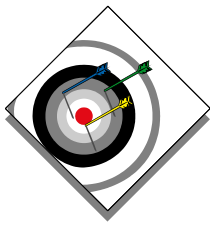


포/커/스

인터넷전화 감청 규제 및 표준화 동향

박소영* 강신각** 한재천***

감청이란 합법적인 형태의 도청을 말하며, 국내외에서 제공되는 여러 통신서비스에 대하여 이미 감청이 이루어지고 있다. 최근 세계 여러 나라에서 인터넷전화 서비스 도입을 위한 제도 확립과 서비스 제공이 활발해져 감에 따라 인터넷전화의 감청에 대한 이슈 또한 중요하게 부각되고 있다. 대표적으로 미국에서는 CALEA 의 적용 범위에 '설비기반 광대역 인터넷접속 사업자'와 '관리형 VoIP 서비스 사업자'가 포함되는 것으로 잠정 결론 내린 바 있다. 이와 같은 인터넷전화 감청 규제의 수립과 더불어 관련 기술의 표준화 활동 또한 활발하게 이루어지고 있다. CableLabs 에서는 PacketCable 프로젝트를 통하여 케이블망 환경에서의 VoIP 서비스에 대한 감청 표준 규격을 최초로 개발하였고, 이 밖에 ETSI, ATIS, IETF 등의 기구에서도 인터넷전화의 감청 표준화를 위한 연구가 진행 중에 있다. 이에 본 고에서는 외국 사례를 중심으로 인터넷전화 감청 규제 및 표준화 동향에 대해 알아본다.

목 차

* 통합망표준연구팀/연구원
** 통합망표준연구팀/팀장
*** 통합망표준연구팀/연구원

Ⅰ. 서 론

도청이란 남의 대화를 당사자의 동의 없이 은밀히 청취 및 녹음하는 것을 말하며, 감청(LI, Lawful Interception)이란 합법적인 형태의 도청을 말한다. ETSI(European Telecommunications Standard Institute, 유럽전기통신표준협회)에서는 감청을 "action (based on the law), performed by an network operator / access provider / service provider, of making available certain information and providing that information to a law enforcement monitoring facility[10]" 로 정의한 바 있다.

유선전화와 이동전화 등 국내외 여러 통신서비스에 대하여 이미 감청이 이루어지고 있으며, 인터넷

전화를 비롯한 여러 가지 IP 멀티미디어 통신서비스에 대하여 감청이 확대될 것으로 예상된다. 미국에서는 인권보호와 수사의 균형을 위해 도청이 헌법의 규제를 받는데, 법관의 영장에 근거해서 행해지는 경우에 한하여 감청이 허용되며, 도청영장을 발부하는 조건이나 절차를 정한 법률이 제정되어 있다. 독일의 경우 도청이 헌법이 보장하는 개인의 인격권을 침해하므로 원칙적으로는 허용되지 않으나, 일정 중대범죄에 관해서 수사에 필요한 경우에 한해 전신/전화 도청을 허용하는 규정이 마련되어 있다. 국내에서는 심의를 통해 일정한 요건 하에 감청을 합법화시켜 범죄수사와 국가안보를 위한 정보 수집을 용이하게 하고, 요건을 갖추지 못한 도청을 금지시켜 시민의 사생활을 제도적 틀 속에서 보호하려는 통신비밀보호법이 1993 년 12 월에 제정된 바 있다.

감청의 난이도는 통신기술의 종류에 따라 다르다. 가장 쉽게 감청할 수 있는 경우는 PSTN을 이용한 유선전화 서비스로, 교환기와의 접속을 통해 실시간으로 통화내용을 들을 수 있다. 개인의 전화번호가 전화기가 아닌 교환기에 설정되어 있어, 일반 개인도 어렵지 않게 도청이 가능하다. 이동전화의 경우 유선전화보다는 감청이 어려운 것으로 알려져 있다. 이동전화의 무선구간에서는 암호화된 CDMA 망을 타기 때문에 도청이 어려우나, 유선구간에서의 감청은 이보다 쉬운 것으로 알려지고 있으며, CDMA 원천기술을 보유하고 있는 미국 퀄컴사에서도 현재의 기술로 CDMA 도청이 충분히 가능하다고 인정한 바 있다. 인터넷전화의 경우 현재의 기술 수준으로 감청이 불가능한 것은 아니나, 일반적으로 유선전화보다는 감청이 어려운 것으로 알려져 있다. 이와 같이 인터넷 전화의 감청을 어렵게 하는 기술적 특성으로는 아래와 같은 것들이 있다.

