

盗聴法の改正問題～通信監視の捜査手法も併せて

2013. 6. 20

弁護士 山下 幸夫

1 現行の盗聴法の成立とその後の状況

盗聴法（犯罪捜査のために通信傍受に関する法律）は、1999年8月12日の参議院本会議において、組織的犯罪対策法の採決を行い、自民、自由、公明3党などの賛成多数で可決、成立した。盗聴法が国会で成立したことにより、2000年8月に盗聴法は施行された。

しかしながら、その後、毎年、盗聴の実施状況が国会に報告がなされているが、毎年10件程度であり、あまり活用されていない。

これについては、この法律が使いづらいという指摘が警察関係者からなされてきた。

2 犯罪対策閣僚会議での検討

自民党・公明党政権下において、全ての閣僚が構成員となっている犯罪対策閣僚会議において、2003年12月に出された「**犯罪に強い社会の実現のための行動計画**」の中の「組織犯罪に対する有効な捜査手法等の活用・検討」において、「組織犯罪に対し、あらゆる捜査手法等を積極的に活用するとともに、通信傍受、おとり捜査、コントロールド・デリバリー、潜入捜査等の高度な捜査技術・捜査手法、犯罪収益規制の拡大を具体的に研究し、その導入・活用に向けた制度や捜査運営の在り方を検討する。」と述べていた。

民主党に政権交代した後も犯罪対策閣僚会議は引き継がれ、上記の行動計画の改訂版である「**犯罪に強い社会の実現のための行動計画2008**」においても、「社会・経済情勢の変化に応じた有効な捜査手法等の導入・活用の検討」として、「犯罪の凶悪化、組織化及び複雑化等に適切に対処し、犯人の特定・検挙や事案の真相解明をより効果的に行うことができるようにするため、諸外国において活用されている刑事免責、おとり捜査・潜入捜査、**通信傍受等の捜査手法の導入又は積極的活用**について検討する。」と述べられて、その内容が基本的には維持されていた。

しかし、その後、具体的な検討は進まなかった。

3 通信傍受法改正に向けた具体的動き

盗聴法改正に向けた思わぬ動きとしては、刑事司法改革の動きの中で、具体化してきた動きがある。

2011年6月29日、法制審議会新時代の刑事司法制度特別部会の第1回会議が開催されて以後、1巡目と2巡目の議論がなされ、2013年1月29日に開催された法制審議会新時代の刑事司法制度特別部会第19回会議において、「時代に即した新たな刑事司法制度の基本構想」が取りまとめられた。

そこでは、盗聴法の改正について、次のとおり、明言されている（基本構想15頁以下）。

ア 通信傍受

通信傍受をより効果的・効率的に活用できるようにするため、傍受の実施の適正を担保しつつ、以下のとおり通信傍受法を改正することについて具体的な検討を行う。

- 通信傍受の対象犯罪を拡大し、振り込め詐欺や組織窃盗を含め、通信傍受が必要かつ有用な犯罪において活用できるものとする。
- 暗号等の技術的措置を活用することにより、立会いや封印等の手続を合理化する。
- 該当性判断のための傍受の方法として、全ての通信を一旦記録しておき、事後的にスポット傍受の方法による必要最小限度の範囲の聴取を行うことも可能な仕組みとする。

イ 会話傍受

会話傍受については、①振り込め詐欺の拠点となっている事務所等、②対立抗争等の場合における暴力団事務所や暴力団幹部の使用車両、③コントロールド・デリバリーが実施される場合における配送物の3つの場面を念頭に置き、指摘される懸念をも踏まえて、その採否も含めた具体的な検討を行う。

→ 通信傍受法の改正は**決定事項**となっており、対象犯罪の拡大、手続の合理化などを具体的に検討することになっていること、会話傍受は新設が既定方針ではないが、具体的に検討することになっていることに注意が必要である。

