoints)
  ► man in the middle
  ► interception, off-line decryption
  ► endpoint interception (trojan)

나. DPI(Deep Packet Inspection) 수행 단계 및 개념

o (Step 1) 물리적 접속을 위한 Tapping

- No Packet Loss가 요구됨
- Mirror Ports
  ► 많은 스위치/라우터에서 제공됨
  ► 성능에 제약이 있으며(Packet loss under High load), 종종 시스템당 미러 포트 수가 제약됨
  ► Full duplex link를 위해 두 개의 미러 포트가 필요

o (Step 2) probe 사용시, 패켓으로 부터 링크 계층 정보 생성

- Probe HW로는 특정 목적의 Network Measurement Systems, 표준 PC, 또는 이들을 결합한 하이브리드 시스템이

있음
► 전용 Probe HW는 값이 비싸나 PC 기반 Probe 장비의 경우, 값이 싸고 유연성을 가지는 장점이 있음
- Dump Probe vs. Smart Probe
► 스마트 프로브는 특정 기준 등에 따라 더욱 정밀하게 패킷 분석 및 결과 제공

o (Step 3) Filter out the IP packets containing relevant Content
- 대상 IP Packet이나 Contents를 어떻게 파악할 수 있는가?
► 클라이언트나 서버가 연결된 링크를 알 경우
► ISS의 빌링 정보 등에 의한 IP 주소정보 알 경우
► 패킷 분석에 의한 주소 정보 등

o (Step 4) 패킷 데이터를 분석 시스템으로 전송
- 데이터 손실이 없어야 함
- 실시간 전송 필요 --> VPN 접속 필요
- IP망은 QoS를 보장하지 않으므로 실시간 전송에 문제가 있을 수 있음

o (Step 5) 패킷 데이터 분석
- 패킷 분석의 첫 번째 단계는 TCP 헤더를 벗겨내야 함
- TCP/IP 통신의 세션 설정 단계에서 송수신되는 SYN, ACK 패켓 제거 필요
- 데이터 전송 단계에서 재전송 등에 의한 중복 패켓 제거가 필요
- 불필요한 패켓을 제거한 후, TCP 페이로드 데이터에 대한 패켓 분석을 계속 수행하여 응용 데이터에 대한 의미있는 분석 수행

다. DPI의 일반 동작 절차

o Flow Tracking (First DPI Operation)

- 양단간 통신에 해당되는 패켓 결정
- 5-tuple Flow Identifier (IP를 기반으로 플로우 구분)

o Pattern Matching (2nd Basic DPI Operation)
- 어떤 위치의 스트링, 숫자 등 검색: 보통 각 프로토콜에 대해 몇가지 패턴 존재
- 특별한 HW에 의해 처리하기도 함: Cavium, RMI etc.
  ► Example: L7-Filter, Netfilter 기반
  ► http://l7-filter.sourceforge.net)
  ► http://netfilter.org
- Linux packet fitering framework (ie. Firewall)
  ► 매우 처리가 늦어 비효율적임
- Open DPI (http://opendpi.org)
  ► 정규 표현(regular expression) 대신에 hard-copied pattern을 사용
  ► 동작 속도는 빠르나 flexible하지 못함
  ► BitTorrent 연결의 경우 복수개의 연결 설정 가능하고, 각 연결은 서로 다른 패턴을 갖게 됨

o Behavioral Analysis (Third basic DPI operation)
- 암호화된 트래픽에 대해서는 패턴 매칭이 불가능
- 대신, 암호화되지 않은 패켓의 패턴 들을 분석
  ► Packtet Sizes, Packet size sequences, Data rates, Number of concurrent flows, Flow arrival rates 등
  ► P2P는 패켓 사이즈가 HTTP와 비교시 그 패턴이 다름
  ► UDP messages의 경우, 송수신자간에 주고 받는 메시지 사이즈의 패턴으로 구분 가능 (클라이언트 - 서버간 통신: 18바이트 메시지 송신, 11바이트 메시지 수신, 23바이트 메시지 전송, 18/51/53 바이트 메시지 수신 등)

라. DPI의 세부 동작 단계 사례

o 1: Application classification with DPI
o 2: Flow Tracking
o 3: Application data stream reassembly (TCP reassembly)
o 4: Application-specific decoding
  - MIME Base64, gzip, etc.
o 5: Layer 7 identity triggers
  - 특정 응용에서 적용 가능한 키워드 검색 등 수행
  - 플로우 버퍼가 필요
o 6: Flow Correlation: intra-probe, inter-probe
  - VoIP의 경우, SIP + RTP
o 7: Intercept data forwarding
  - Content or meta data
  - Negative Filtering

6. 최근의 유무선 감청의 주요 도전 요소 들

o Mass IP Monitoring에 따른 감청의 어려움
  - 데이터 속도율 증가
    ► 감청 장비의 성능 향상 관점 보다 더 급격하게 대역폭이 증가하는 추세이다.
  - 응용 및 프로토콜의 다양화 (즉, 임의의 응용의 출현, 암호화된 프로토콜의 확대)
    ► 암호화된 트래픽이 점점 증가 (BitTorrent: 독일의 경우 23% 이상)
    ► 전세계 인터넷 트래픽 유형: 38%가 스트리밍 데이터, 8%가 암호화된 트래픽
  - 이러한 요인으로 인해 모니터링할 IP 패켓의 양이 급격히 증가하고 있으며, 이는 감청 수행을 위한 가로채기, 데이터 저장, 데이터 분석 등의 관련 작업 처리에 과부하가 걸리게 하는 요인이 되고 있다.

o Network Access 이슈에 따른 감청의 어려움이 있다.

- 패켓 들이 네트워크에서 다양한 루트로 지나가므로, 모든 루트를 모두 가로채지 못할 경우 수집한 데이터가 완전하지 않을 수 있으므로 감청 결과의 신뢰도에 영향을 미치게 됨

o 실제 개인들에 대한 수많은 e-identities의 존재로 인한 감청의 어려움이 있다.
- 일반 인터넷 사용자, 범죄자들 모두 많은 e-id 보유
- 인증되지 않은(Unauthenticated) Network Access 수단이 증가 (ex: 선불 이동전화, 공공 인터넷 접속 등)
- e-ID를 갖는 응용 숫자가 계속 증가하고 있음
  ► 웹메일, 인스턴트 메시징, 소셜 네트워크 등
- 범죄자가 갈수록 전문성을 갖추어 가고 있으며, 범죄자가 전문성이 있을 경우 이를 트랙킹 하기는 매우 어려움

제 3 장 통신비밀자료제공 통계분석업무 개선 연구

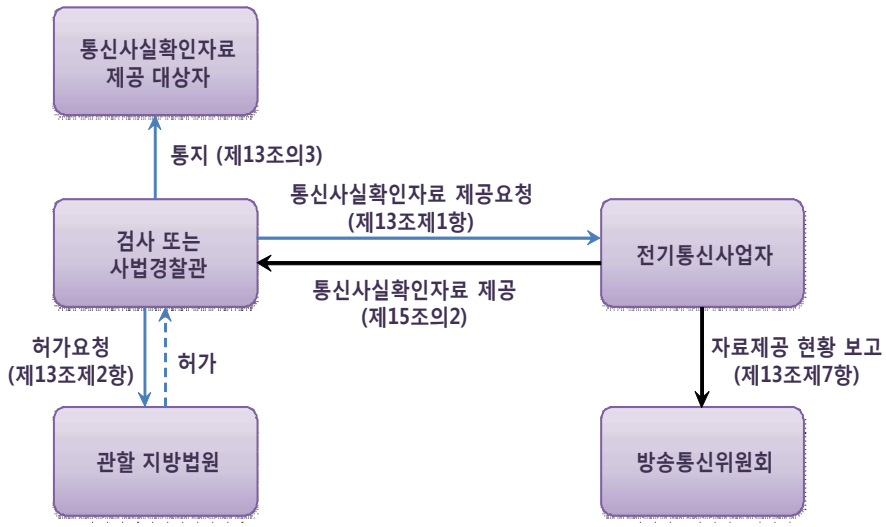
제 1 절 국내 통신비밀자료제공 보고 규정

1. 통신비밀자료 제공 절차

가. 범죄 수사를 위한 통신사실확인자료의 제공

통신비밀보호법에서 규정하고 있는 범죄 수사를 위한 통신사실확인자료의 제공 절차 및 관련 규정을 정리하면 다음과 같다.

[그림 3-1] 범죄 수사를 위한 통신사실확인자료 제공 절차



통신비밀보호법 제13조제1항, 제13조의2 및 제13조의4제1항에 따라 검사, 사법경찰관은 법원, 정보수사기관의 장은 전기통신사업자에게 통신사실확인자료의 제공을 요청할 수 있다. 검사 또는 사법경찰관은 수사 또는 형의 집행

을 위하여 필요한 경우 전기통신사업자에게 통신사실확인자료의 열람이나 제출을 요청할 수 있다(제13조제1항).

검사 또는 사업경찰관이 통신사실확인자료 제공을 요청하는 경우에는 요청사유, 해당 가입자와의 연관성 및 필요한 자료의 범위를 기록한 서면으로 관할 지방법원(보통 군사법원 포함) 또는 지원의 허가를 받아야 한다(제13조제2항). 다만, 관할 지방법원 또는 지원의 허가를 받을 수 없는 긴급한 사유가 있는 때에는 통신사실확인자료 제공을 요청한 후 지체 없이 그 허가를 받아 전기통신사업자에게 송부해야 한다.