- 패킷 형태의 음성 데이터가 일반 데이터와 함께 공중 인터넷망을 통해 흐르기 때문에, 수사기관이 인터넷전화를 감청하려면 해당 호의 패킷주소를 모아서 음성으로 복원해야 함
- 인터넷망 상에서 음성 데이터가 여러 경로로 분산되어 흐름
- 인터넷전화의 경우 전화번호가 교환기에 설정되어 있지 않고 개인이 직접 번호를 바꿀 수 있기 때문에, 감청 대상이 유동IP를 이용할 경우 통화 시 달라지는 IP를 찾아내는데 어려움이 있음

이와 같은 어려움에도 불구하고 인터넷전화가 기존 PSTN 유선전화를 대체하는 서비스로 발전해 감에 따라 인터넷전화의 감청 이슈가 중요하게 부각되고 있다. 이에 본 고에서는 외국 사례를 중심으로 인터넷전화 감청 규제 및 표준화 동향에 대해 알아본다.

II. VoIP 감청 규제 동향

1. CALEA 개요 [3]

1990 년대 초 통신 분야에 새로운 기술이 꾸준히 발전함에 따라 기존의 도청 장치와 가입자 전화 이용상황 기록장치를 공적인 목적 하에 효과적으로 사용하기가 어려워지게 되었다. 과거 유선 네트워크는 고정전환을 위한 중계소에 전선을 통하여 접속되어 있었으며, 도청장치 또는 가입자 전화 이용상황 기록장치 설치를 위해 수사기관은 해당 전화선의 위치를 확인하고 기록장치를 부착하는 것으로 충분하였다. 그러나, 전화망 방식이 아날로그 방식에서 디지털 방식으로 바뀌고 분산형 방식으로 전환되자 전화통화가 어떤 경로로 이동할 것인지 예측하기 어려워 전화를 도청하는 일이 쉽지 않게 되었다. 또한 무선통신 기술이 등장하고, 기존의 전화에 여러 가지 새로운 기능이 부가되어 전자기기를 통한 사법 감시는 더욱 어렵게 되었다. 미국 클린턴 행정부는 이러한 기술적인 발달에 대응하기 위하여 CALEA(Communications Assistance for Law Enforcement Act)를 추진하게 되었다.

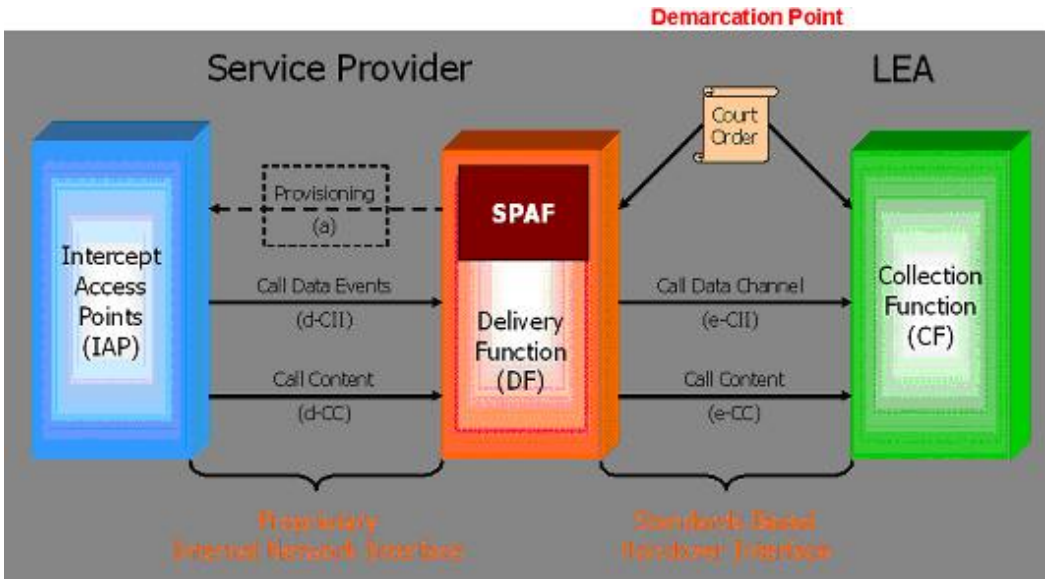
CALEA 수립에 대한 의회의 법안에 대해서 프라이버시 지지자 그룹과 통신 사업자들의 반발이 있었다. 프라이버시 지지자 그룹은 법안이 프라이버시에 대한 위협을 증가시킨다는 사실에 초점을 두었으며, 통신 사업자들은 기업에 대한 요구가 늘어남에 따라 이를 충족시키기 위한 시설 및 관리에의 투자 비용이 과다하게 소요됨을 강조하였다. 이러한 논의에 대하여 당시 FBI 국장이었던 Freeh 는 다음 세 가지 원칙을 제시함으로써 법이 지향하는 목표를 분명하게 밝혔다.