現在、この基本構想に基づいて作業部会が設けられ、2013年6月14日の第20回部会において報告されて意見交換がなされた。今後、7月から10月まで作業部会が開かれ、11月から2014年2月ころまでに要綱案が作成され、法制審議会総会での了承を経て、法務大臣に答申され、2014年の通常国会に通信傍受法改正案が提出される見込みである。

4 現行法の手続と改正が検討されている手続について

現行法の手続は別紙の資料1、警察庁が提案している新たな手続は資料6を参照。暗号技術と鍵を利用して、立会制度の廃止と該当性判断のための傍受を事後的に実施できるようにすることがその主眼である。

① 立会制度の廃止

これまで、捜査官は、通信事業者の事務所に赴いて、通信事業者の従業員を立会人として、通信傍受を実施し、記録媒体の封印も立会人がしていた。

今回、この手続を「合理化・効率化」と称して、通信事業者から、対象となる通信を暗号化して警察署に伝送させ、警察署では暗号を複合化して、立会人なしに傍受することを提案している。

② 事後的な該当性判断の実施

これまでリアルタイムで通信を傍受していたが、新たな手法として、通信を後からまとめて伝送し、警察署において事後的に該当性判断のための通信傍受を実施することが提案されている。

5 その他改正が検討されている項目について

① 傍受対象罪種の変更・拡大

現行法で認められている 4 類型（銃器犯罪、薬物犯罪、集団密航、組織的殺人）の限定のうち、適用例が一度もない集団密行の罪を外し、この 10 年間で出てきた組織窃盗や振り込め詐欺に対応できるように、窃盗や詐欺を追加することが検討されていたが、作業分科会の議論では、これをさらに拡げて、①窃盗、強盗、詐欺、恐喝、②殺人、③逮捕・監禁、略取・誘拐、③その他とさらに大きく拡げることが検討されている。

なお、将来的には、共謀罪が創設された場合、その対象犯罪（600 以上）を、傍受対象にすべきであるという議論が出る可能性がある。

② 会話傍受

振り込め詐欺が典型例で、アジトでの指示の状況や電話の状況を会話傍受するか、暴力団の対立抗争時に、暴力団事務所や車両を会話傍受したり、覚醒剤の宅配物について、覚醒剤が入っているということを知らなかったという弁解に対処するため、宅配物に傍受装置をつけておけば受け取った時の状況が分かるという理由で、会話傍受を実施することも検討課題とされている。

ここで最大の問題は、通信と異なり、その場所で行われる全ての会話が傍受されるということ、室内に傍受するための機器を設置するために侵入することも合法化されることである。前者はプライバシーの侵害において重大であるし、後者は、ドイツでは「住居の不可侵」を保障する憲法を改正して実施されていることと比較して、憲法違反と言わなければならない。

6 既に現行法でも通信監視が広く認められている

① 電子メールの傍受について

通信傍受法における通信には電子メールも含むというのが立法者の見解であるが、これまでの国会報告では 1 件も電子メールの傍受の事例がない。

ただ、メールサーバーに届いた電子メールは、ユーザーが読み出す前の段階でも「通信」を終了しているとして、搜索・差押えや検証によって取得されていると考えられるから、事実上、通信傍受法による制限なく取得されていると考えられる。

さらに、コンピュータ監視法による刑訴改正により、リモートアクセスによる差押えが可能となり、手元のパソコンや携帯電話から、メールサーバーにある電子メールを差し押えることが可能となっている。

② 捜査機関による G P S 携帯電話を利用した位置探索捜査について

総務省は、2011年8月2日から31日まで、「電気通信事業における個人情報ガイドライン」とその解説の改正についてのパブリックコメントを募集した。同年11月2日に、同ガイドライン等が改正され、同日以降、実施可能な捜査となっている。

これは、所在不明の被疑者を逮捕する目的で、被疑者の使用している携帯電話について、携帯電話会社のシステム端末を操作して、その所在位置を探索するために、捜査機関から検証許可状の発付が請求され、裁判官が審査の上、検証許可状を発付し、それを携帯電話会社に呈示し、G P S による位置情報を捜査機関に提供することを可能とするものであり、重大な問題がある（日弁連の2011年8月26日付「電気通信事業における個人情報保護に関するガイドライン及び解説の改正案に対する意見書」を参