전기통신사업자는 검사, 사법경찰관 또는 정보수사기관의 장이 집행하는 통신사실확인자료 제공의 요청에 협조해야 한다(제15조의2제1항).

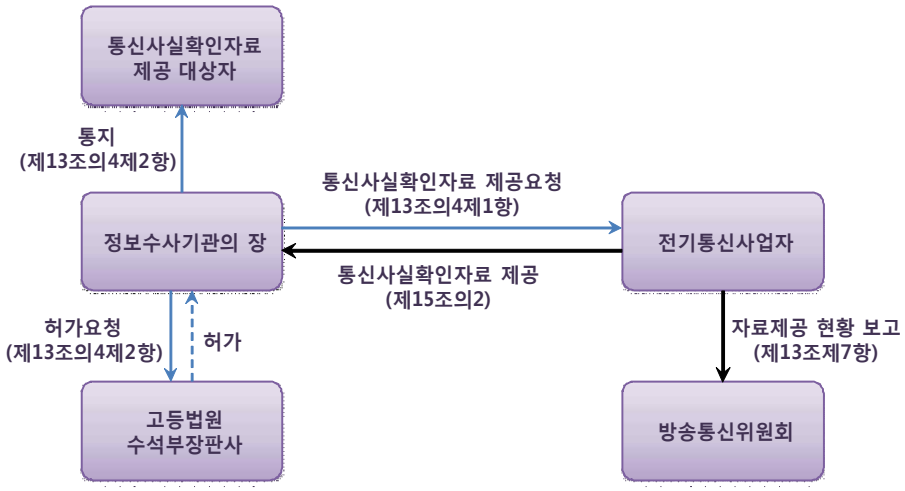
전기통신사업자는 검사, 사법경찰관 또는 정보수사기관의 장에게 통신사실확인자료를 제공한 때에 자료제공 현황 등을 연 2회 방송통신위원회에 보고해야 한다(제13조제7항).

범죄수사를 위한 통신사실확인자료 제공을 받은 사건에 관하여 공소를 제기하거나, 공소의 제기 또는 입건을 하지 않는 처분을 할 경우 그 처분을 한 날부터 30일 이내에 통신사실확인자료를 제공 받은 사실과 제공요청기관 및 그 기간 등을 서면으로 통지해야 한다(제13조의3 제1항).

나. 국가안보를 위한 통신사실확인자료의 제공

통신비밀보호법에서 규정하고 있는 국가 안보를 위한 통신사실확인자료의 제공 절차 및 관련 규정을 정리하면 다음과 같다.

[그림 3-2] 국가안보를 위한 통신사실확인자료 제공 절차



정보수사기관의 장은 국가안전보장에 대한 위해를 방지하기 위하여 정보수집이 필요한 경우 전기통신사업자에게 통신사실확인자료의 제공을 요청할 수 있다(제13조의4제1항). 기타, 국가안보를 위한 통신사실확인자료 제공과 관련한 절차 등에 관해서는 동법 제7조, 제9조 및 제9조의2제3항, 제4항 및 제6항의 규정을 따른다(제13조의4제2항).

2. 통신비밀자료 제공 집계

가. 통신사실확인자료 제공 집계 규정

통신비밀보호법 제13조제1항, 제13조의2 및 제13조의4제1항에 따라, 검사, 사법경찰관, 법원 정보수사기관의 장은 전기통신사업자에게 통신사실확인자료의 제공을 요청할 수 있다. 또한, 동법 제15조의2에 따라 전기통신사업자는 이러한 요청에 협조할 의무를 가진다.

제13조 (범죄수사를 위한 통신사실 확인자료제공의 절차) ①검사 또는 사법경찰관은 수사 또는 형의 집행을 위하여 필요한 경우 전기통신사업법에 의한 전기통신사업자(이하 “전기통신사업자”라 한다)에게 통신사실 확인자료의 열람이나 제출(이하 “통신사실 확인자료제공”이라 한다)을 요청할 수 있다.
제13조의2 (법원에의 통신사실확인자료제공) 법원은 재판상 필요한 경우에는 민사소송법 제294조 또는 형사소송법 제272조의 규정에 의하여 전기통신사업자에게 통신사실확인자료제공을 요청할 수 있다.
제13조의4 (국가안보를 위한 통신사실 확인자료제공의 절차 등) ①정보수사기관의 장은 국가안전보장에 대한 위해를 방지하기 위하여 정보수집이 필요한 경우 전기통신사업자에게 통신사실 확인자료제공을 요청할 수 있다.

이와 관련하여, 전기통신사업자는 시행령 제38조에 따라 법 제13조제1항, 제13조의2 및 제13조의4제1항에 따라 통신사실확인자료를 제공한 경우, 통신사실확인자료 제공대장에 그 제공사실을 기록해야 할 의무를 가진다.

제38조(통신사실확인자료의 제공에 관한 대장) 전기통신사업자는 법 제13조제1항, 제13조의2 및 법 제13조의4제1항에 따라 통신사실확인자료를 제공한 경우에는 통신사실확인자료 제공대장에 그 제공사실을 기록하여야 한다.

또한, 전기통신사업자는 동법 제13조제7항 및 시행령 제39조(통신사실확인자료제공의 현황보고)에 따라 자료제공현황 등을 매 반기 종료 후 30일 이내에 방송통신위원회에 보고할 의무를 가진다.

제13조 (범죄수사를 위한 통신사실 확인자료제공의 절차) ⑦전기통신사업자는 검사, 사법경찰관 또는 정보수사기관의 장에게 통신사실 확인자료를 제공한 때에는 자료제공현황 등을 연2회 방송통신위원회에 보고하고, 당해 통신사실 확인자료 제공사실등 필요한 사항을 기재한 대장과 통신사실 확인자료제공요청서등 관련자료를 통신사실확인자료를 제공한 날부터 7년간 비치하여야

한다.

시행령

제39조 (통신사실확인자료제공의 현황보고) 전기통신사업자는 법 제13조제7항에 따라 자료제공현황 등을 매 반기 종료 후 30일 이내에 방송통신위원회에 보고하여야 한다.

통신비밀보호법 시행에 관한 방송통신위원회 규정(방통위 고시 제2010-03호)에서는 통신사실확인자료제공 현황 보고를 위하여, 전기통신사업자들이 다음의 서식을 이용하도록 규정하고 있다.

1. 통신사실확인자료 제공현황 보고(지역별)

구 분		검찰청	경찰청	국가정보원	군수사기관	기타 (기관명명시)	계
통신사실확인자료제공건수	서 울						
	경기 (인천포함)						
	충남 (대전포함)						
	충 북						
	전남 (광주포함)						
	전 북						
	강 원						
	경북 (대구포함)						
	경 남(부산 ,울산포함)						
	제 주						
	계						

「통신비밀보호법」 제13조제7항, 같은 법 시행령 제39조에 따라 위와 같이 통신사실확인자료 제공현황을 보고합니다.

년 월 일

보 고 자 (서명 또는 인)

각 지역책임자 (서명 또는 인)

방송통신위원회 귀중

※ 기재요령

1. 1월 1일부터 6월 30일까지 접수된 사항은 상반기 통계로 집계하고, 7월 1일부터 12월 31일까지 접수된 사항은 하반기 통계로 집계하여 작성합니다.
2. 각 지역란의 윗칸에는 제공 문서수를, 아래칸에는 제공전화번호수(ID수 포함)를 기재합니다.
3. 기타란은 세부기관(관세청, 해양경찰청 등)별로 작성합니다.

2. 통신사실확인자료 제공현황 보고(종류별)						
구 분	검찰청	경찰청	국가정보원	군수사기관	기타 (기관명 명시)	계
통화내역						
컴퓨터통신 또는 인터넷의 로그기록자료						
발신기지국의 위치추적자료						
컴퓨터통신 또는 인터넷의 접속지 추적자료						
※ 기재요령 ① 통신사실확인자료 종류란의 위 칸에는 제공 문서수를, 아래 칸에는 제공 전화번호수(ID수 포함)를 기재합니다. ② 군수사기관은 국방부, 국군기무사령부로 구분하여 작성합니다. ③ 기타는 세부기관(관세청, 해양경찰청 등)별로 작성합니다. ④ 통화내역란에는 가입자의 전기통신일시, 전기통신개시·종료시간, 발·착신 통신번호 등 상대방의 가입자번호, 사용도수를 제공한 전화번호수를 기재합니다. 하나의 전화번호에 대하여 여러 가지 종류의 통화내역을 제공한 경우에도 제공전화번호수는 1건으로 계산합니다.						

나. 통신제한조치 협조 집계 규정

통비법 제15조 제4항에서는 통신제한조치를 집행하거나 위탁받은 기관 또는 이에 협조한 기관의 중앙행정기관의 장은 위원회 등의 요구가 있는 경우 통신제한조치보고서를 국회에 제출하도록 규정하고 있다.

제15조 (국회의 통제)
④ 통신제한조치를 집행하거나 위탁받은 기관 또는 이에 협조한 기관의

중앙행정기관의 장은 국회의 상임위원회와 국정감사 및 조사를 위한 위원회의 요구가 있는 경우 대통령령이 정하는 바에 따라 제5조 내지 제10조와 관련한 통신제한조치보고서를 국회에 제출하여야 한다. 다만, 정보수사기관의 장은 국회정보위원회에 제출하여야 한다.

