

データ駆動型捜査時代の規律方法 ～令状主義との決別？

一般財団法人 情報法制研究所 参与
成城大学 教授

指宿 信

「データ駆動型捜査手法」における 3つのレイヤー

成城大学の指宿と申します。専門は刑事訴訟法、サイバー法などをやっております。学位は刑事訴訟法で取ったんですが、1990年代、インターネットが商用利用されるようになったぐらいから、サイバー法の研究をしてまいりました。今日は、刑事手続と個人情報の保護の、交錯領域のお話をさせていただきます。サブタイトルの「令状主義との決別？」について説明しますと、データ駆動型捜査、データを収集して捜査を進めるという、こうした手法に対して、事前に裁判官がその捜査が適切かどうか、妥当かどうかということをチェックする事前規制型の手法が令状主義なわけです。搜索差押許可状とか、逮捕令状とか、そういうものを使って、中立的な立場から規律するというのが事前規制、令状主義の考え方ですが、これでは不十分なんじゃないか、事後規制に移行しないといけない時代になっているのではないかと、そういう問題提起が若い世代の刑事訴訟法学者から出てきているんです。刑事法学に興味がない方からすると、「なんのこっちゃ？」というふうに思われるかもしれませんが、それはおいおい話ししていけたらと思います。要するに「裁判所に任せておいていいのか問題」、というわけです。

はじめに、問題の立て方をご説明します。そのあとで、今日はレイヤーを3つぐらいに分けてお話する予定です。こういう区別は、なかなかお目にかからないと思うので、参考になるかと思います。はじめに、問題意識の立て方ですが、ローレンス・レッシング、ハーバード大学教授で『Code』の著者によれば、「他人が自分についての情報を得る方法は2つしかない - モニタリング／監視か、検索・搜索を通じてだ。」ということです。すなわちこれは、電子化・オンライン化された社会では、モニタリング／監視には情報の

「ターゲティング」と「追跡」が必要になります。検索・搜索には情報の「収集蓄積」と「ブラウジング」が必要になるということです。このことはつまり、個人情報（データ）を保護しようとするれば、「ターゲティングと追跡」を規制すること、「収集蓄積とブラウジング」を規制することです。これは民間部門であれ公的部門であれ、まったく同じだと思います。

近時の電子化・オンライン化された捜査の文脈では、電子化問題とは「データ駆動型捜査手法」です。捜査から公判の情報収集過程で、従来は見逃されていたデータ取得後の保護が、近年注目を集めています。先に触れた「事後規制の必要性」です。電子化・オンライン化、これは情報系の方々にとっては当たり前の話かもしれませんが、インプット段階で大規模化するわけですね。人間が張り込んだり、尾行しているのは人的な資源の限界があるわけですが、データを集めるのはあつという間にできるし、しかも大規模化する。それから、処理過程も不透明である。物を集めたりすれば、差し押さえのため物が移転するので明らかですが、情報処理は不透明です。例えば、情報処理のアルゴリズムというのは、外部からは検証ができません。それからアウトプット段階については、データを集めて捜査に使うという段階で、どこにそのデータを置いているのか、誰がデータにアクセスできるのか、最初の捜査と違う捜査の目的でそれを使っていいのか、そういう問題があります。だいたい情報処理の三段階に分けて、こうした問題があるということを最初に指摘しておきたいと思います。では、令状によってコントロールする令状規制の時代は終わったのか、事後規制にはどんな方法が具体的にあるのかということを、今日は話めしていきたいと思います。

先ほど触れたレイヤーですけれども、データ駆動型捜査手法としては3つあります。一番下のレイヤー、これは民間から情報を集めるという方法です。

電子化問題への視座：2

データ駆動型捜査手法の実態を把握分類した上で、

- ✓ それぞれのレイヤーに応じた法的規律・制御方法の検討が必要！
- ✓ データのインプット・処理・アウトプットのいずれの段階についても伝統的な令状主義だけでは、もはや制御不能！

【背景事情】

- 1、個人情報保護法制から警察情報が除外されている（個人情報保護だけの問題ではない）
- 2、任意捜査の情報収集が拡大し、無規制である
- 3、法曹も法学者も政策立案者も、データ駆動型捜査の実態や情報処理技術に知識・能力が乏しい（捜査だけの問題ではない）