- 첫째, 민간 부문이 사법절차에 협력하는 것은 공공 책임을 분담하는 것이며 이를 위하여 표준 설정을 확립할 필요성을 인정함
- 둘째, 이에 따른 보다 강력한 프라이버시 보호 의제를 구체화함
- 셋째, 사법절차에서의 협력이 새로운 통신서비스와 기술 혁신을 저해해서는 안 됨

1994 년 10 월, 미의회는 전자감시 체제의 확립을 위하여 사법기관(LEA, Law Enforcement Agency)으로 하여금 통신사업자에 대하여 일정한 장비 설치를 의무화하는 권한을 부여하는 것을 핵심 내용으로 하는 CALEA 를 제정하였다. 다만 프라이버시 보호 원칙은 이러한 정보를 제한적으로 사용할 것을 요구하여 합리적으로 이용 가능한 범위 내에서 이용할 수 있도록 제한하고 있으며, 그 범위에 관한 구체적 기준은 FCC(Federal Communications Commission, 미 연방통신위원회)와 법원의 해석에 달려 있다. CALEA 에 구체적으로 어떤 표준이 적용될 지에 관해서는 사업자들에게 그 기준을 제시하도록 유보하였으며, 사업자단체 또는 표준화기구들이 공

개적으로 이용 가능한 표준을 제정할 수 있도록 규정하였다. CALEA 102(8)절에서는 CALEA 준수 의무를 가지는 대상의 범위를 정의하고 있는데, 기본적으로 모든 통신사업자가 이에 해당하며 유선 전송 및 스위칭 분야 관련자와 일반 사업자로서 전기통신 분야에 관련된 모든 대상을 포함한다.

1995 년, TIA(Telecommunications Industry Association, 미국통신산업협회)는 CALEA 에서 요청하는 산업계 표준으로 사법기관이 통화자 식별 정보에 접근할 수 있도록 하는 설비에 관한 표준인 IS-J-STD-025(Interim Standard: Lawfully Authorized Electronic Surveillance Standard)를 제정하기 시작하였다. IS-J-STD-025 는 TIA 의 Subcommittee TR-45.2 가 T1 과 함께 유선, 무선, 광대역 PCS 사업자와 제조업체들이 CALEA 표준으로 이용할 수 있도록 하기 위하여 개발한 임시표준이다. 이 표준은 합법적인 전자 감시를 지원하기 위해 필요한 서비스와 피쳐(feature)를 정의하며, 감청된 통신과 CII(call-identifying information)를 LEA 에 전달하기 위해 필요한 인터페이스를 기술한다. 이 표준에 대하여 법무부와 FBI 는 감청 대상에 포함되기를 희망하는 목록인 펀치리스트(punch list)를 별도로 작성하여 공표하였으며, FCC 는 1998 년 이해관계자들의 의견을 수렴하여 표준에 관하여 규칙제정공고(NPRM, Notice of Proposed Rule Making)를 수행하였다.



[그림 1] Common CALEA Implementation [4]

1999 년 FCC 는 CALEA 를 구체화하는 최종 규칙을 공표하였는데, 이는 사법절차에 협력하

여야 하는 통신사업자의 협력 범위를 결정하는 것이었다. 여기에서 TIA 가 제시한 J-STD-025 표준이 공식적으로 채택되었다. 이로써 공공 기관은 민간의 협력을 얻어 자신의 전자 감시 목적을 달성할 수 있게 되었고, 사업자들로서는 최소의 비용으로 최적의 장비를 통하여 위와 같은 의무를 달성할 수 있게 되었다. 법무부와 FBI 의 펀치 리스트에 대한 제안은 9 개 중 6 개만이 채택되었으며 그 내용은 다음과 같다.