제5조 (범죄수사를 위한 통신제한조치의 허가요건) ① 통신제한조치는 다음 각호의 범죄를 계획 또는 실행하고 있거나 실행하였다고 의심할만한 충분한 이유가 있고 다른 방법으로는 그 범죄의 실행을 저지하거나 범인의 체포 또는 증거의 수집이 어려운 경우에 한하여 허가할 수 있다. (이하 생략)

② 통신제한조치는 제1항의 요건에 해당하는 자가 발송□수취하거나 송·수신하는 특정한 우편물이나 전기통신 또는 그 해당자가 일정한 기간에 걸쳐 발송·수취하거나 송·수신하는 우편물이나 전기통신을 대상으로 허가될 수 있다.

또한, 통비법 시행령 제40조 '통신제한조치보고서 기재사항 등' 에서는 법 제15조제4항에 따른 통신제한조치보고서에 기재되어야 하는 사항 및 방송통신위원회의 통신제한조치 집행 위탁 및 협조 기관장에의 통계현황 제출 요청 등에 관하여 규정하고 있다.

제40조(통신제한조치보고서 기재사항 등) ① 법 제15조제4항에 따라 통신제한조치를 집행한 기관의 중앙행정기관의 장이 국회에 제출하는 통신제한조치보고서에는 통신제한조치 허가 및 승인 받은 건수, 통신제한조치 집행건수, 통신제한조치의 집행에 관한 통지건수 등 통계현황이 포함되어야 한다.

② 법 제15조제4항에 따라 통신제한조치의 집행을 위탁받거나 집행에 협조한 기관의 중앙행정기관의 장이 국회에 제출하는 통신제한조치보고서에는 통신제한 조치의 집행을 위탁받은 건수 또는 집행에 협조한 건수 등 통계현황이 포함되어야 한다.

③ 방송통신위원회는 법 제15조제4항에 따른 통신제한조치보고서를 작성하기 위하여 필요하다고 인정되는 경우에는 통신제한조치의 집행을 위탁받거나 집행에 협조한 기관의 장에게 반기마다 제2항에 따른 통계현황의 제출을 요청할 수 있다. 이 경우 제출을 요청받은 기관의 장은 특별한 사유가 없는 한 이에 응하여야 한다.

통신비밀보호법 시행에 관한 방송통신위원회 규정(방통위 고시 제2010-03호)에서는 통신제한조치의 집행을 위탁받거나 집행에 협조한 기관의 장이 통신제한조치보고서 작성을 위한 통계현황 제출 시 다음과 같은 서식을 이용하도록 규정하고 있다.

기재요령

1. 통계는 허가서 제시건수와 전화번호수(ID수 포함)로 각각 구분하여 작성합니다.
2. 총괄자료와 지역별 자료로 구분 작성하되, 지역별 통계는 서울, 경기(인천 포함), 충남(대전 포함), 충북, 전남(광주 포함), 전북, 강원, 경북(대구 포함), 경남(부산, 울산 포함), 제주로 구분하여 작성합니다.

3. 구분의 기타란은 세부기관(관세청, 해양경찰청 등)별로 작성합니다.
4. 긴급감청은 긴급감청서 접수건수로 집계하여 작성합니다.
5. 긴급감청이 사후에 허가서가 제시되어 통상감청으로 전환될 경우에도 1건의 긴급감청으로만 집계하여 작성합니다.
6. 통상감청이 기간 연장될 경우에는 1건을 추가하여 작성합니다.
7. 1월 1일부터 6월 30일까지 접수된 사항은 상반기 통계로 집계하고, 7월 1일부터 12월 31일까지 접수된 사항은 하반기 통계로 집계하여 작성합니다.

번호별 작성요령

① : 통상절차에 의한 집행협조건수
② : 긴급감청의 통상감청 전환건수
③ : 긴급절차중 협조중지건수
④ : ②+③
⑤ : 통상절차에 의한 수탁집행건수
⑥ : 긴급수탁감청의 통상감청 전환건수
⑦ : 긴급수탁감청중 중지건수
⑧ : ⑥+⑦

1. 통신감청 협조현황 보고 (총괄/지역별)

구 분		집 행 협 조						수 탁 집 행						총 계		
		통상감청 ①	긴급감청협조 통상감청전환 ②	긴급감청협조 협조중지 ③	긴급감청협조 소계 ④	협조완료 ①+②	집행협조계 ①+④	통상수탁 ⑤	긴급수탁감청 통상수탁전환 ⑥	긴급수탁감청 수탁중지 ⑦	긴급수탁감청 소계 ⑧	수탁완료 ⑤+⑥	수탁집행계 ⑤+⑧	완료계 ①+②+⑤+⑥	중지계 ③+⑦	총계
검찰	일반범죄															
	국가안보															
경찰	일반범죄															
	국가안보															
국정원	일반범죄															
	국가안보															
군수사기관	일반범죄															
	국가안보															
기타	일반범죄															
	국가안보															
계	일반범죄															
	국가안보															

2. 통신감청 협조현황 보고

구분	검찰	경찰	국 가 정보원	군 수사기관	기 타 (기관	계

					명 명시)	
전기통신 내용의 지득 또는 채록						
전기통신의 송수신 방해						
음성사서함 및 문자메시지 내용의 지득·채록						
계						

기재요령

①통계는 허가서 제시건수와 전화번호수(ID수 포함)로 각각 구분하여 작성합니다.

②군수사기관은 국방부, 국군기무사령부로 구분하여 작성합니다.

③기타는 세부기관(관세청, 해양경찰청 등)별로 작성합니다.

④「전기통신내용의 지득 또는 채록」란에는 유선사업자는 감청집행기관에 협조한 건수를 기재하고, PC통신 및 인터넷 사업자는 전자우편, 비공개모임(Closed User Group) 게시내용의 지득·채록 제공건수를 기재합니다.

다. 통신자료 제공 집계 규정

전기통신사업자는 전기통신사업법 제54조 및 형사소송법 제199조의 규정에 의하여 법원, 검사, 수사관서의 장(군수사기관을 포함), 정보수사기관의 장에게 수사 또는 형의 집행, 국가안전보장에 대한 위해를 방지하기 위해 통신자료를 제공할 수 있다. 또한, 통신사업법 제54조제6항 및 동법 시행령 제53조제2항에서는 전기통신사업자로 하여금 통신자료의 제공 현황 등을 년 2회 방송통신위원회에 보고하도록 규정하고 있다.

법 제54조 (통신비밀의 보호)

⑥ 전기통신사업자는 대통령령이 정하는 방법에 따라 통신자료제공을 한

현황 등을 년 2회 방송통신위원회에 보고하여야 하며,
방송통신위원회는 전기통신사업자가 보고한 내용의 사실여부 및
제5항에 따른 관련자료의 관리상태를 점검할 수 있다.

시행령 제53조 (통신비밀의 보호)

② 법 제54조제6항에 따른 통신자료제공 현황보고 및 같은 조 제7항에
따른 통신자료제공 현황통보는 매 반기 종료 후 30일 이내에 하여야
한다.

전기통신사업법 시행에 관한 방송통신위원회 규정(방통위 고시 제2010-03호)에서는 법 제54조제6항의 규정에 의한 통신자료제공 현황 보고 시, 다음의 서식을 이용하도록 규정하고 있다.

통신자료제공 현황보고

구 분		검찰청	경찰청	국 가 정보원	군수사 기 관	기 타 (기관명 명시)	계
가입자 인적사항 제공건수	서울						
	경기 (인천포함)						
	충남 (대전포함)						
	충북						
	전남 (광주포함)						
	전북						
	강원						
	경북 (대구포함)						
	경남(부산, 울산포함)						
	제주						
	계						

「전기통신사업법」 제54조제6항과 같은 법 시행령 제53조제2항에 따라 위와 같이 통신자료제공현황을 보고합니다.

년 월 일

보 고 자 (서명 또는 인)

각 지역책임자 (서명 또는 인)

방송통신위원회 귀중

※ 작성요령

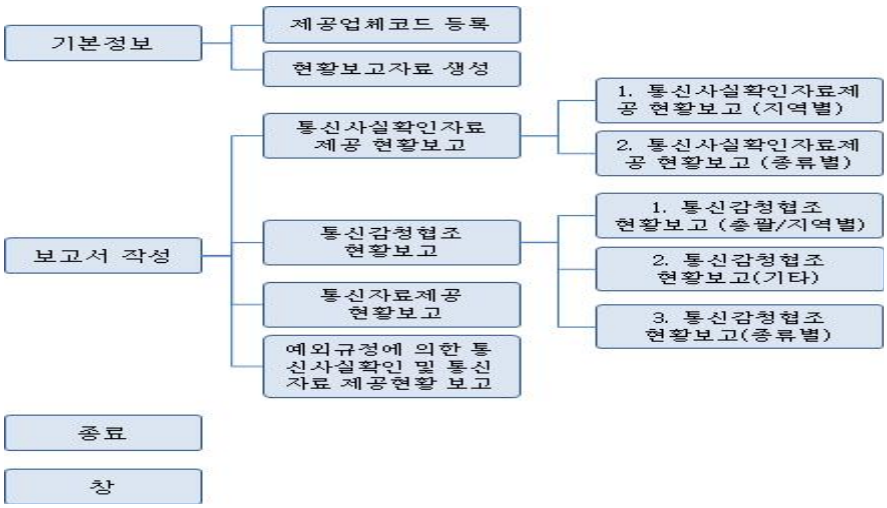
1. 1월 1일부터 6월 30일까지 접수된 사항은 상반기 통계로 집계하고, 7월 1일부터 12월 31일까지 접수된 사항은 하반기 통계로 집계하여 작성합니다.
2. 각 지역란의 윗칸에는 제공 문서수를, 아래칸에는 제공 전화번호수(ID수)를 기재합니다.
3. 기타란은 세부기관(관세청, 해양경찰청 등)별로 작성합니다.