照)。

③ 通信記録(通信履歴)のリアルタイム収集について

いわゆるコンピュータ監視法が成立し、電気通信回線で接続されたコンピュータに対する差押え(リモート・アクセス)や通信履歴の保全要請などが刑事訴訟法に新設され、既に施行されている。

これとは別に、コンピュータ監視法案の審議の際に、サイバー犯罪条約20条が締約国に整備を求めている通信記録のリアルタイム収集、すなわち、犯罪の種類を問わず、通信記録(通信履歴)を将来に向かってリアルタイムで収集する制度について、江田元法務大臣は、現行法の検証により実施できると答弁した。

2012年11月1日に、我が国はサイバー犯罪条約に正式に加盟しており、今後、通信記録のリアルタイム収集が検証許可状で取得する捜査が実施されると考えられる。

7 今後の通信監視のための捜査について

政府の情報セキュリティ政策会議(議長・菅義偉官房長官)は、2013年6月10日、2015年度までの「サイバーセキュリティ戦略」を正式決定した。サイバー犯罪の複雑化と被害の深刻化を踏まえ、通信事業者がインターネットの利用状況を解析したり、利用内容の履歴を保存したりすることについての検討を打ち出したと報じられている。

その報告書では、「サイバー空間の犯罪対策」として、「サイバー犯罪に対する事後追跡可能性を確保するため、関係事業者における通信履歴等に関するログの保存の在り方やデジタルフォレンジックに関する取組を促進するための方策について検討する。特に、通信履歴の保存については、通信の秘密との関係、セキュリティ上有効な通信履歴の種類、保存する通信事業者等における負担、海外でのログの保存期間、一般利用者としての国民の多様な意見を勘案した上でサイバー犯罪における捜査への利用の在り方について検討する。」

通信履歴の保存については、法制審議会特別部会の基本構想においても、「携帯電話等の通信履歴は、事件関係者の行動を把握し又は供述の信用性を吟味する上で極めて有用な資料となるものであるので、これが十分な期間保存されるような仕組みが構築されることが望ましいとの意見が少なからず示された。この問題は、法制審議会の所掌を超える問題であり、通信事業者側の事情も踏まえた検討を行う必要があるものの、当部会としては、適切な場における検討を経た上で、通信履歴が十分な期間保存されるような仕組みが構築されることを希望することとしたい。」と述べられている(基本構想17頁)。

自民党の治安・テロ対策調査会は、2013年5月21日、提言「世界一の安全を取り戻すために～緊急に取り組むべき3つの課題」を取りまとめている。

提言は、①持続可能な民間の安全形成システムの強化、②サイバー犯罪等新たな対応を必要とする犯罪対策の強化、③頼りがいのある治安インフラの3点で構成され、サイバー犯罪に対処するため、官民による新組織「総合的サイバー犯罪対策のための産学官連合」(日本版NCFTA)を設置することなどを盛り込んでいる。

この中で、通信履歴の保存の義務化や、通信傍受・会話傍受、携帯電話等のGPS位置情報の取得要件の緩和などが提案されている。

8 アメリカにおける通信監視の暴露

アメリカ国家安全局（NSA）の**秘密監視システム「PRISM」**が、内部告発者である元CIAのエドワード・スノーデン氏によって暴露された。同氏はあらゆる人物が対象となっていたと暴露している。

NSAは、グーグル、マイクロソフト、フェイスブック、ツイッター、ヤフーなど主要な通信企業のサーバーから、個人の電子メールやユーザー情報を直接取得していた疑うが浮上している。

かつて、全世界の無線通信を傍受するエシュロンが明らかとなったが、今回は、インターネット通信を対象とする監視システムである。

（ニューズウィーク日本版 6 月 25 日号「アメリカの陰謀？ ネット監視」と題する特集記事が参考になる。）

日本政府は、これと同じことをやろうとしているのではないかと考えられる。

以上