한국경호경비학회 – 제62호(2020): 347–367
https://doi.org/10.36623/KSSR.2020.62.15
투고일 2020. 01. 19 심사일 2020. 03. 09 게재확정일 2020. 03. 16

도청보안의 취약성 및 개선방안에 관한 연구

KSA

이 영 호 · 최 경 철 · 우 상 엽

도청보안의 취약성 및 개선방안에 관한 연구

이 영 호* · 최 경 철** · 우 상 엽***

〈요 약〉

급속한 산업의 발전으로 사회는 지식정보화 되고 정보통신의 발전으로 인하여 정보를 공유하는 측면에서 보면 손쉬운 접근과 활용이 강조되고 있다. 그러나 이러한 정보통신의 순기능과 함께 도청의 위협이라는 역기능도 증가하고 있는 실정이다.

도청 위협의 대상은 어느 기관이나 시설도 예외가 될 수 없으며, 특히 국가안보, 군사·외교정보, 정책 등의 국가 기밀 주요 정보와 첨단 산업핵심 기술, 핵심 R&D 기술, 주요 영업전략 등의 기업정보와 개인의 사생활 정보 등 불법적인 무선 정보유출로 인한 피해는 해당 영역뿐 아니라 국가적인 손실로 이어지게 된다. 아울러 도청장비의 첨단화 추세와 주변국의 도청 능력 신장 등에도 불구하고 우리나라 각 기관이나 시설은 도청 위협에 대한 보안대책이 미흡한 실정이며 대(對)도청 방지에 대하여 소극적이다. 또한 도청장비의 반입경로 및 은닉장소는 나날이 지능화되고 있으나 이에 대한 대(對)도청 보안은 여전히 취약성을 보이고 있다.

따라서 본 연구에서는 도청의 위협으로부터 정보유출을 막기 위하여, 대(對)도청 보안의 취약성을 살펴보고 기술적 측면에서의 개선방안을 제안하고자 한다. 이를 위하여 국내·외 각종 단행본 및 논문, 신문, 세미나자료 등을 수집하여 문헌연구를 통한 내용분석을 실시하였다.

분석 결과, 대(對)도청보안을 개선하기 위해서는 크게 다음과 같은 두 가지 방향의 대책이 필요하다는 사실이 발견되었다. 첫째, 도청으로 인한 보안 위협으로부터 중요 정보를 보호하기 위하여 각 대상시설 또는 부서를 보안등급화 하고 각 등급에 맞는 도청 방지 및 탐지 장비를 운용하여야 한다. 둘째, 도청보안 등급에 따라 방어 및 탐지 장비를 적용하고, 상시형 도청탐지 시스템은 도청보안 1등급에 적용하여 24시간 감시가 이루어져야 하며 회의실 또는 기타 주요시설에는 휴대형 탐지기를 이용하여 수시로 탐지 점검을 실시하여야 한다.

주제어 : 도청보안, 도청방지기술, 도청탐지기술, 도청방지시스템, 도청탐지시스템

* 경기대학교 경호보안학과 박사과정 (제1저자)
** 경기대학교 경호보안학과 박사 (교신저자)
*** 경기대학교 경호보안학과 박사과정 (공동저자)

목 차

Ⅰ. 서 론

급속한 산업의 발전으로 사회는 지식정보화 되고 정보통신의 발전으로 인하여 정보를 공유하는 측면에서 보면 손쉬운 접근과 활용이 강조되고 있다. 또한 정보통신을 이용한 정보의 공유는 인터넷, 이메일, SNS(Social Network System), 스마트폰 등과 같이 다양한 방법에 의하여 이루어지고 있다. 그러나 이러한 정보통신의 순기능과 함께 해킹이나 악성코드 감염과 같이 부정하게 국가, 기업, 개인의 정보를 빼내거나 시스템을 마비시키는 등의 침해사고도 발생하고 있다.

“이와 같은 침해위협 방법과 더불어 실내외 음성 정보 등에 대하여 불법적으로 정보를 입수하는 도청의 위협도 증가하고 있는 실정이며, 특히 중요한 기밀과 정보를 다루는 기관이나 기업의 경우 스파이에 의한 도청위협에 무방비 상태로 노출되어 각종 정보 및 기술이 유출되고 있다. 과거 냉전시대의 산물인 첩보위성, 도청장비 등이 오늘날 첨단화, 소형화 되면서 각종 정보 수집활동을 위한 매개체로 개발·진화되면서 활용되고 있다(윤해성, 2006).”

“도청 사고사례를 살펴보면, 재선의 목적으로 상대방 후보의 선거사무실에 도청장치를 하여 현직 대통령의 사임을 몰고 온 ‘워터게이트 사건’[1]이나, 최근 미국 국가

1) 워터게이트 사건(Watergate scandal)은 1972년부터 1974년까지 2년 동안 미국에서 일어난 각종 일련의 사건들을 지칭하는, 미국의 닉슨 행정부가 베트남전에 대한 반대 의사를 표명했던 민주당을

안보국(National Security Agency, NSA)이 정보 수집 차원에서 주요 국가 정상 및 주요 인사들을 대상으로 지속적인 통신 감청을 실시해왔음이 밝혀지면서, 도청에 대한 심각성이 대두되면서 대책 마련이 시급한 실정이다(이준복, 2014).”

선행연구를 살펴보면, 권오훈 외(2013)는 군사기반시설에 대한 관리 및 기술적 환경측면에서 발생할 수 있는 보안 사고를 대응하기 위하여 국내외 관리체계 및 우수사례를 분석하여 실시간 보안관리 체계를 제안하였다. 최광복(2011), 안정철 외(2008)는 사이버 국방 보안을 위한 보안관리 모델 및 대응방안을 제안하였다. 이와 같이 정보보호를 중심으로 보안관리 모델 및 보안위협에 대한 대응방안을 제시하고 있지만, 도청 위협과 관련된 관리 체계에 대한 연구는 아직 진행되지 않고 있다.