제 2 절 통신비밀자료제공 통계도구 보완기능 개발

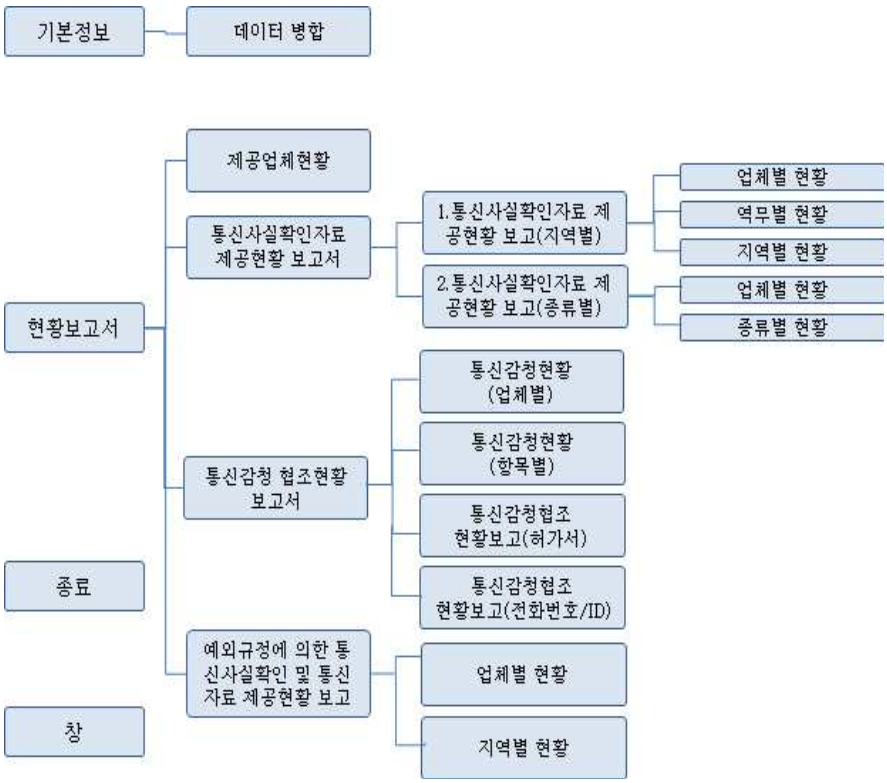
1. 개요

전기통신사업자가 방송통신위원회에 반기별로 통신비밀자료제공에 관한 통계자료를 보고하는 데 있어, 보고 및 취합의 효율성 및 정확성을 향상시키고자 당 과제에서는 통신비밀자료제공 통계보고 툴을 개발하였다. 통계보고 툴은 기본적으로 통신비밀자료 현황을 입력하기 위한 클라이언트 프로그램과, 클라이언트에서 입력된 다수의 자료를 취합하고 통계를 추출하고 보고서를 작성하기 위한 서버 프로그램으로 구성되어 있다. 통신비밀자료제공 클라이언트 프로그램은 기본적으로 통신비밀자료를 제공하는 통신사업자 및 통신서비스의 정보를 입력하는 부분, 통신비밀자료를 입력하는 부분을 포함하며, 서버 프로그램은 입력 결과를 취합하여 통계 및 보고서를 생성하는 기능 등을 포함한다. 프로그램의 메뉴 구성은 다음과 같다.

[그림 3-3] 통신비밀현황입력 툴(클라이언트 프로그램) 메뉴 구성도



[그림 3-4] 통신비밀통계분석 툴(서버 프로그램) 메뉴 구성도



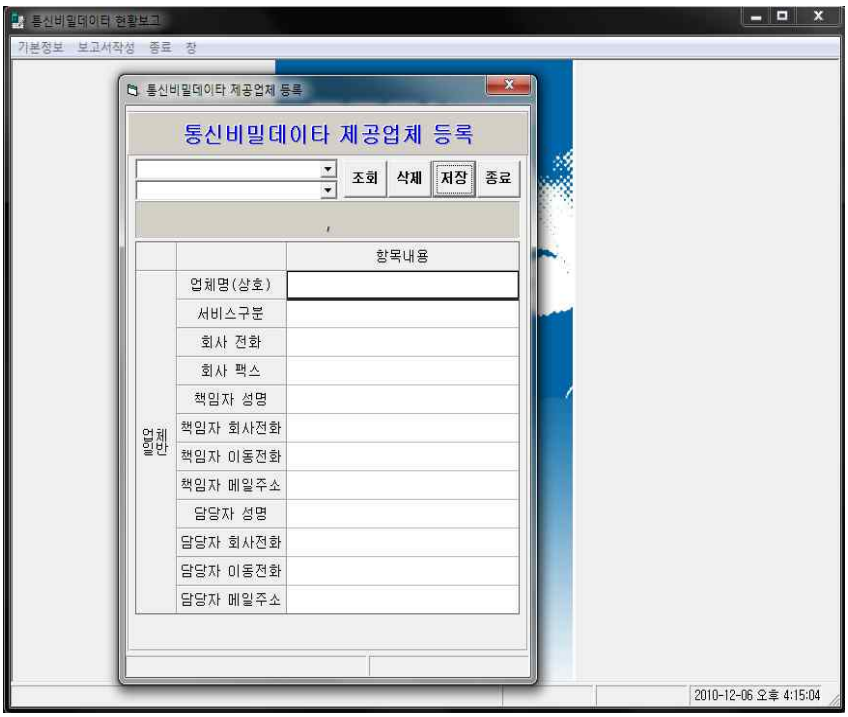
각 메뉴별 기능 및 활용 방법에 대해서는 2절과 3절에서 기술한다.

2. 통신비밀현황입력 툴(클라이언트 프로그램) 메뉴 설명

가. 통신사업자 정보의 등록

프로그램을 처음 실행시키면 다음 그림과 같이 통신비밀제공 통신사업자와 해당 통신서비스의 정보를 필수적으로 입력하도록 되어 있다.

[그림 3-5] 통비통계보고 툴 초기 화면



- 업체명(상호): 전기통신서비스 사업자 명(예. KT, LG U+)
- 서비스구분: 전기통신서비스 명(예. 유선전화, 이동전화, 전자우편 등)을 입력하되, 데이터 값의 일관성을 위하여 콤보 박스에서 선택하도록 함
- 회사 연락처: 전화, 팩스 등의 연락처 정보 입력
- 책임자 성명 및 연락처: 사업자 내부에서 통신비밀업무에 대하여 책임을 가진 자에 성명 및 연락처 정보 기입
- 담당자 성명 및 연락처: 통신비밀보호업무를 담당하는 실무자의 성명 및 연락처 기입

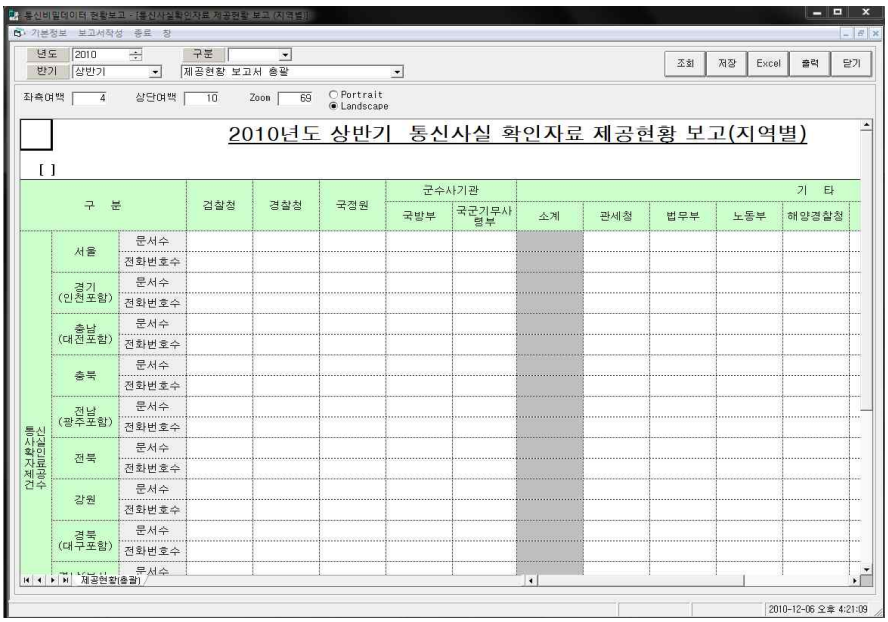
나. 데이터의 입력

통신비밀 통계 보고가 이루어질 통신사업자 및 통신서비스에 대한 정보 입력이 완료되면, 종류별 통신비밀 통계 데이터를 입력할 수 있다. 앞 장에서 살펴본 바와 같이, 통신비밀보호법 등에서 정하는 양식과 동일한 포맷을 이용하여 통신비밀데이터를 입력할 수 있다.