12/21/2021
5

「ちょっとあの人のデータを出してよ」とか、「ちょっとこの本を読んでいる人の名前を知りたいんだけど貸出記録を見せてよ」とか、そういう民間情報を集めてデータを収集するのがレイヤー1。レイヤー2は、任意処分・任意捜査と呼ばれているもので、先ほどから例に挙げている尾行とか張り込みとかはこの任意処分に当たるわけです。最上位層がレイヤー3。これが強制処分といわれるもので、先ほどご紹介した、裁判官が事前に審査をして強制捜査をやっているよと言われたのでお宅に入ります、搜索します、あなたを逮捕しますという、こういう捜査です。それぞれのレイヤーに応じた法的規律が必要なんだけれども、日本はどうなっているのだろうか。それぞれのレイヤーでインプット・処理・アウトプットがあるんだけど、伝統的な事前規制型の令状で、これらをちゃんと制御・統制できているのかというのが問題意識です。背景事情としては、個人情報保護法制から警察情報が除外されています。これは皆さん常識ですよ。個人情報保護法系の枠組みからこの問題にはアプローチしにくいというのがあるから、だから私にお鉢が回ってきました。このレイヤー1とレイヤー2のデータの収集量は膨大なわけです。ほぼ無規制といってもいいぐらいです。さらに深刻なのは、法律家も法学者も政策立案者も、データ駆動型捜査の実態や情報処理技術に対して知識や能力が乏しい。そういう問題があります。

レイヤー1－民間協力

では、レイヤー1からいきましょう。これは最下層（民間協力）ですね。具体的には、捜査関係事項照会という書面でやることが多いんですけども、これすら持っていけない場合もあるわけですね。口頭で、先ほど言ったような、「誰々さんの情報を見せてよ」とか、「この本を誰が読んでいるのか見たいんだけど」というような要請がある。そういうことは日常的に行われています。一昨年 of JILIS の講演会でやっていますが、詳しくはそちらを見ていただきたいんですが、今日は簡単に紹介します。これは刑事訴訟法の中に、条文で定めがあり、「捜査関係事項照会書」というものを作って、相手先に持っていく。ただし、搜索差押え令状のような強制力はないので従う義務はありません。

根拠条文は「捜査については、公務所又は公私の団体に照会して必要な事項の報告を求めることができる。」（刑事訴訟法197条2項）というものです。情報を提供する側からすると、第5項「第二項又は第三項の規定による求めを行う場合において、必要があるときは、みだりにこれらに関する事項を漏らさないよう求めることができる。」この条項が問題になるわけです。保秘条項が付いているんです。こういう情報を取りに警察が来たんだけど、この情報の所有者とか、個人情報の提供者に対して「あなたの情報を伝えましたよ」と言っちゃダメですよということです。伝えたとしても罰則はありませんけれども。

この照会書の利用実態についてですが、警察の元

利用実態について（３）・・・捜査関係事項照会を拒絶する例

- ・ 日本図書館協会の対応指針
- ・ 照会に緊急性がなければ捜査関係事項照会による情報提供は拒絶し、捜索差押令状を要求する

12/21/2021



（２）捜査関係事項照会書への対応は図書館で判断する

『同上書』『法令との関係』（39頁）にあるように、刑事訴訟法第197条第2項は「捜査に関し公務所への照会」ができることを規定しているが、照会に応じなかった場合の罰則規定はないことがわかります。合理的な理由（正当な理由）がないときは照会に応じる義務があると解されていますが、公務員の守秘義務は正当な理由となります。この「職務上知り得た秘密」は、「公務員がひろくその担当する職務を行ううえでそのできた行政の客体的個人の秘密をも含む」とされています（渡辺重夫「図書館利用記録とプライバシー」（『知る自由の保障と図書館』102頁）参照）。

単純に言えば、「警察からの照会に緊急性が認められるか否か図書館で判断する。緊急性がなければ、照会状による提供は断る。警察はそれでも情報がほければ、捜索差押令状を裁判所に請求して出してくる（任意捜査から強制捜査に）。」ということになります。

捜査機関は1～2日で裁判所から捜索差押許可状を得ることができます。照会に応じるのは、

- ・ その余裕がなく、
 - ・ 他に代替方法がなく、
 - ・ 人の生命、財産等の危険が明白に認められる場合、
- に限定されるべきです。

12

改訂年月日：2019年7月3日 <http://www.jla.or.jp/committees/jiyu/tabid/658/Default.aspx>

幹部とか、元検察官の方々が証言しているように、「形式は任意だが、事実上は強制だ」というのです。それから、「企業などが拒否しても罰則はないが、ほぼ100%、数日～2週間程度で任意に回答が返ってくる」ということです。だから、捜査関係事項照会書をガンガン出していくというのが今の捜査のイロハになっているのではないかと想像できますし、私が前回JLISで講演した時も、そのあとの懇親会で、企業関係の方がツーっと私のところに来られまして、「うちはもう専門部隊がある。捜査関係事項照会に対応するのは組織的にやっていますよ。そうじゃないと業務に差し支えがありますから」といわれた。それぐらい大量に日常的に行われているということです。