도청에 대한 보안 위협은 어느 기관이나 시설도 예외가 될 수 없으며, 국가·기업·개인의 주요한 기밀이나 정보의 불법적인 취득으로 인한 그 피해는 해당 분야에 그치는 것이 아니라 국가적인 손해로 이어지게 된다. 아울러 도청장비의 첨단화 추세와 주변국의 도청 능력 신장 등에도 불구하고 우리나라 각 기관이나 시설은 도청 위협에 대한 보안 대책이 미흡한 실정이며 대(對)도청 방지에 대하여 소극적이다.

따라서 본 연구에서는 도청으로 인한 보안 위협을 최소화하기 위하여, 대(對)도청 보안의 취약성을 살펴보고 기술적 측면에서의 개선방안을 제안하고자 한다. 이를 위한 연구방법으로 국내·외 도·감청 시스템 및 관련 법규에 대한 선행연구와 더불어 각종 단행본 및 논문, 신문, 인터넷, 세미나 자료 등을 수집하여 내용분석(Contents analysis) 연구를 실시하여 문헌연구 하였으며, 대(對) 도청방지 및 탐지에 대한 기술적 접근 방법은 현재 실무에서 활용하고 있는 장비에 대한 자료를 관련업체에 요청·수집하여 분석하였다.

저지하려는 과정에서 일어난 불법 침입과 도청 사건과 이를 부정하고 은폐하려는 미국 행정부의 조직적 움직임 등 권력 남용으로 말미암은 정치 스캔들이었다. 사건의 이름은 당시 민주당 선거운동 지휘본부(Democratic National Committee Headquaters)가 있었던 워싱턴 D.C.의 워터게이트 호텔에서 유래한다. 처음 닉슨과 백악관 측은 ‘침입사건과 정권과는 관계가 없다’는 입장을 고수했으나, 1974년 8월, ‘스모킹 건’이라 불리는 테이프가 공개됨에 따라 마지막까지 남아 있던 측근들도 그를 떠나게 되었다. 닉슨은 미 하원 사법위원회에서 탄핵안이 가결된 지 4일 뒤인 1974년 8월 9일, 대통령직을 사퇴하였다. 이로써 그는 미 역사상 최초이자 유일한, 임기 중 사퇴한 대통령이 되었다(위키백과, 검색일 2019. 10. 15.).

Ⅱ. 이론적 배경

도청(Eavesdropping)이란 '대화 등을 몰래 엿듣는 일'로 개인의 이익을 위한 목적으로 타인의 동의나 허락 없이 각종 정보를 입수하는 행위로, 유·무선 및 기타 장치에 의한 감시 또는 녹음·청취하는 행위를 의미한다(오혁근, 2001).

한편, 「통신비밀보호법」에 의하면, 감청이란 전기통신에 대하여 당사자의 동의 없이 전자장치·기계장치 등을 사용하여 통신의 음향·문언·부호·영상을 청취·공독하여 그 내용을 지득 또는 채록하거나 전기통신의 송·수신을 방해하는 것을 말한다(동법 제2조 제7호).

1. 도청을 이용한 보안위협 기술

1) 무선 도청 기술

도청 기술이 첨단화되면서 저주파(Very Low Frequency, VLF), 극초단파(Extreme High Frequency, EHF)와 디지털로 그 영역을 넓혀가고 있으며, 불법 도청 운용방식 또한 지능화되고 있다. 구체적인 무선 도청 방법은 다음과 같다.

"Throwdown Bug는 도청탐색자가 의도적으로 설치된 도청기를 발견하고, 도청탐지가 끝났다고 생각되도록 유도하는 도청의 방법으로 실제 도청기는 더 은밀하게 숨긴다. Snuggled Bug는 일반 공중파 방송의 주파수에 도청기의 주파수를 밀착시켜 도청탐색자가 도청주파수를 찾았을 경우 공중파 방송으로 오인할 수 있도록 유도하는 방법이다. Burst Bug는 도청기에서 3~4시간 가량의 음성정보를 압축 저장한 후 일정시간이 되면 저장된 정보를 일순간에 송신하는 기술로 평상시에는 주파수가 나타나지 않는다. Frequency Hopping Bug는 보안용으로도 사용하는 기술로써 일정한 주파수 대역에서 주파수를 변경하는 도청기로 50MHz 대역을 초당 500번의 주파수로 변경 가능한 기종도 있다. Carrier Current는 음성을 반송파에 실어 전선이나 전화선에 흘려보내는 기술로 여러 방법에 적용되어 도청되는 장소에서 벗어난 지역에서 녹음, 무선 송신기로 재전송 등을 할 수 있다. Laser Transmission은 레이저 도청으로 외부에서 창문으로 레이저를 쏘아 창문의 진동을 수신기에서 분석하여 음성으로 변환하는 것이다(한국정보통신기술사협회, 2005)."

2) 유선 도청 기술

유선 도청 기술은 전화기 내부, 선로 단자함, 전주 등 모든 구간에서 도청의 위협에 노출되어 있으며, 도청 목표물 주변뿐만 아니라 원격지에서도 도청이 행해질 수 있다. 구체적인 유선 도청 방법은 다음과 같다.

"직렬 연결형 도청기는 전화선 한 쪽 라인에 도청기를 연결하여 전화사용 시 통화내용을 무선으로 송출하여 도청하는 방법이다. 병렬 연결형 도청기는 전화선에 병렬로 접속되어 전화선의 전류 및 소리로 작동되며 별도의 전원 공급이 필요하다. 유도(Inductive Pickups) 도청기는 전화사용 시 전화선로 주위에 유도되는 자기장의 변화를 이용하여 음성을 도청하는 방법이다. 슬레이브(Slaves) 도청기는 도청 대상자가 전화를 사용할 때 도청기의 자동 회로가 도청 수신지로 전화를 걸어서 도청하는 방법이다. 톤 활성(Tone Activated) 도청기는 전화 통화가 가능한 어느 곳에서든지 도청 대상에게 전화를 걸어서 특정 주파수를 송출, 톤 활성 도청기를 작동시켜 별도로 설치한 마이크로폰을 통해 내부음성을 도청하는 방법이다. 훅 스위치 바이패스(Hook switch Bypasses)는 훅 스위치에 저항, 콘덴서, 작동유지 다이오드 등을 연결하여 송수화기를 통해 내부의 음성을 도청하는 방법이다. '여유배선 도청'은 전화기에 연결된 선로 중 여분의 선로에 마이크소자(전화기 내부의 수화기 마이크, 스피커폰의 마이크, 스피커, 링거 등)를 연결하여 내부의 음성을 도청하는 방법이다. 'T1 및 E1 회선 도청'은 중·소규모의 교환기에 주로 연결된 DID(Direct Inward Dialing) 회선(T1, E1)을 Check하는 장비의 기능 중에 각 채널을 모니터링 하는 기능을 이용하여 도청하는 방법이다.[2] 녹음형(Tape Recorders) 도청기는 전화선에 병렬로 녹음기를 연결하여 전화사용 시 자동으로 작동시켜 도청하는 방법이다(한국정보통신기술사협회, 2005)."