앞 절의 그림에서 본 것과 같이, 보고서 작성 메뉴를 통하여 통신비밀 통계 데이터의 입력이 가능하다. 보고서 작성 메뉴는 1) 통신사실확인자료 제공 현황보고, 2) 통신감청협조 현황보고, 3) 통신자료제공 현황보고, 4) 예외규정에 의한 통신사실확인 및 통신자료 제공현황 보고로 구성되어 있다. 이 때 각 메뉴는 통신비밀보호법에서 정한 양식에 따라, 지역별 및 종류별 등으로 입력 메뉴가 세분화되어 있다.

아래 그림은 2010년 상반기 통신사실확인자료 제공현황보고(지역별) 입력 화면을 예로 보여준다.

[그림 3-6] 통신사실확인자료 제공현황보고(지역별) 입력 화면



데이터를 입력하기 전에, 해당 년도 및 반기, 입력하고자 하는 데이터가 긴급인지 총괄인지의 여부를 선택하고, 제공현황 보고서 총괄, 현황 또는 기타 중에서 해당 항목을 선택한다. 제공현황 보고서 현황은 지침에서 정하는 양식과 동일한 입력양식이며, 제공현황 보고서 총괄은 이 양식에서 기타 부분을 구체적인 기관명을 써서 나열한 양식이며, 제공현황 보고서 기타는 이 중에서 기타만을 뽑아낸 양식이다. 각 양식에서 데이터를 입력하고 저장하면, 각 양식은 상호 연동되어 데이터 저장이 이루어진다. 회색으로 된 소계 란은 별도의 입력이 이루어지지 않으며, 개별 란에 데이터를 입력하면 자동으로 합계 데이터가 생성된다.

데이터 입력 시, 전기통신사업자가 통신비밀통계자료를 엑셀 형태로 기 정리한 자료가 있을 경우, 복사 및 붙여넣기 기능을 통하여 데이터

입력에 소요되는 노력을 줄일 수 있다.

데이터 입력이 완료되면 저장 버튼을 눌러서 데이터를 저장할 수 있다. Excel 버튼을 누르면 입력된 데이터를 엑셀 양식으로 저장할 수 있으며, 출력 버튼을 통해서 입력된 데이터를 출력할 수 있다.

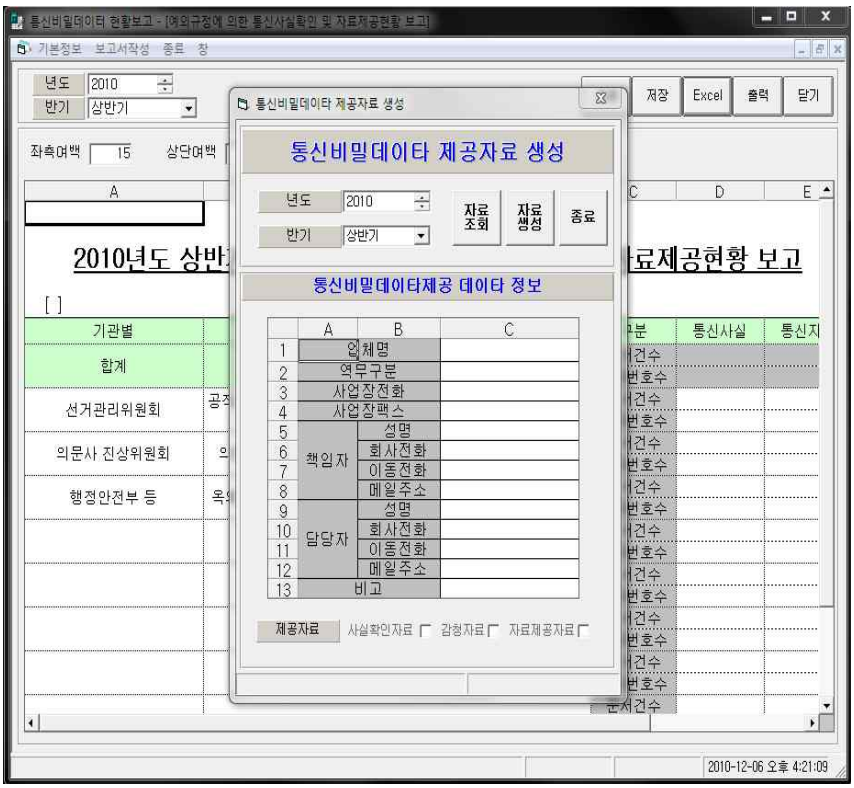
동일한 종류의 데이터를 다른 기준으로 입력하는 경우에 대한 유효성 검증 기능도 제공된다. 예를 들어, 통신사실확인자료제공 현황보고를 입력할 때, 지역별로 입력한 데이터와 종류별로 입력한 데이터의 소계가 일치하지 않을 경우 해당 내용을 메시지로 알려준다.

다. 보고서의 생성

통신비밀통계제공 데이터 입력이 끝나면, 보고서를 생성할 수 있다. 기본정보 내 현황보고자료 생성 메뉴로 들어가면 아래 그림과 같이 통신비밀데이타 제공자료 생성 창이 뜬다.

보고서를 생성하고자 하는 해당 연도 및 반기를 선택하고 자료 조회를 하면, 통신비밀통계자료를 제출하고자 하는 사업자의 정보, 통신서비스의 정보 및 현재까지 입력된 데이터가 사실확인자료, 감청자료, 자료제공자료 중 어떤 항목들을 포함하는 지를 보여준다. 조회된 데이터를 확인하고 자료 생성 버튼을 누르면 현재까지 입력된 데이터를 바탕으로 보고서가 생성된다. 다만, 입력된 데이터의 유효성 검증 결과, 데이터 간 오류가 있을 경우 보고서 생성이 이루어지지 않는다.

[그림 3-7] 보고서 생성 화면



생성되는 보고서는 지침에서 제공하는 방송통신위원회로의 보고 양식을 그대로 따르며, 생성되는 보고서를 출력하며 책임자의 서명 후 제출이 가능하다.

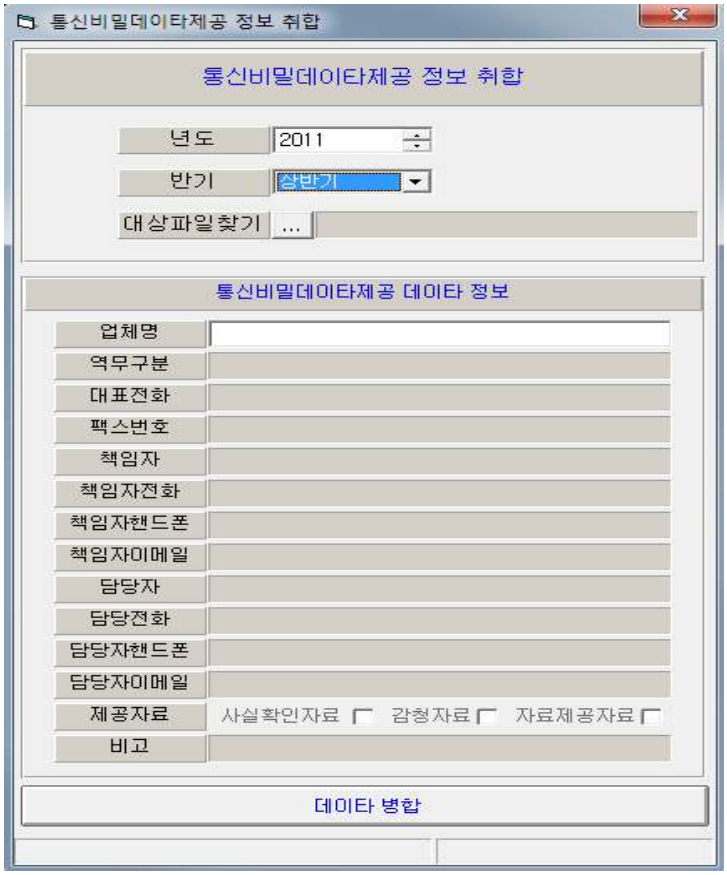
3. 통신비밀통계분석 툴(서버 프로그램) 메뉴 설명

가. 기본정보

통신비밀 통계분석 및 보고서 생성을 위하여 서버프로그램 실행후 가

장 먼저 실행하는 메뉴이다. 기본정보 메뉴의 데이터병합 서브메뉴를 클릭하면 파일로 저장되어 있는 통신비밀 관련 데이터를 통계분석 및 보고서 작성을 위하여 데이터베이스로 입력하는 기능을 수행한다.