具体例については共同通信が非常に詳細な報告を『世界』2019年6月号に書いています。そこに挙げた掲載企業だけでもすごい数です。カードの利用履歴、氏名・生年月日、住所、銀行口座、メールアドレス等々、照会書に応じて出しているということがわかっています。

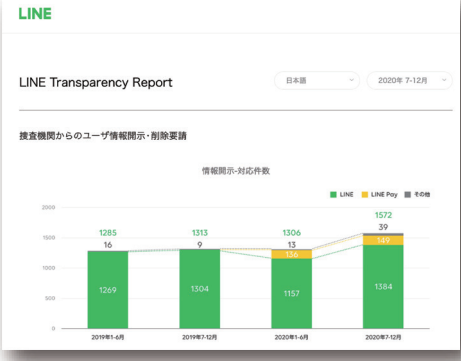
捜査関係事項照会をあらかじめ拒絶しますよとはっきり言っているのは、日本図書館協会さんだけです。照会に緊急性がなければ捜査関係事項照会による情報提供は拒絶し、捜索差押令状を要求するべきだと指針が示されています。ただ、図書館というのはそれぞれの図書館が独立した権限を持っていますし、管理権がありますので、協会の指針に従う必要はないわけです。日本中の図書館の頂点にある協会としてこういうふうを考えていますとはっきりと明示しているということは、利用者の思想信条を守る

という観点から当然でしょう。

企業の透明性レポートでも、こうした捜査関係事項照会を受けていますよということが明示されている場合もあります。これはLINEのTransparency Reportです。大部分は捜査関係事項照会というふうに報告が出ています、Facebookの場合はアメリカでデータを公開しているので、日本を検索してみると出てきます。2020年の下半期で66件あり、令状では0件、全部Emergency disclosure requests。捜査関係事項照会と思われそうですが、とにかく出してくれという緊急の要請があったので出しているようです。

捜査関係事項照会の問題点

この捜査関係事項照会について何が問題かという、たくさん問題があります。守秘義務には反しないとはいえ、個人情報保護の立場から見ると問題が多い。「必要な事項を求める」と刑事訴訟法は定めていますが、何が「必要な事項」なのかの判断は全部警察に委ねられていますし、照会先の選定も委ねられているし、外部からチェックすることはないし、照会業務のコストは全て照会を受けた側が負担することがほとんどです。照会手続が記録化されることはありません。そして極め付けは「保秘要請条項」が最初から事項照会書にプリントされています。「みだりに本照会に関して事項を漏らさないように」、と。つまり、個人情報の提供者本人には知らされないまま、全ての必要な事項とされているものが本人には知らせないまま警察に伝えられているということです。



2020年7-12月の要約

- 要請件数**: 2,100件の要請がありました。
- 対応の割合**: 75%の要請に対応しました。
- 対象回線数**: 2,120回線に対し情報が開示されました。
- 捜査機関**: 受領した要請のうち80%が日本の捜査機関からのものでした。

利用実態について（４）

・・・企業の透明性レポートに見る実態：１

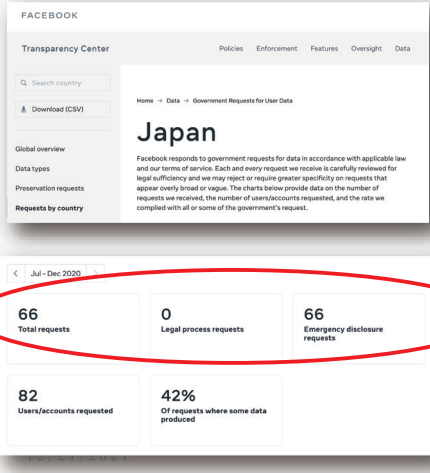
LINEの例

- 日本における捜査関係事項照会の内訳はLINE Payに関わる対応（113件）が大部分を占めております。LINE Payでは、捜査関係事項照会により詐欺やマネーロンダリングなどの具体的な嫌疑が示されており、かつLINE Payで被害を受けているか、LINE Payが犯罪の手段として用いられている場合にのみ対応しております。犯罪の具体的な嫌疑が捜査機関から示されていないユーザーの個人情報を開示することはありません。対応方針や開示される情報の詳細、具体例は[捜査機関への対応](#)をご覧ください。