3) 키폰시스템(Key-Phone) 및 구내교환기(PBX) 도청 기술

키폰시스템이나 구내교환기의 프로그램을 활용하여 도청하는 방법은 다음과 같다.

"통화 중 듣기 기능(Executive override)은 통화중인 도청대상에게 프로그램을 활용하여 인지하지 못하도록 끼어들어서 통화내용을 도청하는 방법이다. 브릿지접속(Bridged Extension)은 도청대상 회선에 물리적으로 직접 연결하지 않고 프로그램 상

2) 북미방식(T1) – 음성24채널, 유럽방식(E1) – 음성30채널

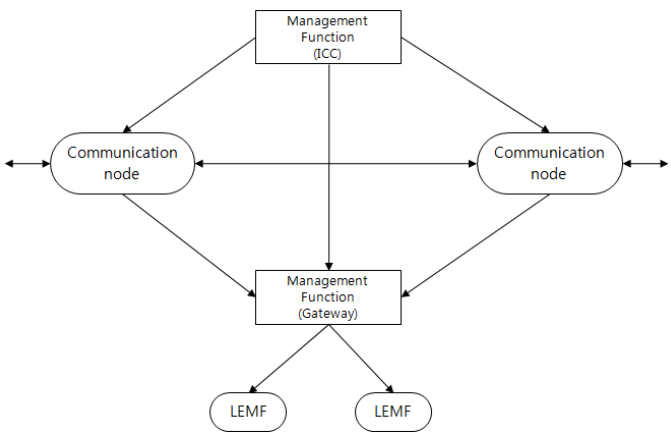
으로 도청대상 전화에 걸려오는 전화를 다른 회선과도 연결시켜 도청하는 방법이다. 음성사서함 연결(Voice-mail)은 음성사서함에 녹음된 내용은 비밀번호 유출여부에 따라서 쉽게 재생하여 엿들을 수 있는 방법이다(한국정보통신기술사협회, 2005).”

2. 도청 관련 표준 기술

1) ETSI 도청 기술

ETSI(European Tele-communications Standards Institute)는 유럽 통신 표준화 기구로서 전기 통신 분야의 단일 유럽 표준을 제정하고 조정하기 위해 설립된 표준화 기구이다.

“<그림 1>은 ETSI의 공중전화망 도청 시스템 구조를 나타낸 것으로 공중 전화망의 노드를 제어하는 Management Function(ICC : Intercept control Center)과 도청하여 받은 데이터를 선별 처리하는 MF(Mediation Function), 그리고 MF로부터 받은 데이터를 이용할 수 있는 LEMF(Law Enforcement Monitoring Facility)로 구분되어 진다(노효선 외, 2005).”



〈그림 1〉 ETSI의 공중전화망 도청 시스템 구조

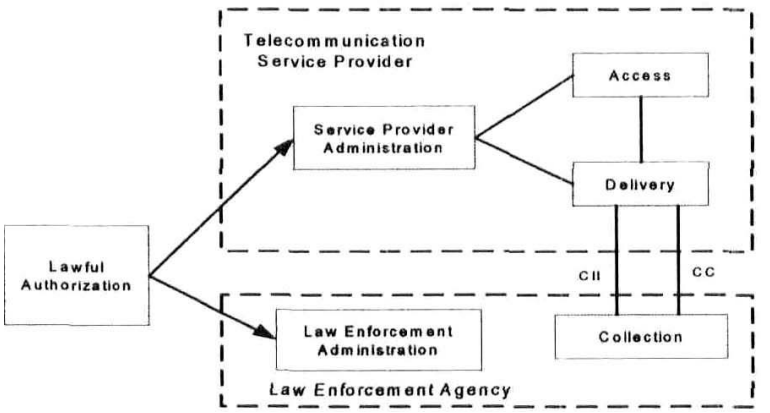
※ 출처 : 노효선 외, 2005, p.242

2) ATIS 도청 기술

“ATIS(Alliance for Telecommunication Industry Solutions)는 ANSI(America National

Standard Institute)의 ASD(Accredited Standard Developer)로서 실용적(pragmatic)이며 탄력적(Flexible)·개방적(Open) 접근에 따라 전 세계적으로 사용되는 통신 및 관련 정보기술산업의 기술적·운용 표준을 신속히 개발·홍보하는 기술기회 및 표준개발기구이다(한국정보통신기술협회, 2005).”

“ATIS에서 표준화된 합법적 감청구조는 <그림 2>와 같이 여러 개의 IAP들로 구성되어 call-identifying 정보와 Intercept subject 간의 통신 접근, 도청을 수행하는 AF, 하나 또는 여러 개의 CF로 이루어져 있는 DF, 전달받은 call-content와 call-identifying 정보 등을 수집하고 분석하는 기능을 담당하는 CF, AF와 DF를 관리하며 조절하는 기능을 담당하는 서비스 제공자 관리, LEA의 CF를 관리하고 조절하는 기능을 담당하는 법 집행 관리 등으로 이루어져 있다(노효선 외, 2005).”