- Subject 의 서비스에 의해 지원되는, subject 가 발생시킨 전화회의의 내용
- 다자 통화에 참가한 당사자
- Subject 나 subject 의 feature 사용으로부터 알 수 있는 모든 다이얼링 및 시그널링에의 접속 정보 제공
- Subject 의 서비스가 subject 나 상대방에게 tone 또는 네트워크 메시지를 보낼 때 이를 LEA 에 알림
- 감청된 통신의 CII 와 call content 를 연관시키기 위한 시간 정보 제공
- 통화 연결이 이루어진 이후에 subject 가 다이얼링 한 번호 제공

이후, 인터넷전화가 발달함에 따라 인터넷전화에의 CALEA 적용 여부가 주요 이슈로 떠오르게 되었다. 인터넷전화 감청에 대한 CALEA 의 적용 및 관련 규제는 다음 절에서 다루도록 한다.

2. 미국의 VoIP 감청 규제 동향

IP 기술의 발전으로 패킷 기반 통신망에 음성, 메세징, 컨퍼런스, Push-to-Talk 등 다양한 형태의 통신 서비스가 출현하면서 패킷망 환경에서의 이러한 통신 서비스에 대한 감청 요구가 제기되어 미국, 유럽 등에서 활발하게 논의되고 있다. 미국의 경우 약 2 년 전부터 적극적으로 감청 문제를 다루고 있으며, FCC 는 관련 지침 초안을 작성하여 각계 관련 기관의 의견수렴 등을 진행하고 있다.

2004 년 3 월 미 법무부, FBI 등은 CALEA 시행이 지연되는 것에 대해 해결해 줄 것을 FCC 에 요청하였다. FCC 는 IP 트래픽의 감청에 대한 이슈를 명확하게 하기 위해 2004 년 8 월에 NPRM 절차를 시작하였으며, 2005 년 8 월경 구체적 결정이 이루어질 것으로 예상된다. NPRM 은 잠정적으로 CALEA 가 '설비기반 광대역 인터넷접속 사업자'와 '관리형 VoIP 서비스 사업자'에 적용되는 것으로 결론 내렸다. 위 두 가지 서비스 사업자를 포함시킨 것은, 정보와 컨텐츠를 가진 통신이 광대역 접속 사업자와 VoIP 사업자로의 접속을 통해서만 가능할 것이기 때

문이다. 이에 따라 Vonage 와 같은 VoIP 사업자들이 FCC 의 결정에 따라 CALEA 의 적용을 받게 될 것이며, Skype 과 같은 Peer-to-Peer 통신은 CALEA 의 적용을 받지 않을 것으로 예상된다[7].

FCC 는 인터넷전화 서비스뿐 아니라 이동망에서 무전기형 음성 통화가 가능하게 하는 PoC(Push-to-Talk over Cellular) 서비스도 감청 대상으로 고려하고 있으며, 메일, 메세징 등의 서비스도 포괄적으로 포함시키려 하고 있다. PoC 는 많은 경우에 무선 데이터 네트워크 상에서 VoIP 기술을 이용하며, 여러 주요 무선 서비스 사업자들이 PoC 도입을 계획하고 있다.

3. CALEA 제시 참조표

CALEA 의 지원 기능 요구사항을 산업 전반에 실행하기 위해, CALEA Implementation Unit 은 다른 연방, 주, 지방 법원과 함께 통신산업 표준기관에 자문을 구하여 CALEA 적용의 기반으로 삼는다. 다음은 여러 종류의 통신서비스에 대하여 해당 법 집행 시 필요한 문서, 그리고 해당되는 감청 표준 간의 전후참조를 위하여 CALEA 에서 제시한 참조표와 그림이다. [3]