[그림 3-8] 기본정보 메뉴의 서브메뉴인 데이터병합 실행화면



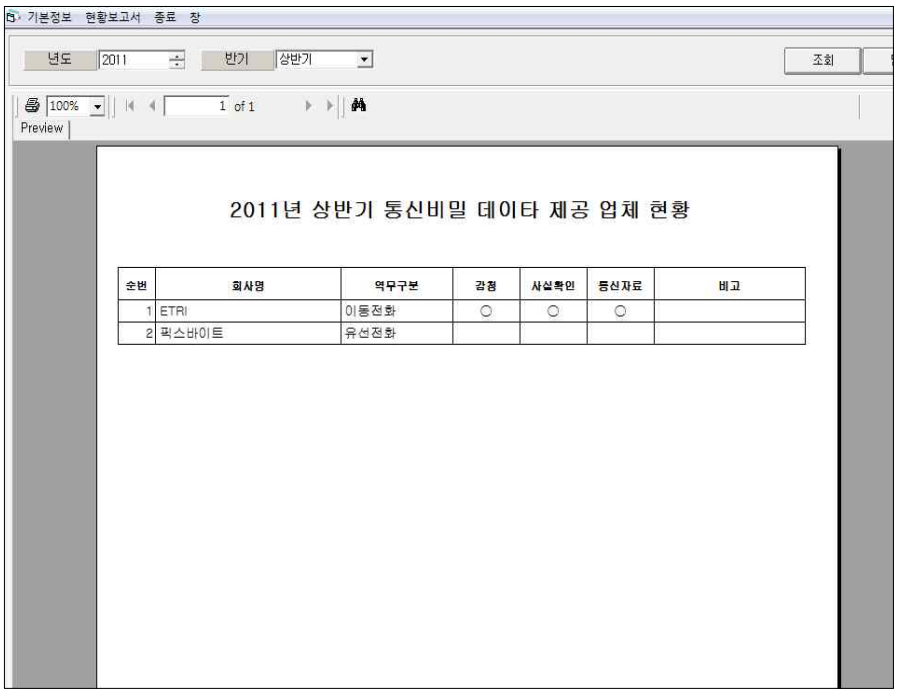
나. 현황보고서

데이터병합을 하고 나서 통계분석 및 보고서 작성을 할 수 있다. 현황

보고서 메뉴에서는 통신비밀데이타 제공업체 현황을 조회할 수 있으며, 감성/사실확인/통신자료 제공여부를 확인할 수 있다. 현황보고서 메뉴는 제공업체현황, 통신사실확인자료제공현황 보고서, 통신감청 협조현황 보고서, 예외규정에 의한 통신사실확인 및 통신자료 제공현황보고 메뉴로 구성되어 있다.

제공업체현황 메뉴에서는 년도, 분기별로 통신비밀 데이터 제공업체 현황을 조회할 수 있다.

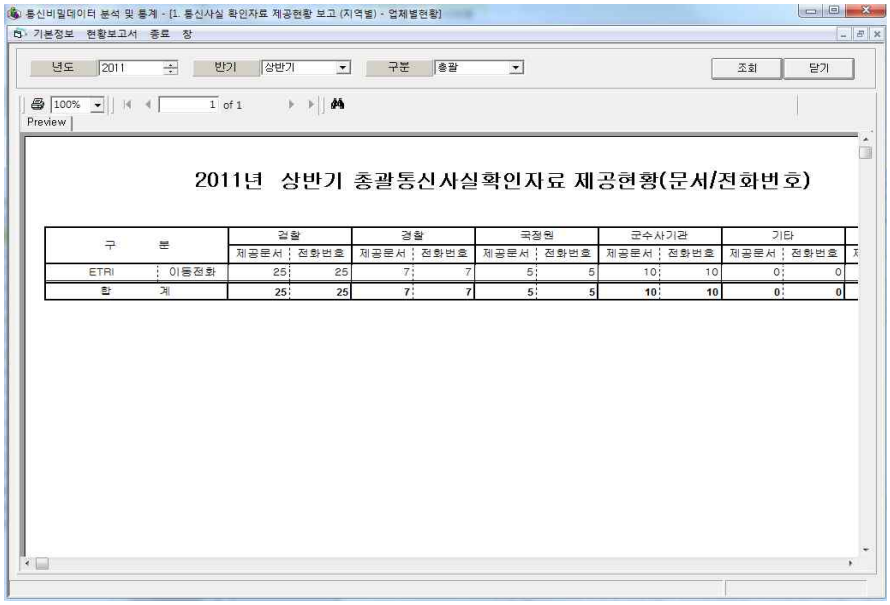
[그림 3-9] 제공업체현황 실행 화면



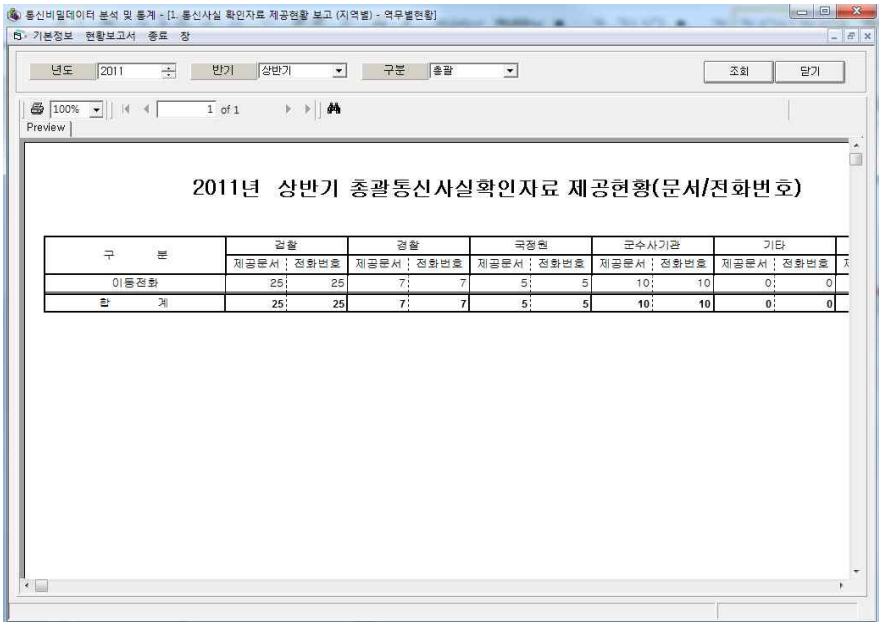
통신사실확인자료 제공현황 보고서 메뉴에서는 지역별 통신사실 확인자료 제공현황(지역별)(역무별현황, 업체별현황, 지역별 현황 구분)과 통

신사실확인자료 제공현황(종류별)(업체별 현황과 종류별 현황으로 구분)을 볼 수 있다.

[그림 3-10] 통신사실확인자료 제공현황 보고서 실행화면(지역별-업체별)

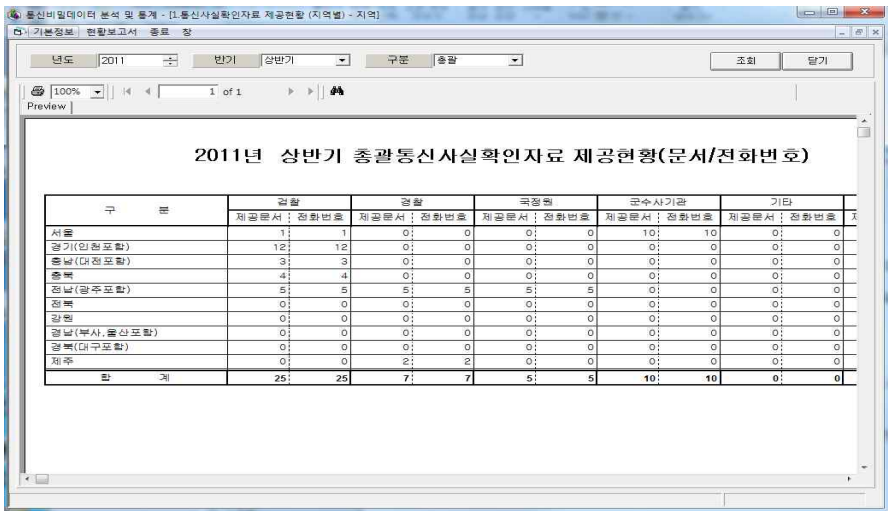


[그림 3-11) 통신사실확인자료 제공현황 보고서 실행화면(지역별-역무별)



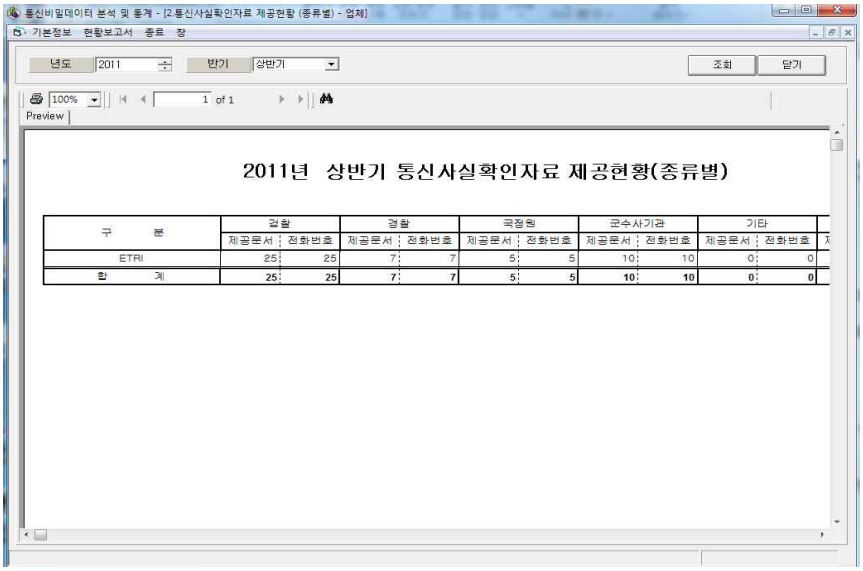
구 분	검찰		경찰		국정원		군수사기관		기타	
	제공문서	전화번호	제공문서	전화번호	제공문서	전화번호	제공문서	전화번호	제공문서	전화번호
이동전화	25	25	7	7	5	5	10	10	0	0
합 계	25	25	7	7	5	5	10	10	0	0