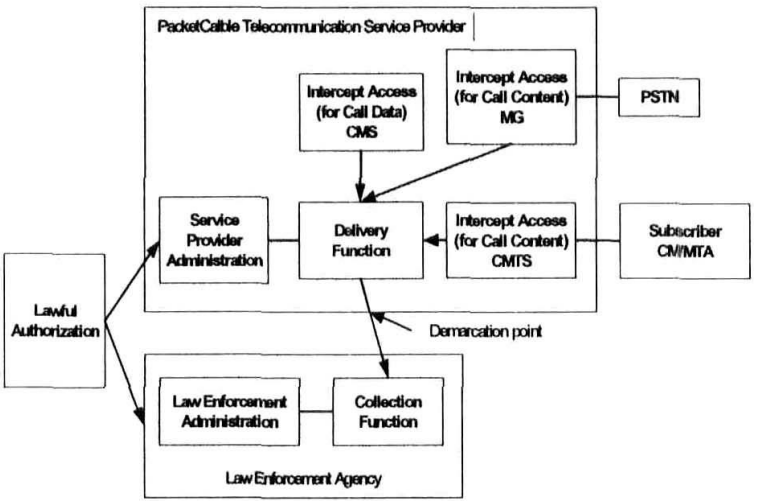
〈그림 2〉 ATIS 도청 구조

※ 출처 : 노효선 외, 2005, p.242

3) Cable Lab 도청 기술

Cable Lab은 케이블 모뎀, 케이블 텔레비전 오퍼레이터와 개인 비즈니스 컴퓨터 사이에 주고받는 자료의 신호를 취급하는 장치 또는 설비들의 표준재정에 관련된 미국에 존재하는 단체이다.

“<그림 3>은 Cable Lab 도청 구조로 감청을 위해 필요한 기능들을 보여주고 있으며, 이런 기능들 간의 원활한 통신을 위해 여러 가지 인터페이스를 정의하고 있다(노효선 외, 2005).”



〈그림 3〉 Cable Lab 도청 구조

※ 출처 : 노효선 외, 2005, p.242

3. 도청방지 및 탐지 기술

1) 도청방지 기술

"유선전화에서 도청방지 장치는 음성 메시지의 암복호화를 위한 비밀키를 생성하는데 있어 암호화 알고리즘은 DES(Data Encryption Standard) Diffie - Hellman 암호화 기법을 사용하고 있다(김순석, 이용희, 2008)."

한편, "키교환 알고리즘인 Diffie-Hellman 알고리즘의 연산 과정은 키를 교환하고자 하는 양 party(A, B)가 prime n과 g의 사용에 동의하였다고 할 때, 프로토콜은 다음과 같이 동작한다(김현석 외, 2005)."

A : X = g**x mod n (x는 large random integer)

B : Y = g**x mod n (x는 large random integer)

이때 A, B는 각각 X와 Y를 상대방으로 전달한다.

A : k = Y**x mod n

B : kp = X**y mod n

이때 k와 kp는 g**(xy) mod n과 동일하다.

2) 도청탐지 기술 및 장비

(1) 도청탐지 기술

“도청탐지 기술은 도청장치 등의 기기에서 발생하는 미약한 전파를 감지하여 이를 증폭시키는 방식으로, 미리 설정된 주파수와 비교하여 도청이 이루어지고 있는지를 판단하는 방식이다(김현석 외, 2008).” 이러한 방식은 시그니처 기반의 침입탐지 시스템과 같이 패턴 매칭으로 탐지를 수행하게 된다(Reddy, 2001). 즉, 도청탐지 지역에서 발생되는 주파수에 대한 ‘주파수 검색’을 실시하게 되고, 탐지된 주파수는 ‘도청 주파수 저장부’에 로깅(Logging)하게 된다. 로깅(Logging)된 주파수 콘텐츠는 기존 도청에 사용되었던 주파수와 ‘비교 분석’을 통하여 최종적으로 도청장치에 노출 유무를 판단하게 된다. 하지만 이러한 시그니처 기반의 도청탐지의 단점은 기존 도청 주파수와 달리 새로이 생성되는 주파수에 대한 탐지가 어렵기 때문에 다양하고 최신의 도청 주파수 콘텐츠의 확보가 전제되어야 한다.

(2) 도청탐지 장비

도청탐지 기술을 바탕으로 한 탐지 장비는 전파탐지기류, 스캐너, 전화라인 점검, 논리니어정션, 스펙트럼 유닛, 주파수카운터, 비화해독기, 전용안테나, 영상유닛 등이 있다.

전파탐지기류 기반의 장비는 무선전파의 전계강도를 측정하는 장비로써 10kHz~21GHz까지 RF를 탐색할 수 있는 ‘OSCOR 광대역 복합탐지기’, 0.01~13GHz 대역의 광대역 분석을 할 수 있는 ‘PCR-100s 광대역 주파수 분석기’, 200Hz~3GHz 주파수를 탐색할 수 있는 ‘ProCOM-700’, 100kHz~6GHz 주파수를 탐색할 수 있는 ‘REMON - 10’, ‘ALPHA - S’ 등이 있다.

광대역 수신기로 불리는 스캐너는 도청장치나 몰래 카메라에서 누출되는 신호를 직접 수신하여 음성을 들을 수 있는 장비로 주파수 대역은 3GHz 대역정도의 광대역이어야 한다. 스캐너 기반의 도청 탐지 장비로는 0.495~2450MHz 주파수가 검사 가능하며, 전파의 발신방향을 탐지할 수 있으며, 밴드 스코프 기능을 갖춘 ‘IC-R3 무선·영상 탐색기’와 1.7MHz~2.4GHz 주파수가 검사 가능하며, 원격지원 및 Auto Setup 기능 및 도청기, 몰래 카메라, Vox 형 도청 주파수 탐지 기능을 갖춘 ‘WatchDog 네트워크 주파수 검색기’ 등이 있다.

4. 국내 · 외 도청 관련 법 · 제도

1) 국내 도청 관련 법(통신비밀보호법)

(1) 통신 및 대화 비밀의 보호

누구든지 「통신비밀보호법」과 「형사소송법」 또는 「군사법원법」의 규정에 의하지 아니하고는 우편물의 검열·전기통신의 감청 또는 통신사실 확인 자료의 제공을 하거나 공개되지 아니한 타인간의 대화를 녹음 또는 청취하지 못한다(통신비밀보호법 제3조 제1항). 따라서 「통신비밀보호법」에 의하면, 기본적으로 타인의 대화를 녹음 또는 청취하는 행위는 허용되지 않는다. 이를 위반한 경우에는 1년 이상 10년 이하의 징역과 5년 이하의 자격정지에 처한다(동법 제16조 제1항 제1호).