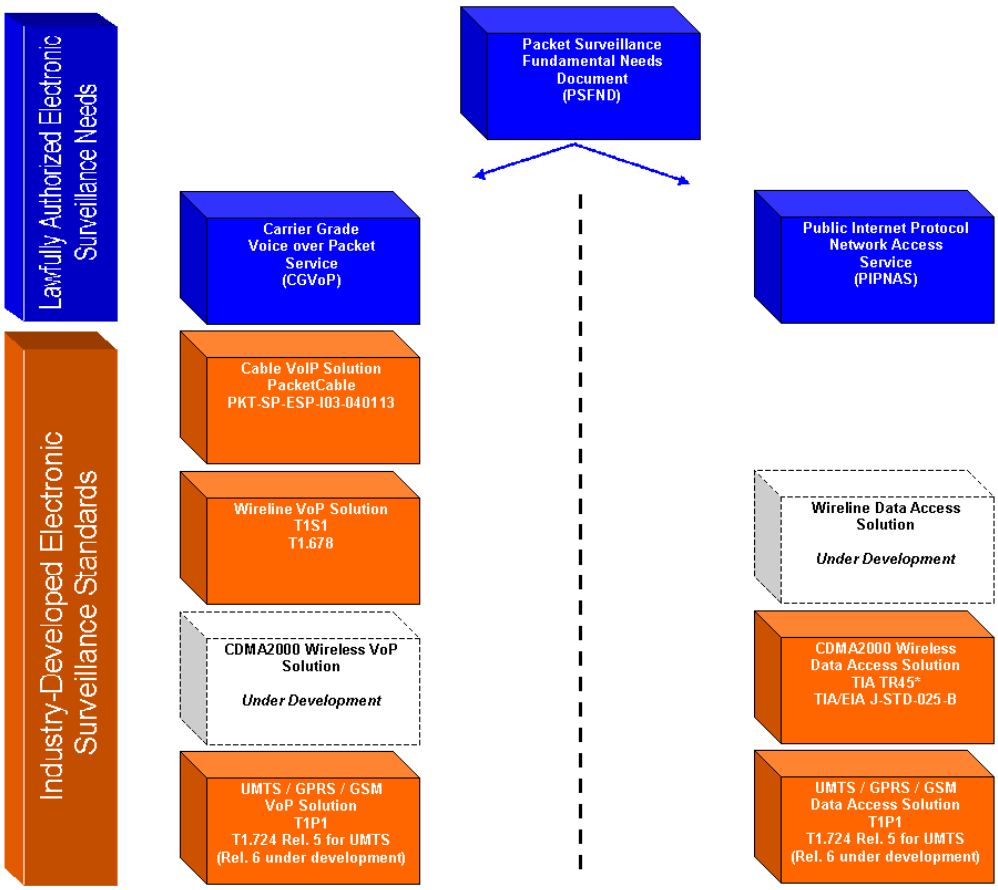
[표 1] Lawfully Authorized Electronic Surveillance Standards

Baseline	Service Type	Law Enforcement Needs	Technology & Industry Standard
Electronic Surveillance Interface Document Ver. 1.0	Voice	-	<WIRELINE / WIRELESS> TIA TR45 TIA/EIA J-STD-025-A
	Push-To-Talk		<ESMR> AMTA Electronic Surveillance for ESMR Dispatch Ver. 1.0
			<ESMR> Unknown
	Paging		<PAGING> Traditional Paging, Advanced Messaging, and Ancillary Services AAPC Suite of Standards CALEA - Ver. 1.3
Packet Surveillance Fundamental Needs Document (PSFND)	Voice	Electronic Surveillance Needs for Carrier Grade Voice over Packet Service (CGVoP)	<CABLE> PacketCable Electronic Surveillance Specification PKT-SP-ESP-I03-40113
			<UMTS / GPRS> T1P1 T1.724 Rel. 5 - UMTS
			<WIRELINE> T1S1 T1.678

			<CDMA 2000> TR45.6 - Under Development
	Push-To-Talk		<CDMA 2000 PTT> None
			<UMTS / GPRS> None
	Data Access	Electronic Surveillance Needs for Public IP Network Access Service (PIPNAS)	<CDMA 2000> TIA TR45 LAES J-STD-025-B
			<UMTS / GPRS> T1P1 T.724
			<WIRELINE> T1S1 - Under Development