利用実態について（５）

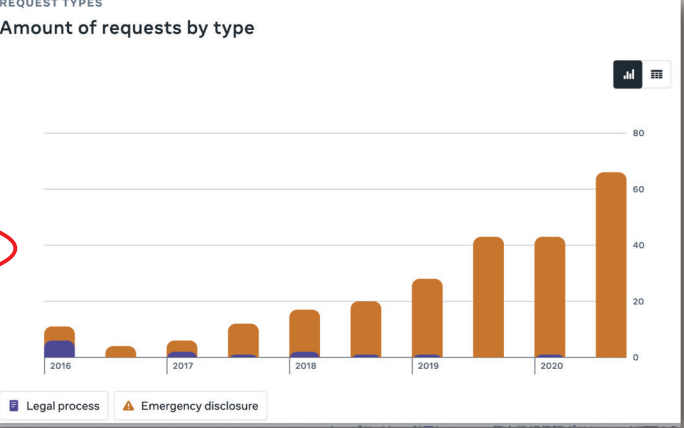
・・・企業の透明性レポートに見る実態：２

Facebookの例



REQUEST TYPES

Amount of requests by type

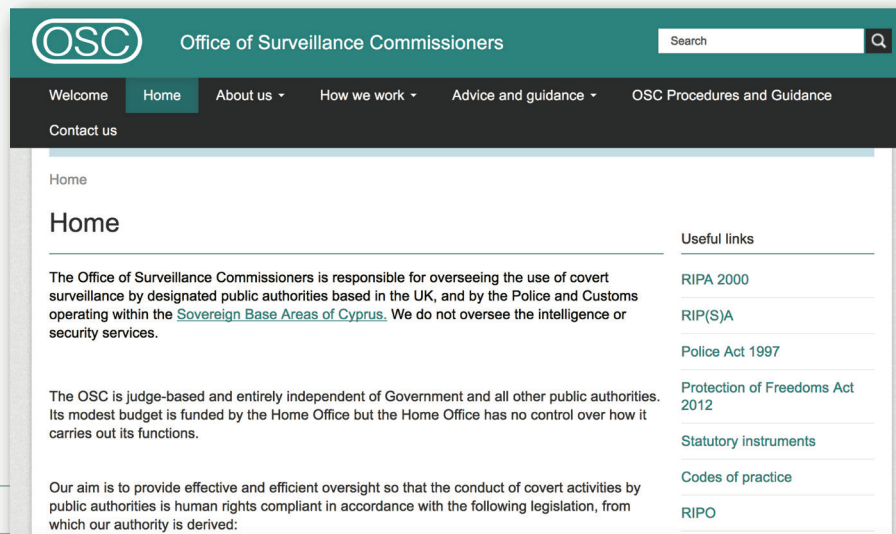


利用実態についてみると、GPSの個人位置の把握は、スマホゲームを利用していたら、そこから位置が特定できます。GPS発信装置などを装着する必要もないのです。

JILISでは、昨年3月に、非常に慎重な姿勢を取るべきだというガイドラインの提案をしています。あくまで案ですが、機微情報が含まれている場合には、捜査関係事項照会に対して慎重な判断を行わなければいけない、と警告しています。本来は強制処分に当たる捜査について、事業者は、捜査関係事項照会に応じず、令状を求めるべきだ、としました。

通信の秘密に属する事項については、捜査関係事項照会に応じるのは適切ではない、と具体的に提案しています。その理由は、先ほどから見てきたように、捜査関係事項照会には事前規制も事後規制も存在しないからです。加えて、保秘要請が含まれていますから、個人情報保護の観点から情報提供者に対するコンプライアンスを、その企業が果たさない可能性がある。約款上は、「法令に基づく場合」と個人情報保護法の規定に基づいていますから、表面上たしかにクリアされています。しかしそこにはいくつもの問題がありますよということを指摘しておきたいと思

監視検査官制度(Surveillance Commissioners)



います。

では続いて、海外事例を見てみましょう。

民間から情報を集めるときの例としてイギリスの街頭監視撮影、いわゆる街頭監視カメラの規律のやり方を挙げておきます。イギリスの場合には街頭監視カメラの使用に対して「監視検査官制度」(Surveillance Commissioners)というものがある。ホームページもありますね。つまり、街頭監視については事前規制と事後規制が用意されています。まず、事前規制に当たるのが先ほどの「監視検査官」です。市民に対して街頭監視していることを告知しているかどうかといったチェックをします。事後規制に当たるのは「監視検査官」(Surveillance Inspector)です。監視カメラ技術の精度であるとか、情報をどれぐらい保存して提供しているとかチェックしています。1998年のデータ保護法に基づいて第三者機関が監視することになっています。