(2) 국가기관의 도청방어 규제

「통신비밀보호법」상 도청방어에 대해서는 어떠한 의무나 규제조항이 없는 실정이며, 감청설비[3]의 기술적 차원의 인가는 과학기술정보통신부가 담당한다. 즉, 감청설비를 제조·수입·판매·배포·소지·사용하거나 이를 위한 광고를 하고자 하는 자는 과학기술정보통신부장관의 인가를 받아야 한다. 과학기술정보통신부장관은 인가를 하는 경우에는 인가신청자, 인가연월일, 인가된 감청설비의 종류와 수량 등 필요한 사항을 대장에 기재하여 비치하여야 하며, 인가를 받아 감청설비를 제조·수입·판매·배포·소지 또는 사용하는 자는 인가연월일, 인가된 감청설비의 종류와 수량, 비치장소 등 필요한 사항을 대장에 기재하여 비치하여야 한다(통신비밀보호법 제10조).

또한 「통신비밀보호법」은 불법감청설비탐지업[4]에 대해서만 당해 사업 운영에 대하여 공익적 차원에서 관리할 필요성을 인정한다고 할 수 있다. 즉, 영리를 목적으로 불법감청설비탐지업을 하고자 하는 자는 대통령령이 정하는 바에 의하여 과학기술정보통신부장관에게 등록을 하여야 하며, 등록은 법인에 한하여 할 수 있다. 등록을 하고자 하는 자는 대통령령이 정하는 이용자보호계획·사업계획·기술·재정능력·탐지

3) '감청설비'라 함은 대화 또는 전기통신의 감청에 사용될 수 있는 전자장치 · 기계장치 기타 설비를 말한다. 다만, 전기통신 기기 · 기구 또는 그 부품으로서 일반적으로 사용되는 것 및 청각교정을 위한 보청기 또는 이와 유사한 용도로 일반적으로 사용되는 것 중에서, 대통령령이 정하는 것은 제외한다(통신비밀보호법 제2조 제8호).

4) '불법감청설비탐지'라 함은 이 법의 규정에 의하지 아니하고 행하는 감청 또는 대화의 청취에 사용되는 설비를 탐지하는 것을 말한다(통신비밀보호법 제2조 제8의2호).

장비 그 밖에 필요한 사항을 갖추어야 한다. 등록의 변경요건 및 절차, 등록한 사업의 양도·양수·승계·휴지·폐지 및 그 신고, 등록업무의 위임 등에 관하여 필요한 사항은 대통령령[5]으로 정한다(통신비밀보호법 제10조의3).

2) 국외 주요국 통신감청 제도

(1) 미국의 통신감청 제도

"미국의 통신감청제도는 1994년 CALEA(Communications Assistance for Law Enforcement Act)를 근간으로 하고 있으며, 통신사업자가 감청을 수행하기 위하여 일정한 장비 설치를 가지게 되는 것을 핵심 내용으로 1994년 10월에 제정되었다. CALEA에 의해 전기통신사업자는 통신 감청을 수행하기 위한 능력을 구비하여야만 하는데 이때 전기통신 가청의무 대상 사업자는 PSTN기반의 유선전화 사업자, 상업용 무선통신사업자(이동통신, 위성이동통신 등), 호 부가서비스 제공사업자, 일부 재판매 사업자 등이 해당하며, 자가용 무선통신 제공사업자, 사설 네트워크 제공사업자, 정보서비스 제공사업자는 통신감청 의무면제 사업자에 해당된다(김성철, 민대홍, 2009)."

(2) 영국의 통신감청 제도

"영국은 1985년에 IOCA(Interception of Communications Act)를 제정함으로써 통신서비스에 대한 감청을 시작하였다. 법 제정 당시 PSTN 기반 전화서비스에 대해서만 감청을 집행하였으며, IP 서비스의 발전으로 2000년 RIPA(Regulation of Investigatory Powers Act) 2000을 제정하여 모든 종류의 감시·감독을 그 범위로 Part1에서 감청에 대한 부분을 규정하고 있다. 영국은 보안당국, 수사기관 등 9개의 기관에 대해서 감청을 허가하고 있는데, 감청은 국가의 보안 등 주요한 목적의 달성을 위하여, 그리고 최후의 수단으로 제한적으로 사용하도록 규정하고 있으며 감청결과를 법원에서 증거로 사용할 수 없도록 하고 있다(김성철, 민대홍, 2009)."

---

5) 과학기술정보통신부장관은 법 제10조의3 제4항에 따라 다음 각 호의 사항에 관한 권한을 중앙전파관리소장에게 위임한다(통신비밀보호법 시행령 제35조).
1. 법 제10조의3 및 이 영 제31조에 따른 불법감청설비탐지업의 등록 및 변경등록
2. 법 제10조의5에 따른 불법감청설비탐지업의 등록취소 및 영업정지
3. 제26조에 따른 불법감청설비탐지업의 등록취소에 대한 청문
4. 제32조에 따른 불법감청설비탐지업의 양도 · 합병신고
5. 제34조에 따른 불법감청설비탐지업의 휴지 · 폐지신고

(3) 독일의 통신감청 제도

"독일에서는 기본법(Grundesetz) 제10조의 규정에 의하여 원칙적으로 감청이 허용되지 않으며, 형법에서도 역시 감청, 녹음, 녹음의 공개 및 그 미수를 처벌하는 규정을 두고 사인 상호간의 감청을 규제하고 있다. 그러나 범죄수사·국가의 안전에 관한 감청을 허용한 「형사소송법」과 1968년에 제정된 '편지·우편 및 통신비밀의 제한에 관한 법률(Gesetz zur Beschräkung des Brief-, Post- und Fernmeldegeheimnisses)' 및 2001년 제정된 '정보통신감청을 위한 수단의 기술적 조직적 전환에 대한 법률(Verordnung üer die technische und organisatorische Umsetzung von Maβ nahmen zur Üerwachung der Telekommunikation)'이 있다(김성철, 민대홍, 2009)."