출처: http://www.askcalea.net/standards.html

출처: http://www.askcalea.net/standards_packet.html#02



[그림 2] Lawfully Authorized Electronic Surveillance Standards

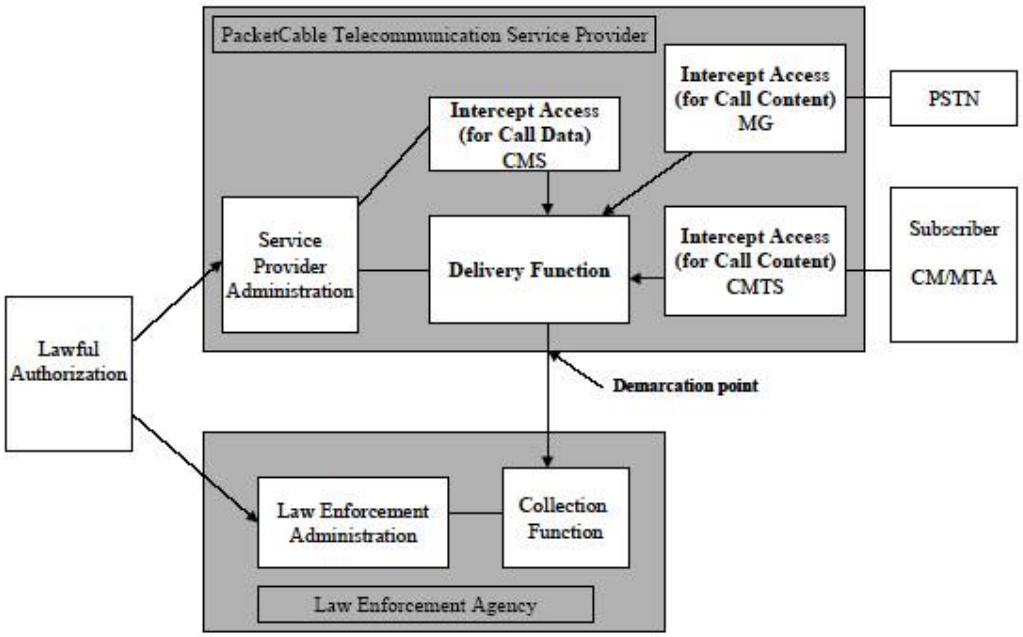
III. VoIP 감청 표준화 동향

가. CableLabs

CableLabs®(Cable Television Laboratories)는 케이블 TV 산업 구성원들에 의해 1988 년 미국에서 설립된 비영리 연구개발 컨소시엄으로, 새로운 케이블 통신 기술을 추구하고, 이러한 기술적 진보를 케이블 사업자들이 그들의 사업에 적용하는 것을 돕는 데 주력하고 있다[2].

CableLabs 에서는 PacketCable 프로젝트를 통하여 케이블망 환경에서의 VoIP 서비스에 대한 감청 표준 규격을 최초로 개발하였다. PacketCable™ 1.5 Specifications 의 일부로 개발된 Electronic Surveillance(PKT-SP-ESP1.5-I01-050128)는 합법적으로 인정되는 감청을 수행하는 LEA 를 지원하기 위하여, PacketCable™ Capabilities 를 이용하여 통신서비스를 제공하는 통신사업자와 LEA 간의 인터페이스를 정의한다. 이 표준에서 제시하는 모델은 크게 access, delivery, collection, service provider administration, law enforcement administration 의 다섯 부분으로 되어 있는데, 감청 모델과 기능 간 관계를 그림으로 나타내면 아래와 같다.

출처: PacketCableTM 1.5 Specifications [5]



[그림 3] Electronic Surveillance Model

이 밖에, 본 표준에서는 CALEA 의 요구사항을 수행할 수 있는 장비의 개발을 위해서, 해당 통신사업자는 자사의 장비, 설비 및 서비스가 아래와 같은 능력을 가지도록 해야 함을 명시하고 있다.

- 감청 대상이 되는 정보에의 접근을 위한 IAP(Intercept Access Point)의 정의
- 법원명령(court order)의 제공 및 IAP 에서의 감청 대상의 일치 확인
- 감청 대상의 통신 채널로부터의/채널로의 IAP 로부터 정보 수신
- 표준에 근거한 감청된 정보 포맷
- 법원명령에 근거한 정보 필터링
- 하나 또는 그 이상의 승인된 LEA 에게 감청된 통신 전달
- 감청된 통신의 수집, 저장 및 분석

PacketCable™ Specifications – Electronic Surveillance 표준 규격에 대한 논의는 앞으로 계속 진행될 예정이다.