スライドは、どういう人が「監視検査官制度」に就いているかを紹介したページです。重要な点は、監視カメラ検査官実務規範、これは非常に詳しく定められていることでしょうか。どうことが検査の対象かということが具体的に規定されています。さらに、市民が自分の監視データについて情報開示要請ができます。スライドはロンドンの交通機関に対して、自分の情報を提供するように求めることができる、そういう告知です。

こうした民間による情報収集がレイヤー1です。以上は民間部門からの情報収集について海外の事例を示しました。おわかりのように、日本では全くレイ

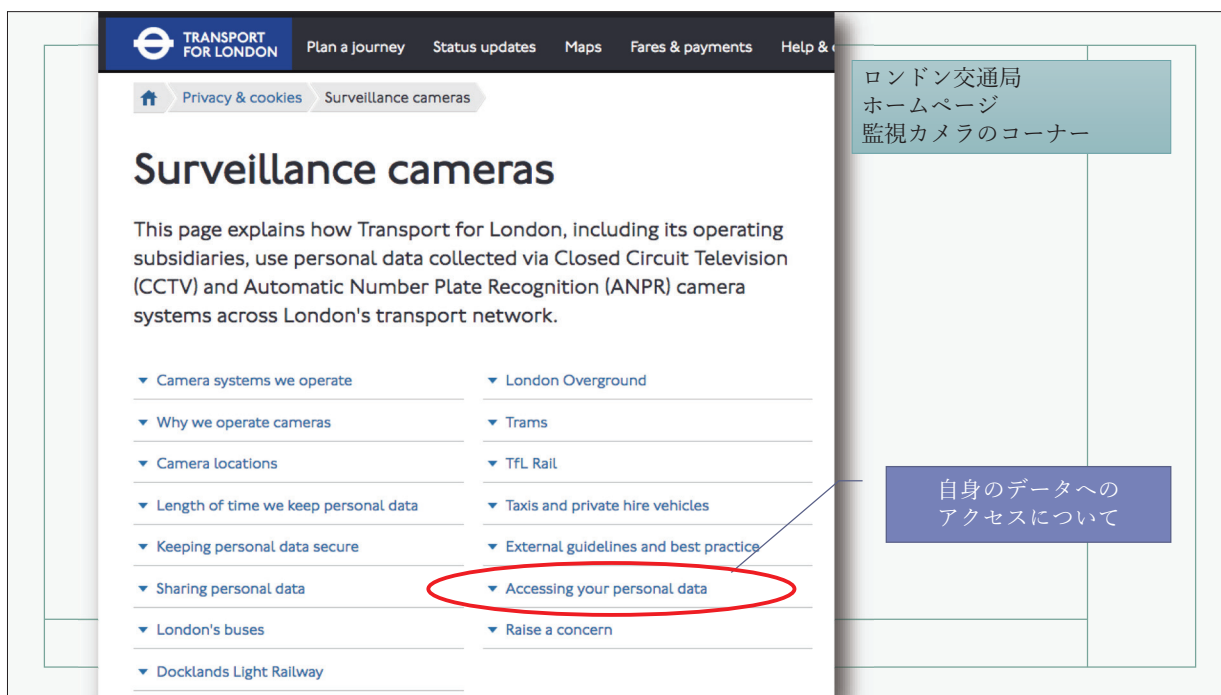
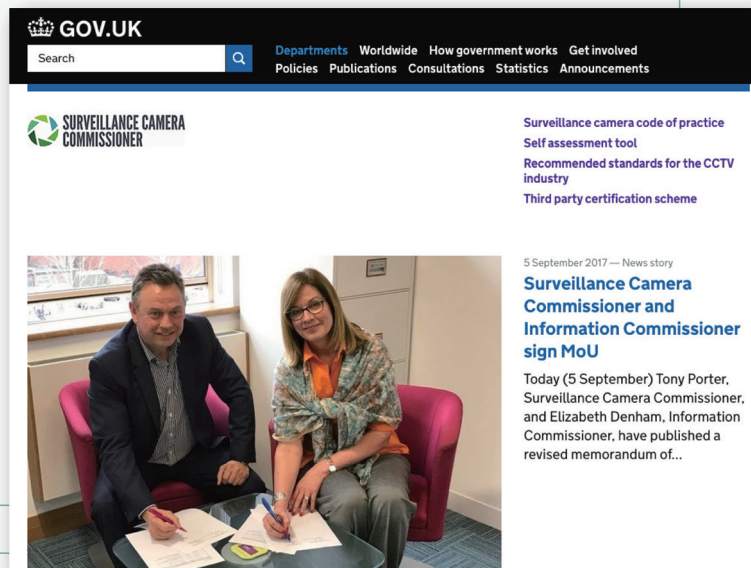
ヤー1について外部から統制するという制度がありません。