Ⅲ. 대(對)도청 보안의 취약성

최근 정보통신기술 발전으로 도청장비 또한 소형화, 첨단화로 보안 위협에 대한 대책이 시급함에도, 주요 기관 또는 시설 등의 대(對)도청 보안대책은 여전히 체계화되지 못한 실정이다. 이하에서는 기술적 측면에서의 취약성에 대하여, 특히 도청방지 및 탐지시스템 운용 현황과 도청방지 및 탐지시스템 운용의 문제점에 대하여 분석하고자 한다.

1. 도청방지 및 탐지시스템 운용 현황

도청장비의 발전으로 도청 가능 취약장비의 반입·사용에 대한 대(對)도청 방지를 위해서는 보안시설의 구축만으로는 역부족이기 때문에 이와 더불어 도청방지 및 탐지시스템을 복합적으로 운용하여야 한다. <표 1>은 도청 가능 취약장비를 나타낸 것이다.

불법 도청의 경우 주요 핵심시설 내에 도청장치를 은닉하고 외부에서 비밀대화 내용을 수신하는 방법과, 장거리에서 눈에 보이지 않는 적외선 레이저 빔을 활용하여 목표대상을 감시하는 고도로 정교한 감시 장치를 활용하는 방법 등을 사용하게 된다.

이러한 도청장치는 소형화, 첨단화로 발전하면서 불법 송·수신 장치 색출을 어렵게 하고 있고, 불법 도청장치의 내부 반입은 택배나 소포, 우편을 이용하거나 직접

〈표 1〉 도청 가능 취약장비

구분	취약장비
비인가 상용 정보통신 장비	· 시계형 및 볼펜형 녹음기 · 보이스펜 · 초소형 디지털 녹음기
인가 상용 정보통신 장비	· 스마트폰
기 타	· 불법 도청기 · 제공받은 기념품 內 은닉된 도청기 (특히 외국 정부 및 기관 제공 기념품)

※ 출처 : 이영호, 2015, p.28

방문 또는 내부 인원과의 결탁을 통하여 집무실이나 회의실에 불법 도청장치를 은닉하게 된다. 특히, 국내·외 타 기관에서 제공되는 기념품 내에 은닉하는 형태의 불법 도청기에 대한 경계가 이루어져야 한다.

주요 핵심시설 내부에 도청장치가 반입 및 설치되는 경로는 반입되는 물건 내부에 도청기가 은닉되는 경우이며, 외부에서 주요 핵심시설에 직접 레이저 도청장치를 이용하여 도청하는 경우도 있다.

또한 기술의 발전에 따라 도청장치도 소형화 및 다양화 되었다. 이로써 불법 도청장치의 은닉 장소는 집무실의 경우, 컴퓨터 본체에 연결되는 잭 모양의 '캡처'를 이용하거나 인터넷 연결라인 및 전원 멀티캡 내에 도청기를 삽입하는 방식, 송수화기 내부, 계산기 내부, 스프링클러 내부에 도청기를 삽입하는 방식, 그림 뒤 몰래카메라를 설치하거나 외부에서 레이저도청기를 이용하여 불법 도청을 하게 된다. 또한 회의실의 경우 탁자 밑에 무선 도청기를 은닉하거나 전원 콘센트 내에 도청기를 삽입하는 방식으로 불법 도청을 하게 된다.

이와 같이 도청장비는 물론 반입경로 및 은닉장소는 나날이 지능화되고 있으나 이에 대한 대(對)도청 보안은 여전히 취약하다. 다만, 국방부 등 일부 기관에서만 도청방지 및 탐지 시스템을 도입하여 불법 도청을 방지하고 있는 실정이다. 즉, 도청방지 장치로는 레이저도청 방어장비[6]와 PC 전자파 차폐장비[7]를 활용하고 있으며, 도청탐지 장치로는 상시 도청탐지 장비[8], 휴대형 탐지장비[9], UWB(Ultra Wide Band)

6) 음향 및 진동 잡음을 발생시켜 외부에서의 레이저 도청 및 건물 벽면과 환풍구를 통한 도청을 방지하는 장비이다(이영호, 2015).

7) 전파 잡음을 발생시켜 PC에서 방사되는 전자파를 상쇄, 외부에서의 PC 화면 정보 재생을 차단하는 장비이다(이영호, 2015).

영상탐지장비[10]를 활용하고 있다. 또한 도청방지 장치 및 도청탐지 장치의 운용은 상시 도청탐지 장비를 바탕으로 창문이 있는 경우 레이저 도청 방어 장비 및 전자파 차폐장비를 활용하여 대(對) 도청 탐지 및 측정 활동을 시행하고 있다.

2. 도청방지 및 탐지시스템 운용의 문제점

정보통신의 발전과 더불어 보안위협에 대한 문제점도 증가하고 있다. 무선통신의 경우 통신로가 노출되어 있기 때문에 스니핑과 같은 도청에 매우 취약하다. 이러한 점을 보완하기 위하여 암호화 기능을 사용하게 되는데 상시 도청탐지 장비의 경우 무선 기술이 대부분의 경우를 차지하고 있기 때문에, 중앙관제와의 통신에 있어 암호화 알고리즘을 사용과 상시 도청탐지 장비에 사용되는 단말기의 경우 전력이 단선되었을 경우에도 상시 운용이 가능하도록 보조 배터리와 같은 예비전력을 적용하여야 한다.

또한 상시 도청방지 및 탐지시스템의 운용에 있어 효과적인 도청 보안을 위해서는 각 보안 등급 및 특성에 맞게 시스템을 적용하여야 하며, 사전 및 사후 대책을 위해 물리적 보안인 출입통제 시스템과의 연계가 필요하다. 출입통제 시스템의 경우 사람의 출입뿐만 아니라 주요직위자 집무실에 설치된 통신 단자함 등과 같이 도청장치가 설치될 만한 곳에 대한 통제도 필요하다.