[그림 3-12] 통신사실확인자료 제공현황 보고서 실행화면(지역별-지역별)



구 분	검찰		경찰		국정원		군수사기관		기타	
	제공문서	전화번호	제공문서	전화번호	제공문서	전화번호	제공문서	전화번호	제공문서	전화번호
서울	1	1	0	0	0	0	10	10	0	0
경기(인천포함)	12	12	0	0	0	0	0	0	0	0
충남(대전포함)	3	3	0	0	0	0	0	0	0	0
충북	4	4	0	0	0	0	0	0	0	0
전남(광주포함)	5	5	5	5	5	5	0	0	0	0
전북	0	0	0	0	0	0	0	0	0	0
강원	0	0	0	0	0	0	0	0	0	0
경남(부사,울산포함)	0	0	0	0	0	0	0	0	0	0
경북(대구포함)	0	0	0	0	0	0	0	0	0	0
제주	0	0	2	2	0	0	0	0	0	0
합 계	25	25	7	7	5	5	10	10	0	0

[그림 3-13] 통신사실확인자료 제공현황 보고서 실행화면(업체별-업체별)

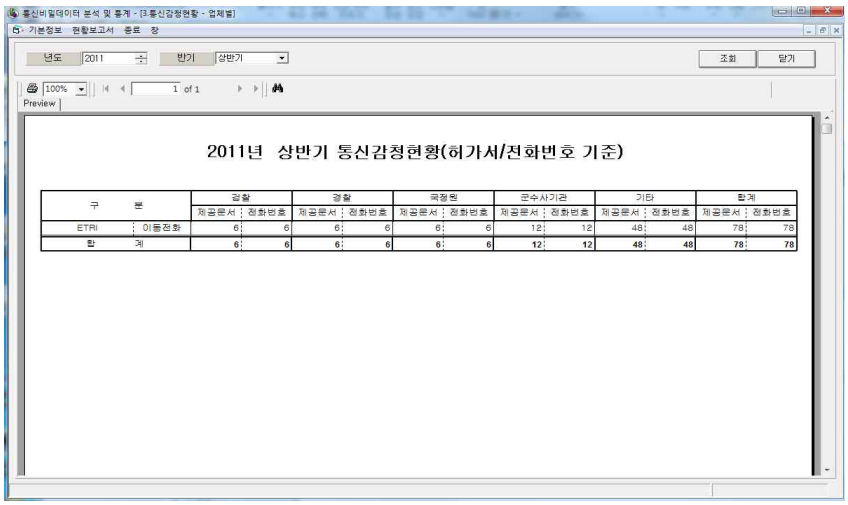


[그림 3-14] 통신사실확인자료 제공현황 보고서 실행화면(업체별-종류별)

구 분	검찰		경찰		국정원		군수사기관		기타		합계	
	제공문서	전화번호	제공문서	전화번호	제공문서	전화번호	제공문서	전화번호	제공문서	전화번호	제공문서	전화번호
통화내역	5	5	5	5	5	5	10	10	40	40	65	65
컴퓨터통신또는 인터넷의 로그 기록자료	6	6	6	6	6	6	12	12	48	48	78	78
발신기지국의 위치추적자료	7	7	7	7	7	7	14	14	56	56	91	91
컴퓨터통신 또는 인터넷의 접속지 추적자료	8	9	8	9	8	9	16	18	64	72	104	117
합 계	26	27	26	27	26	27	52	54	208	216	338	351

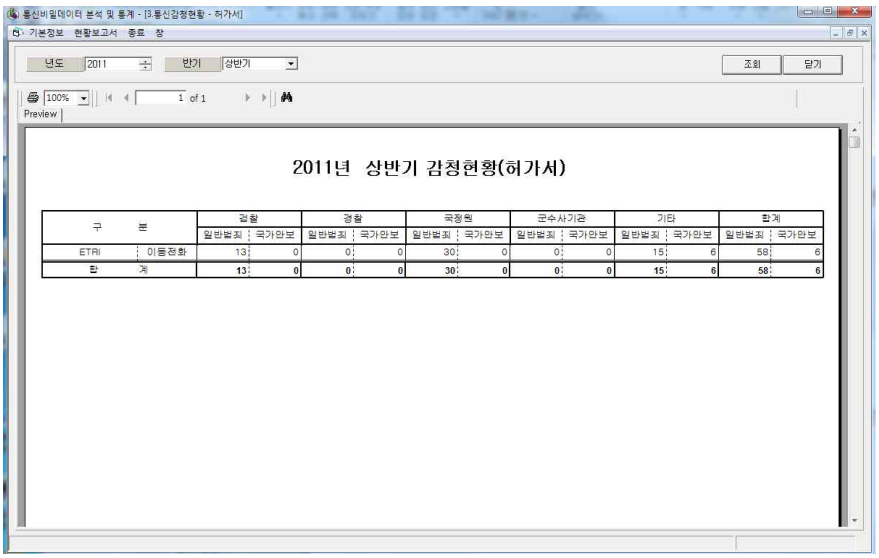
통신감청 협조현황 보고서 메뉴에서는 업체별 통신감청현황, 항목별 통신감청현황, 통신감청협조현황보고(허가서), 통신감청협조현황보고(전화번호/ID)를 조회 하고 보고서 생성을 할 수 있다.

[그림 3-15] 통신감청 협조현황 보고서 실행 화면(업체)

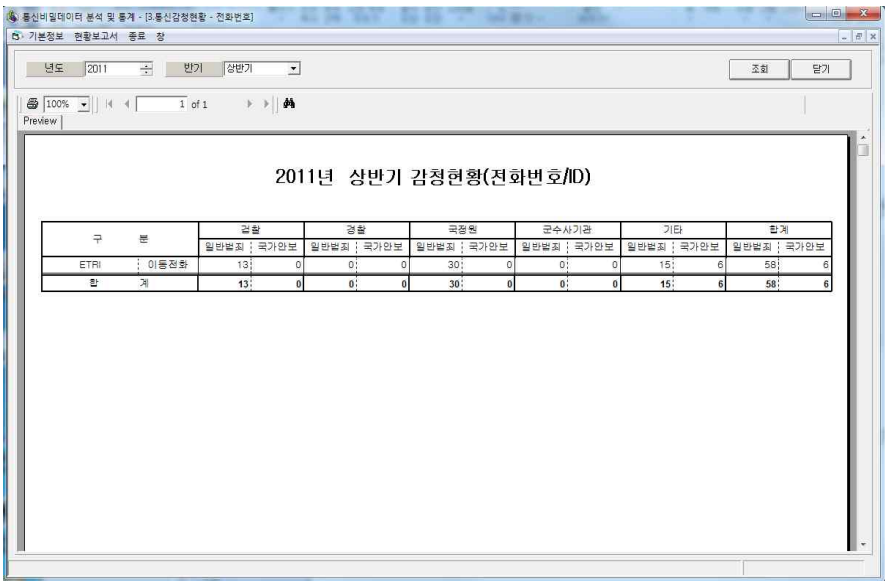


[그림 3-16] 통신감청 협조현황 보고서 실행 화면(항목)

[그림 3-17] 통신감청 협조현황 보고서 실행 화면(허가서)

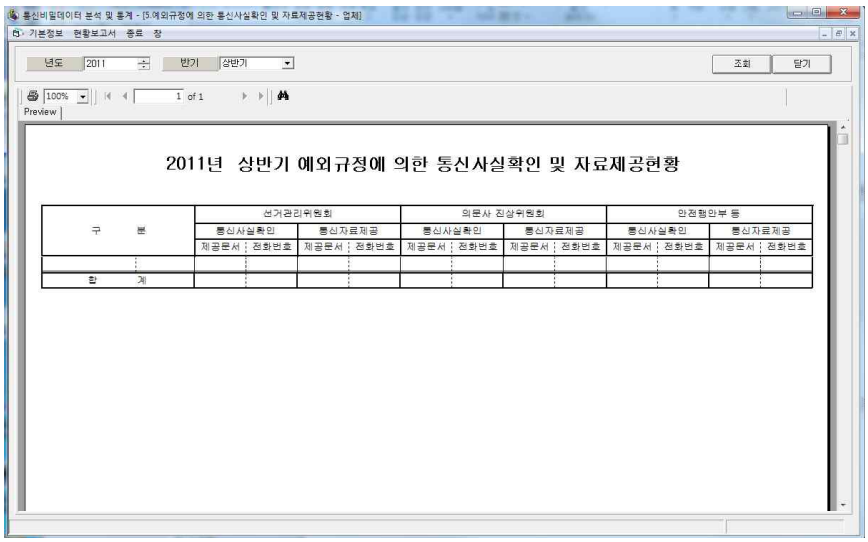


[그림 3-18] 통신감청 협조현황 보고서 실행 화면(전화번호/ID)