나. ETSI

ETSI 는 국내 및 국제 협약과 법률제정에 부합하는 감청의 경제적 실현을 용이하게 하고자 하는 목적 하에 감청 관련 표준화 작업을 수행하고 있다. ETSI 하에 있는 LI, AT, TISPAN, TETRA, 3GPP(3rd Generation Partnership Project) 등의 여러 TC(technical committee)에서 감청 관련 표준화 작업이 이루어지고 있는데, 특히 TC LI(Technical Committee on Lawful Interception)는 ETSI 내의 감청 표준화 활동에 있어서 주도적인 역할을 담당하고 있으며, TC TISPAN 에서는 VoIP 감청에 관한 표준화 활동을 수행 중에 있다. 2005 년 6 월 기준, ETSI 에서 개발 중인 인터넷전화, IP 서비스의 감청과 관련된 주요 표준문서와 이들의 내용을 요약 정리하면 아래와 같다[6].

[표 2] ETSI 에서 개발 중인 감청 표준문서

TC	Title	Scope
LI	TS 102 232 “Lawful Interception (LI); Handover specification for IP delivery”	• Specifies the general aspects of HI2 and HI3 interfaces for handover via IP based networks – HI2: Handover Interface 2 (for Intercept Related Information) – HI3: Handover Interface 3 (for Content of Communication)

LI	TS 102 233 "Lawful Interception (LI); Service specific details for E-Mail delivery"	• Contains a stage 1 like description of the interception information in relation to the process of sending and receiving E-mail • Contains a stage 2 like description of when Intercept Related Information (IRI) and Content of Communication (CC) shall be sent, and what information it shall contain
LI	TS 102 234 "Lawful Interception (LI); Service specific details for Internet Access Services"	• A stage 1 description of the interception information in relation to the process of binding a "target identity" to an IP address when providing Internet access • A stage 2 description of IRI and CC shall be sent, and what information it shall contain
LI	TS 101 671 "Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic"	• Step 3 of a three-step approach to describe a generic Handover Interface for the provision of lawful interception from a Network Operator, an Access Provider or a Service Provider (NOW/AP/SvP) to the Law Enforcement Agencies (LEAs)
SEC LI	TR 101 944 "Telecommunications Security; Lawful Interception (LI); Issues on IP Interception"	• Identifies the problems of lawful interception of IP Stack technically
TIPHON	TR 101 750 "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON™); Security; Studies into the Impact of lawful interception"	• Describes LEA requirements for LI and the impact in a TIPHON implementation • Provides an abstract requirements and outlines a study on the impact of LI for TIPHON compliant systems
TIPHON	TR 101 772 "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 3; Service independent requirements definition; Lawful interception - top level requirements"	• Describes the top-level requirements for lawful interception in a TIPHON environment
TISPAN	TS 102 227 " Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 4; Functional Entities, Information Flow and Reference Point Definitions; Lawful Interception"	• Defines the intercept-related information to be derived from TIPHONTM release 4 networks, and its relationship to the LI framework. • Describes when messages are to be sent across the IRI reference point X2 and what they should contain

다. ATIS / TIA / IETF /ITU-T

이 외에도 ATIS, TIA, IETF 등의 기구에서 인터넷전화 및 IP 서비스 감청에 대한 논의 및 관련 표준 개발 작업이 진행되고 있다. ATIS(Alliance for Telecommunications Industry Solutions)는 빠르게 발전하는 세계의 통신 및 정보기술 분야에서 기술 및 운용 표준을 개발하기 위하여 미국에서 만들어진 단체로, 인터넷전화 감청을 위한 표준규격으로 T1.678, "Lawfully Authorized Electronic Surveillance(LAES) for Voice over Packet Technologies in Wireline Telecommunications Networks"을 개발하고 있다. 이 문서는 현재 부가 서비스와 관련된 추가적인 요구사항을 확인하는 version 2 작업이 진행중이며, transfer, conferencing 등의 multi-party call control 에 초점을 두고 있다. [1]