Ⅳ. 대(對)도청 보안의 개선방안

1. 도청보안 등급별 시스템 적용

대(對) 도청보안을 운용하고 있는 기관 또는 시설의 경우에도 업무의 성격과 중요

8) 원격 단말기를 설치하고 네트워크를 이용, 24시간 도청신호를 상시 탐지 · 분석할 수 있는 시스템이다(이영호, 2015).

9) 유 · 무선 도청신호를 탐지하는 휴대형 장비로써 신호 탐지 시 도청장비설치 방향까지 측정 가능한 시스템이다(이영호, 2015).

10) 벽돌 내부에 숨겨져 있는 무게를 투시할 수 있는 장비로 벽돌에 일정한 주파수 펄스를 발사하여 반사 주파수를 분석하여, 해당 물체를 3차원으로 형상화(위치, 깊이 등)하는 시스템이다(이영호, 2015).

도 및 장소를 고려하지 않고 운용하는 경우가 많으므로 효율적이지 않다. 따라서 도청으로 인한 보안 위협으로부터 중요 정보를 보호하기 위하여 각 대상시설 또는 부서를 보안등급화 하는 것이 선행되어야 한다. 즉, 도청에 노출될 경우 미치게 될 사회적 파장, 회의 내용의 영업비밀성 정도, 회의 주체의 직위 등 중요도에 따라 도청보안 1등급(Level-1), 도청보안 2등급(Level-2), 도청보안 3등급(Level-3)으로 구분하여야 한다. 이와 같은 보안등급화를 기준으로 해당 등급에 <표 2>와 같은 도청 방지 및 탐지 시스템의 적용이 필요하다.

〈표 2〉 보안등급별 적용될 도청방지 및 탐지 시스템

구분	시스템	비고
도청방지 시스템	레이저 도청 방어	유선 도청기, 콘크리트 도청기, 레이저 도청기 등에 방어
	레이저 및 전자파차단 필름	무선도청장비의 출력신호를 차단, 유리면에 접착하여 사용
	전자파 차폐	전자기기에서 방사되는 전자파 상쇄
도청탐지 시스템	상시 도청 탐지	365일 24시간 도청 신호 탐지 관리 서버를 통해 모니터링 및 DB 관리 탐지 단말기에 대한 보안 요구
	휴대형 탐지	대(對)도청에 대한 수시 점검을 위한 장비로 도청에 대한 방향성까지 측정
	영상 탐지	콘크리트 도청기와 같이 일정한 물체나 공간 내에 설치된 장치 탐지

※ 출처 : 이영호, 2015, p.40

위와 같은 도청 방지 및 탐지 시스템의 보안등급별 적용을 살펴보면 다음과 같다.

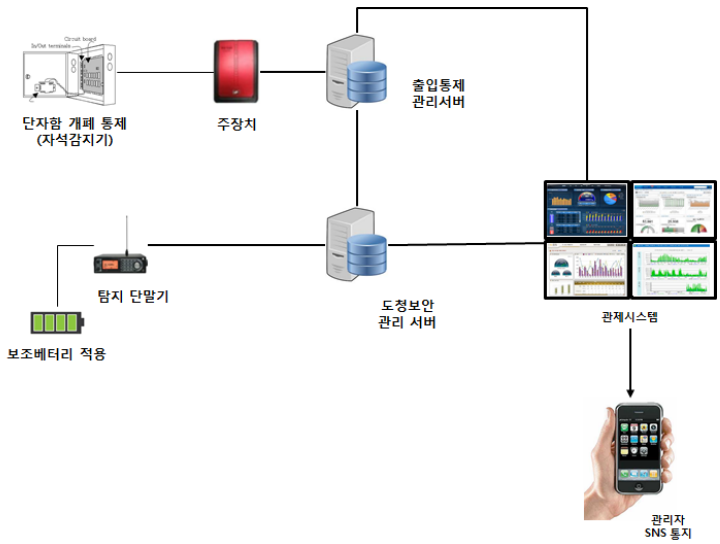
도청보안 1등급의 경우 레이저 도청방어, 레이저 및 전자파차단 필름, 전자파 차폐장치, 영상탐지, 상시 도청 탐지 단말기가 적용되어야 할 것이다. 상시 도청탐지 단말기의 적용하여 24시간 감시가 이루어져야 하며, 회의실과 기타 부서의 경우는 휴대형 탐지기를 이용하여 회의시간 내 탐지 및 점검 시에 사용하여야 할 것이다.

도청보안 2등급의 경우 레이저 및 전자파차단 필름 및 전자파 차폐장치 그리고 상시 도청 탐지 단말기를 적용하여야 하고, 휴대형 탐지장치를 적용하여 주 1회 이상 수시 점검을 실시하여야 할 것이다.

도청보안 3등급의 경우 각 부서의 창문에 레이저 및 전자파차단 필름을 적용하여야 하고, 휴대형 탐지장치를 이용하여 월 1회 이상 수시 점검을 실시하여야 할 것이다.

2. 상시 도청탐지 시스템의 구성

<그림 4>는 상시 도청탐지 시스템의 구성도로 도청보안 관리 서버와 출입통제 서버와의 연계로 인한 통합관제로 구성하여, 신속한 사후관리를 통한 역추적이 가능하도록 구성하여야 할 것이다. 관제시스템은 도청보안 1등급의 경우 상황실에 설치를 기준으로 하며, 2등급 이하의 경우 전산실에 설치하고 관리자 및 관제사를 지정하여 모니터링하게 된다. 도청 위협에 대한 역추적의 경우 시설 내부의 출입하는 인원에 의한 위협에 대한 관리를 위해 통합관제의 형태로 이루어져야 하며, 위협이 발생한 경우 관리자에게 문자로 통보하게 된다.



※ 출처 : 이영호, 2015, p.43

〈그림 4〉 상시 도청탐지 시스템 구성도

또한 중요 부서에 적용되는 상시 도청탐지 단말기의 경우 전원이 단선되었을 경우를 대비하여 단말기 내에 보조 배터리가 적용되어야 하며, 출입통제 관리시스템과의 연계로 도청장치를 은닉할 수 있는 단자함 등의 개폐를 출입통제 시스템의 기존 인프라를 통해 관리할 수 있다. 단자함의 경우 출입통제 시스템에서 사용되는 자석감지기를 이용하여 단자함 열림 유무를 확인할 수 있으며, 소화전이나 환풍구에도

적용이 가능하다.