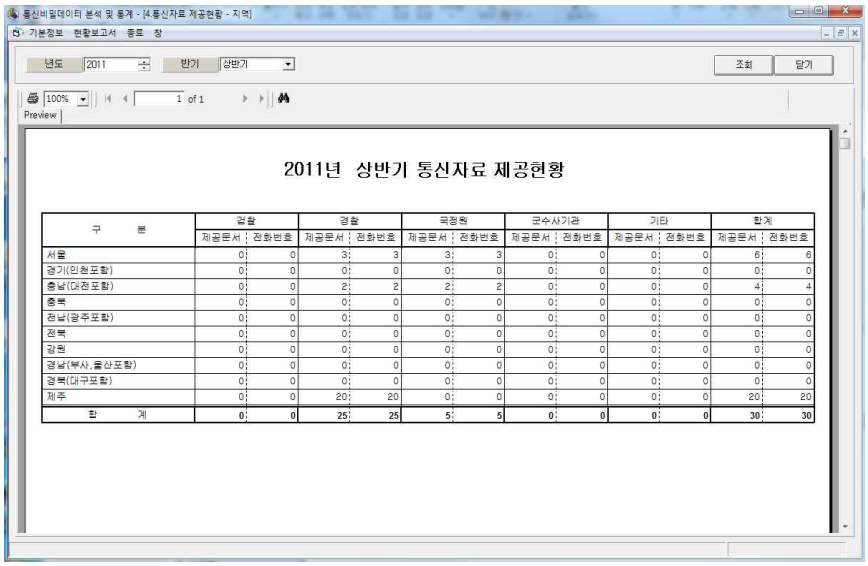


통신자료제공현황에서는 업체별 지역별 통신자료 제공현황을 년도별, 분기별로조회하고 보고서 생성을 할 수 있다.

[그림 3-19] 통신자료 제공현황-업체별

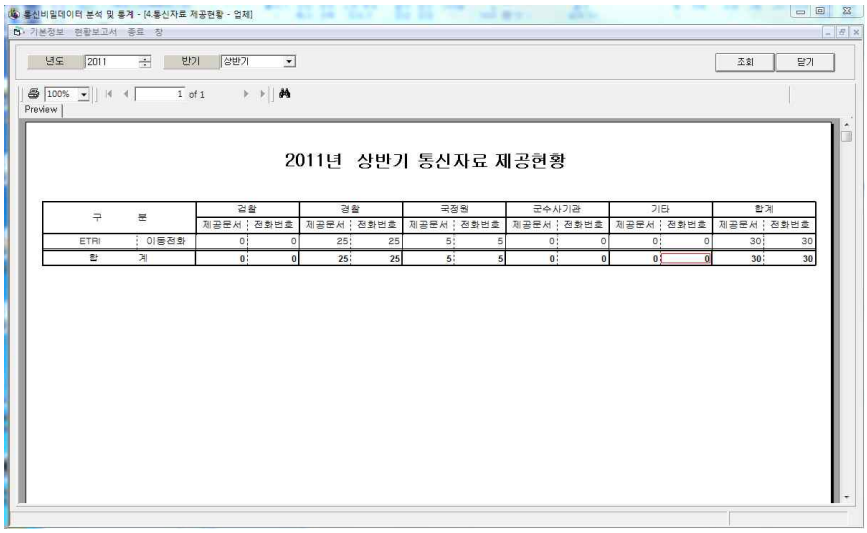


[그림 3-20] 통신자료 제공현황-지역별

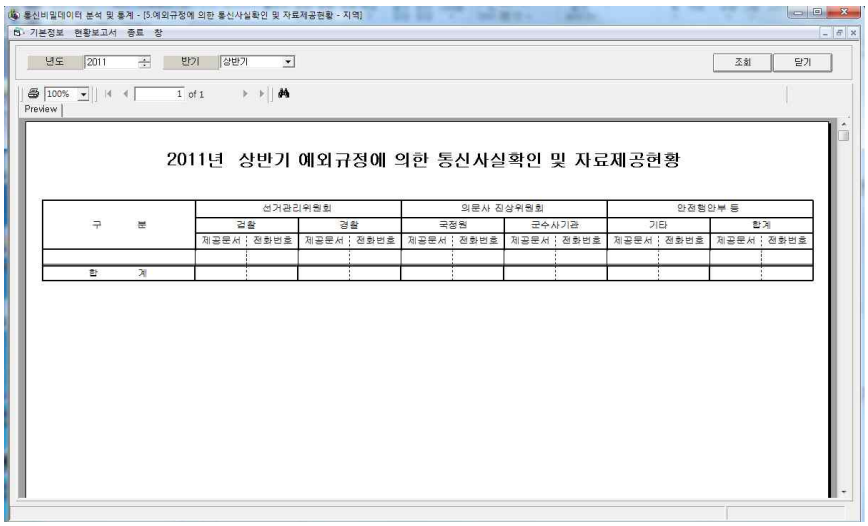


예외규정에 의한 통신사실확인 및 통신 자료 제공현황 보고에서는 업체별 현황과 지역별 현황을 조회하고 보고서 생성을 할 수 있다.

[그림 3-21] 예외규정에 의한 통신사실확인 및 통신자료 제공현황 보고-업체별



[그림 3-22] 예외규정에 의한 통신사실확인 및 통신자료 제공현황 보고-지역별



제 4 장 결 론

스마트폰 활성화와 함께 이용자가 급증하고 있는 SNS(Social Networking Service), mVoIP 등 유·무선 환경에서의 IP 응용서비스에 대한 통신제한조치의 필요성이 증가 하고 있다. 즉, 인터넷회선의 감청, 전기통신사업자에게 감청협조설비 구축의무 부과, 전자우편 감청 등의 통신제한조치의 시행의 필요성이 점증하고 있다.

이러한 추세에 맞추어 전기통신서비스에 대한 통신제한조치 집행 및 통신비밀자료 제공 등을 규제하는 현행 통신비밀보호 제도를 개정하기 위하여 다수의 통신비밀보호법 일부개정법률안이 국회에 발의되어 있다. 개정법률안은 인터넷회선의 감청, 전기통신사업자에의 감청협조설비 구축 의무 부과, 전자우편 감청 등과 같은 통신제한조치 제도 시행에 관한 규정과, 위치정보의 통신비밀자료로의 활용, 통신사실확인자료 및 통신자료의 통합 규제 등과 같은 통신비밀자료 제공 제도의 시행에 관한 규정을 신설 또는 개정하고자 하고 있다. 이와 같은 법률 개정안의 추이를 파악하였고, 또한 이와 관련하여 통신비밀보호제도 수립에 활용하기 위하여 유·무선 IP응용서비스상의 통신제한조치 기술동향을 파악하고, 인터넷 서비스 감청 국제 표준화 현황을 파악하였고, 해외사례의 연구를 수행하였다.

본 과제에서는 통신비밀보호법 개정 이슈들에 대하여 검토하고 국내외 IP응용서비스 감청제도 수립현황, 스마트폰 응용서비스 통신비밀 기술동향, 유무선 환경에서 SNS, 메신저, VoIP 서비스 감청방안 및 통신비밀 보호방안을 연구하였다.

특히, 통신비밀자료제공 통계 분석 업무의 효율성 및 정확성 향상을 위한 통계분석 및 보고서 생성 툴을 개발/업그레이드 하여 실제로 적용하고 이에

따른 보완사항을 검토하고 성능을 개선하였다. 전기통신사업자의 의견 수렴 과정을 거쳐 배포할 예정이다. 툴의 적용은 2012년 초에 이루어지는 2011년 하반기 통계자료 보고 시점부터 이루어질 예정이다. 향후 툴의 적용 사례를 기반으로 통계 분석 툴의 기능을 보완함으로써 통계자료 집계 및 분석 부분에 대한 효율성 향상을 이룰 수 있을 것으로 예상된다.

참 고 문 헌

국내 문헌

법무부, 『통신비밀보호법』, 방송통신위원회

법무부, 『통신비밀보호법 시행령』, 방송통신위원회

해외 문헌

USA Federal law, "Children's Internet Protection Act", *Congress of USA.*

USA Federal law, "Communication Assistance for Law Enforcement Act of 1994", *Congress of USA.*

● 저 자 소 개 ●

김 성 혜

· 이화여자대 전자계산학과 졸업
· 충남대 데이터베이스학과 석사
· 충남대 컴퓨터통신학과 박사수료
· 현 한국전자통신연구원 책임연구원

정 영 식

· 영남대 전자공학과 졸업
· 포항공대 전자공학과 석사
· 충남대 전자공학과 박사
· 현 한국전자통신연구원 선임연구원

박 소 영

· 한국과학기술원 산업공학과 졸업
· 한국과학기술원 산업공학과 석사
· 현 한국전자통신연구원 선임연구원

방송통신정책연구 11-진흥-가-11

IP응용서비스상의 통신제한조치 기술동향 및 해외사례연구

(Study on lawful interception policy and technology of IP applications)

2011년 12월 11일 인쇄
2011년 12월 11일 발행

발행인 방송통신위원회 위원장
발행처 방송통신위원회
서울특별시 종로 구 세종로 20
TEL: 02-750-1114
E-mail: webmaster@kcc.go.kr
Homepage: www.kcc.go.kr
인 쇄 아 회