レイヤー2ー任意捜査

続いてレイヤー2は、中間層（任意捜査）の段階、任意処分といってもいいです。任意処分＝任意捜査、強制処分＝強制捜査を同義で使っています。法律上、強制処分は法の定めがないとできないということになっていますが、任意処分については法の定めがなくてもできる捜査です。一般的には内偵・聞き込み・尾行・張り込です。判例で認められているものとして写真撮影があります。公共空間での写真撮影です。それから、自動速度取締装置、おとり捜査、動画撮影、Nシステムなどです。Nシステムは皆さんご存知のように、全国主要幹線道路で網羅的にすべての通過車両の車両ナンバーを記録している装置です。それから、DNA情報の収集もあります。これは個人情報の究極ですがこれも任意処分として判例で認めています。平成20年に最高裁は、ゴミからDNAの情報を採取するのは占有権を放棄しているから構わない、という理屈でした。一方で、東京高裁平成28年判決では、相手方を騙してDNA情報を取得した場合はこれは違法としています。

このレイヤー2の問題を見ていきましょう。様々な収集されるデータ、例えば音声であるとか、映像、位置情報や行動履歴など広範囲にレイヤー2で集められています。先ほどの捜査関係事項照会のような不秘条項はありませんが、収集した相手方に収集した

監視カメラ検査官(Surveillance Camera Commissioner)：イギリス



事実を明らかにしませんから、情報を取得された側は認識することはできないという特性があります。最高裁は、この任意捜査については3つの要件、必要性、緊急性、相当性に照らして、適法判断をずっと続けてきています。このことは、裁判所による事前規制がないということを意味します。学説も、公道上を舞台としたデータ収集、例えばNシステムなどについては任意処分説に立っていて、任意捜査で収集していいと考えています。つまり、学説上も判例上も、大量収集であっても長期収集であっても、こと公道上に関する限り、事前規制の必要性を認めていないのです。

これに対して、海外の参考事例を見てみましょう。例として挙げるのは「スティングレイ」と呼ばれる携帯位置情報の探知装置です。スティングレイは、“ポストGPS捜査”などと言われているんですが、偽装携帯基地局のことで、IMSI(International Mobile Subscriber Identification) ナンバーを同意なく収集する装置です。そのため“IMSIキャッチャー”などとも呼ばれます。すなわち、この装置を使うと装置の周囲の一定範囲にある携帯電話番号を特定、収集できるのです。すべての携帯基地局は、設置した企業が契約しているIMSIナンバーだけを通信につなぐとい

“ステイングレイ”とは？

：偽装携帯基地局(Cell Site Simulator)の登場

- 別名「IMSI*キャッチャー」
 - 1. 特定の携帯電話の位置情報取得
 - 2. 特定の携帯電話の追尾監視
 - 3. 特定のエリアの携帯電話の割り出し
 - 4. 特定の携帯電話の通信を制御
- 1台7万ドル以上
- もととは軍・諜報機関用に開発、後に法執行機関に普及（13の連邦法執行機関と50以上の州法執行機関）
- ハリス社「ステイングレイ」（右写真）
- 可動式で自動車やドローンに搭載可能
- 2G通信への対応済み、新機種は4G通信まで

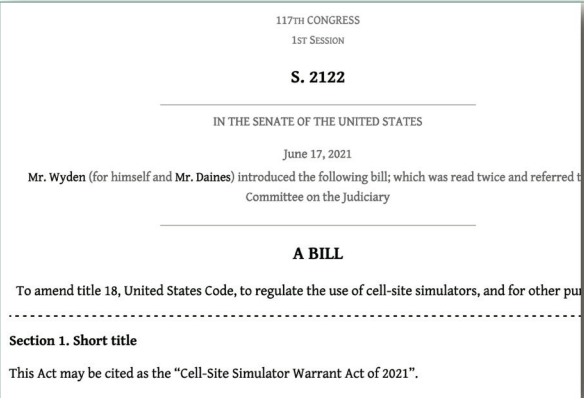
* International Mobile Subscriber Identity の略