이상과 같은 도청탐지 시스템을 구축하게 되면 대(對)도청 보안성이 더욱 강화될 것이다.

V. 결 론

국가안보, 군사·외교정보, 정책 등의 국가 기밀 주요 정보와 첨단 산업핵심 기술, 핵심 R&D 기술, 주요 영업전략 등의 기업정보와 개인의 사생활 정보 등 불법적인 무선 정보유출로 인한 피해는 해당 영역뿐 아니라 국가적인 손실로 이어지게 된다. 따라서 대(對)도청에 대한 보안성 확보가 무엇보다도 시급하나 현재 주요 기관이나 시설 등은 대(對)도청 방지에 대하여 소극적이며, 도청위협에 대하여 방어 장비 설치 기준이 미흡한 실정이다.

도청으로 인한 보안 위협을 최소화하고, 대(對)도청 위협으로부터 중요 정보를 보호하기 위하여 대(對)도청 보안의 취약성을 분석한 결과 도청방지 및 탐지시스템 운용의 문제점으로 인하여 보안위협에 노출되어 있다. 이를 개선하기 위하여 첫째, 도청으로 인한 보안 위협으로부터 중요 정보를 보호하기 위하여 각 대상시설 또는 부서를 보안등급화 하여야 한다. 둘째, 도청보안 등급에 따라 방어 및 탐지 장비를 적용하고, 상시형 도청탐지 시스템은 도청보안 1등급에 적용하여 24시간 감시가 이루어져야 하며 회의실 또는 기타 주요시설에는 휴대형 탐지기를 이용하여 수시로 탐지 점검을 실시하여야 한다.

이상과 같은 대(對) 도청보안의 시스템 구축으로 인한 기대효과는 주요 기관 또는 시설의 안전망 구축에 대한 정보보호와 융합보안관제로 사후 역추적을 가능하게하며, 통합관제로 인하여 도청위협 시 정보의 유출을 방지하고 위험 요인을 제거할 수 있다. 다만, 급속히 발전되는 도청기술과 보안위협에 적절히 대처하기 위해서는 대(對) 도청보안에 대한 지속적인 연구 및 기술개발이 필요하다 할 것이다.

참고문헌

권오훈, 이명훈, 이재우, 임채호 (2013). 국방망의 지속적인 시실시간 보안관체계. **정보보호학회지, 23**(6), 54-66.

김성철, 민대홍 (2009). 해외의 통신감청제도 현황 및 시사점. **한국통신학회 학술대회논문집,** 422-423.

김순석, 이용희 (2008). 의사난수발생기를 이용한 새로운 유선전화 도청방지장치에 관한 연구. **한국해양정보통신학회논문지, 12**(6), 1006-1009.

김현석, 김일곤, 최진영, 노정현, 유희준 (2005). Diffie-Hellman기반 M-Commerce 프로토콜 분석. **한국정보과학회 2005 한국컴퓨터종합학술대회 논문집(A),** 226-228.

노효선, 정수환, 김영한, 강신각 (2005). 합법적 감청을 위한 표준 아키텍처 비교 분석. **대한전자공학회 전자정보통신 학술대회 논문집,** 241-244.

안정철, 권혁진 (2008). 국방분야 무선 Network 도입을 위한 보안기술 측면의 고려사항. **정보과학회지, 26**(11), 128-134.

오혁근 (2011). 개인정보와 사생활을 위한 정보 유출 방지기 디자인 개발. **디자인지식저널, 20,** 21-30.

윤해성 (2006). 비밀정보 검토에서 바라본 기업보안의 활성화 방안. **치안정책연구, 20,** 214-215.

이영호 (2015). **도청보안의 국방모델링 연구.** 국방대학교 석사학위논문.

이준복 (2014). 산업스파이 및 M&A에 따른 산업기술유출 대응방안에 관한 법적 연구. **경찰학연구, 39,** 89-119.

좌봉준 (2008). 도청방지·감지 분야 특허 동향. **주간기술동향, 통권1342호.**

최광복 (2011). 도사이버전 대응을 위한 국방 정보보호환경 분석과 보안관리 모델 연구방향 고찰. **정보보호학회논문지, 21**(6), 7-15.

한국정보통신기술사협회 (2005). **불법감청설비 탐지업 등록제 세부기준에 관한 연구.**

한국정보통신기술협회 (2005). **정보통신 표준화 추진체계 분석서.**

Reddy, S. V., Ramani, K. S., et al. (2010). Wireless hacking-a WiFi hack by cracking WEP. *2010 2nd International Conference on Education Technology and Computer*, Shanghai, 189-193.

http://www.law.go.kr/main.html (국가법령정보센터)

https://ko.wikipedia.org/wiki (위키백과)

【Abstract】

A Study on the Threats of Wiretapping and Effective Security Management Strategies

Lee, Young Ho · Choi, Kyung Cheol · Woo, Sang Yeob

Rapid advancement of technology in today's society has allowed for easy access and use of data, promoting the process of informationization. Along with the merits of such development, unintended consequences of security risks involving wiretapping have been increasing as well. The security threats posed by wiretapping technology must be addressed by every organization and individual, as it could be used to leak confidential information about the nation's security, military and diplomatic strategies, industrial technologies, and personal information.

Despite increasing threats stemming from the surrounding nations using advanced wiretapping technology, there is a lack of awareness at the government level, and the existing security measures for detecting and counteracting the wiretapping equipment are ineffective.

In this research, the authors offered technical suggestions for improving the security strategies against the threats of wiretapping and information leakage by conducting a content analysis. The authors suggested the units of an agency be assigned a security grade based on its importance, and that adequate security equipment should be operated according to the grade. For instance, around-the-clock surveillance is recommended for grade-1 facilities, and portable wiretapping equipment detectors should be used to protect conference rooms and other key sites.

Keywords: Security Against Wiretapping, Protection from Wiretapping, Wiretapping Detection Technology, Wiretapping Prevention System