TIA 에서는 IP 서비스 감청을 위한 표준규격으로 J-STD-025-B, "Lawfully Authorized Electronic Surveillance"를 개발하였다. 이 문서는 LEA 가 합법적인 전자 감시를 수행하는 것을 지원하기 위한 TSP(telecommunication service provider)와 LEA 간의 인터페이스를 정의하고 있다. 이 표준은 safe harbor[1]를 지원하기 위해 개발되었으며, 따라서 이를 따르는 TSP, 제조업자 등은 CALEA Section 107 하의 safe harbor 를 가질 것이다. 향후 J-STD-025-B 에 대한 수정 작업이 이루어져 J-STD-025-C "Lawfully Authorized Electronic Surveillance"이 개발될 예정이다. 이 밖에, TIA 는 PoC 에 대한 새로운 감청 표준규격을 만들기 위한 작업을 진행 중이다. 이는 2005 년 중반 즈음에 완료될 예정이며, 모든 컨퍼런스 참여자로부터 정보와 호 이벤트를 얻는 것이 기술적인 어려움으로 작용하고 있는 것으로 알려졌다.

IETF 의 인터넷전화 감청 관련 표준문서에는 RFC 3924, "Cisco Architecture for Lawful Intercept In IP Networks" 가 있으며, 이는 IP 네트워크에서의 감청 지원을 위한 Cisco Architecture 에 대해 기술한다. 이 문서는 최소의 common interface 를 가지는 일반적인 솔루션을 제공하며, 법적 요구사항이나 규제는 다루지 않는다[8].

ITU-T 의 NGN(Next Generation Network) 표준화 작업에서도 감청 이슈에 대한 논의가 시작되었으며 감청을 포함하는 Regulatory Service 에 대한 논의가 진행되고 있으나, 아직 초기 단계에 있어 구체적인 결론에는 도달한 바가 없는 것으로 판단된다.

[1] A [TSP] shall be found to be in compliance with the assistance capability requirements under [CALEA] Section 103, and a manufacturer of telecommunication transmission or switching equipment or a provider of telecommunication support services shall be found in compliance with [CALEA] Section 106.

Ⅳ. 결론

IP 기술의 발전으로 인터넷전화, instant messaging, push-to-talk 등 다양한 형태의 통신 서비스가 출현하면서, 이러한 서비스의 감청에 대한 정책적 이슈와 기술적 이슈가 동시에 논의되고 있다. 미국의 경우에는 여러 IP 서비스에의 CALEA 적용에 관하여 약 2 년 전부터 의견 수렴이 진행되고 있어 2005 년 8 월 즈음에는 구체적인 결정이 이루어질 것으로 예상되며, 감청 기술의 표준화를 위해서 ETSI, ATIS, TIA, CableLabs 등 여러 국제표준화 기구와 단체들이 표준화 활동을 진행 중에 있다. 국내의 경우 인터넷전화 서비스 활성화를 위한 정책 수립이 상당 부분 진행되어 있어, VoIP 감청 문제 또한 정부 차원에서 해결되어야 할 필요성이 있으나, 정책적 기술적 측면에서 그 논의가 미미한 것이 현실이다. 이에, 인터넷전화 서비스가 기존 PSTN 기반 음성 서비스의 보완 서비스가 아닌 대체 서비스로 자리잡아 감에 따라, 인터넷전화의 감청 이슈는 인터넷전화의 긴급통신 서비스, 인터넷전화 스팸 등 여러 현안과 더불어, 정책적 기술적 관점에서의 적극적인 검토가 이루어져야 할 것으로 생각된다.

<참 고 문 헌>

[1] ATIS, http://www.atis.org

[2] Cable Television Laboratories, http://www.cablelabs.com/projects/

[3] CALEA, http://www.askcalea.net

[4] Cemal Dikmen, “CALEA Implementation in VoIP Networks”, Internet Telephony Conference & EXPO Miami 2005, 2005.2.

[5] “Electronic Surveillance”, PacketCableTM 1.5 Specifications (PKT-SP-ESP1.5-I01-050128), CableLabs®, 2005.1.

[6] ETSI, http://www.etsi.org

[7] FCC, http://www.fcc.gov

[8] IETF, http://www.ietf.org/rfc.html

[9] ITU, http://www.itu.int/ITU-T/publications/index.html

[10] Jaya Baloo, "Lawful Interception of IP Traffic: The European Context", 2003.7.