出典：指宿「偽装携帯基地局を用いた通信傍受—携帯電話の無差別傍受装置「ステイングレイ」」法学セミナー60巻11号p.1-4 (2015)



米国連邦議会に規制法案提出(2020~)

- Cell-Site Simulator Warrant Act of 2021（基地局令状法）
- 個人・組織が合衆国内における基地局に規則で定められた場合を除いて故意に使用することは違法とされる
- 例外：
 - ✓ 令状が発布されている場合
 - ✓ 緊急性のある場合
 - ^{1,2} ✓ 開示要請のある場合



<https://www.govtrack.us/congress/bills/117/s2122/text>

32

う機能を持っていますが、この偽装携帯基地局というのは選別をしないんです。電波が届くすべての移動体のIMSIナンバーを収集してしまいます。その商品名のひとつがステイングレイです。これは、ハリス社の商品名で、他にもいろんな会社が同種機器を作っていますので商品名は異なりますが、一番有名なのがこのハリス社の製品です。IMSIナンバー以外に、特定の携帯の位置情報の取得、特定の携帯電話の追尾、特定のエリアにいる全ての携帯番号の割り出し、特定の携帯電話の通信を制御することができます。非常に高額なんですけれども便利な装置だと

いうことで、軍用で使われています。有名なのは米軍がオサマ・ビンラディンの位置を突き止めたのも、軍およびCIAがこのステイングレイを使って突き止めたんだろうというふうにいわれています。映画の中にもその場面が描かれていました。

このIMSIキャッチャーについては、2020年に米国議会に規制法案が提出されています。州によっては、令状を要求するところもあります。

レイヤー2に関する小括ですが、従来の任意処分説では「データ駆動型捜査手法」の本質・特性を捉えていないというのが私見です。これを規制するため

には、まず、こうした捜査手法を強制処分化して事前規制、すなわち令状でやればいいと考えられます。多くの強制処分論者がそうした主張をしています。けれどもそれでは、データを取得したあとの情報の在り方、保護の仕方、アクセスの仕方、廃棄の仕方がノーチェックです。事前規制万能説はやっぱりまずいでしょう。

これに対して、同じ強制処分説でも立法必要説は、データ取得後の規制に十分な留意をすること、つまり、今述べたような点についての事後規制が望ましいという立場です。この方向性については解釈学ではなく立法政策学に属するため、法学の世界ではまだきちんと検討されていないと思います。

レイヤー 2 と長期撮影の問題

レイヤー 2 の問題が出てきているもう一つの例として、長期撮影についてお話ししたいと思います。先ほど、写真撮影は任意処分として認められると紹介しました。憲法・刑事訴訟法では最も有名ないわゆる肖像権という概念が出てきた昭和 44（1969）年の最高裁大法廷判決が始まりです。京都府学連デモ事件という名前でも有名ですが、デモをやっている学生たちが府の条例違反で、整然とデモをせず、ジグザグデモみたいなことをやったので、その場を写真撮影したところ、撮影が適法かどうかということが争われた事案です。最高裁は規範として、憲法上保護される“肖像権”が個人にはあってみだりに撮影されない自由がある、と認めました。一方で、こうした現

場での撮影について任意処分として緊急性、必要性、相当性があれば適法だとしました。

このような撮影は一瞬の撮影、静止画です。ところが、今日、捜査機関が行っている長期撮影についてはまだ最高裁はきちっとした判断を示したことがありません。長期撮影がなぜ問題かという、様々な目的や手法が多岐にわたるいろんな撮影行為が登場していて、京都府学連デモ事件の際に 1969 年に立てたような基準では規律しようがない。警察には大量の撮影機器が集積されていて外部からまったく規制なく使われています。この問題について詳しくは、2020 年の法とコンピュータ学会のシンポジウムでお話ししました。これは、『法とコンピュータ』という雑誌に掲載されていますので、詳しくはそちらをご覧ください（39 号 45 頁以下）。

さて、レイヤー 2 の捜査手法に関して、社会的便益損失論者の見地から、事前規制より事後規制を主張される論者の中には、尾行と GPS を比較して、GPS の場合は位置情報・位置履歴が刻々と蓄積されるので害悪が大きいけれども、尾行はそれほど大きな害悪はないと考える考え方もあります。こうした考え方のアナロジーを撮影に当てはめてみましょう。すなわち、長期撮影の場合にも任意捜査と位置付けられている尾行と同じように考えてよいかという問題なんです。撮影記録データは（規制がないわけですから）長期間にわたって蓄積されているので、害悪の深刻さは十分にあると考えられます。

網羅的無選別な撮影に関する下級審判例では、定点的にずっと撮っているケースとして大阪のあいり

東京高判平成 21 年 1 月 29 日 N システム 国賠訴訟

- 公権力が正当な目的のために相当とされる範囲において **相当な方法で個人の私生活上の情報を収集し、適切に管理する限りにおいては**、その自由が制約を受け、国民にその受忍を強いても、憲法に違反しないとされる場合があると解すべき
- N システム等により個人の情報を収集し管理する **目的**は、自動車使用犯罪の犯人の検挙等犯罪捜査の必要及び犯罪被害の早期回復に限定されていて、**正当なもの**と認められ
- 収集、管理される情報は、何人も **公道を走行する際には外部から容易に認識することができるようにしなければならない**ことが法律によって義務づけられている **車両データに**限られていて、**公権力に対して秘匿されるべき情報ではなく**
- 取得されたデータは、上記目的達成に必要な短期間保存されることはあるが、その後 **消去され、目的外に使用されることはない**

手段の相当性

目的の正当性

秘密性パラダイム

目的外利用
の不使用

ん地区で何十カ所も定点で監視カメラによって撮影していた事案について、民事の損害賠償請求訴訟で、1箇所だけを除いて適法判断が出ています。

刑事事件では国交法違反事件というケースがあります。国家公務員の方が、休日を利用して共産党のチラシをポスティングしていたことが国公法が禁じる政治的中立に反するという事で起訴されたケースです。国交法違反については、最終的に最高裁で無罪になります。この事件では逮捕したのが公安の警察官なんですけれども、証人として出てきて、「証拠もありますし」と口を滑らしたんです。実はずっと

国家公務員の方を長期間ビデオ監視していたんです。それが裁判中に分かったので証拠開示を求めて数十本のテープが出てきて実態がわかったというものです。最近では、さいたま地裁で第三者の刑事裁判で検察側が出してきたという7ヵ月間という長期にわたるビデオ撮影について任意捜査として違法だとする判決が出ています。

こうした撮影方法のタイプ別に分けたのがこのスライドです。昭和44年の京都府学連デモ事件というのがマニュアルの静止画がタイプ1です。今の国公法事件のように、マニュアルで動画、しかも連続で、

東京地判平成18年6月29日（国公法違反事件）

・・・任意捜査として適法（一部違法）

- 多い日では、捜査官が11名もの多数に及び、かつ、捜査用車両が三、四台、ビデオカメラが4ないし6台も用意され、しかも29日間という長期間にわたり、毎日、実施
- 徒歩で被告人を尾行する際に、バック様の入れ物の中に入れたビデオカメラでもって、いわば隠し撮りする形で、被告人の行動をほぼ連続的に撮影したものであり、その余については、被告人の移動に従い次々と車両を移動させて公道上に停め、その車両内から又は降車して被告人の近くから、ビデオカメラでもって、同じく隠し撮りの形で被告人の行動を断続的に撮影
- 衆議院解散の翌日から総選挙の投票日前日までの29日間に限定してなされた行動確認について、その期間が長期間に過ぎるとまではいえない
- 本件の行動確認捜査（ただし、尾行、ビデオ撮影等の点は後述）は、社会通念上相当と認められる範囲内にあるというべきであって、警察比例の原則を逸脱しているとは認められず、適法に遂行されたというべき
- 本件ビデオ撮影は、公道上又はこれに準じるマンションの玄関内で行動している被告人を、通常の性能のビデオカメラで撮影したもの過ぎず、居宅内にいる被告人を撮影した場合等と比較して、プライバシーの保護の必要ないし期待が一段と低いことは否定できず、令状がない限りおよそ許されないとするまでの必要はないから、「強制の処分」ではなく、任意処分と解するのが相当

大量の機材投入、長期間撮影

隠し撮り方式

社会通念上相当との認定

公道上での撮影がプライバシーの期待を減殺

監視・撮影記録の種類と特徴

	撮影方法	撮影時点	被写体	撮影場所	判 例
タイプ1	マニュアル 静止画	現行 犯時	特定	不特定	京都府学連デモ事件 （最大判S44. 12. 24）
タイプ2	自動 静止画	現行 犯時	不特定	特定	オービス3事件 （最二判S61. 2. 14）
タイプ3	自動・動画	連続	不特定	特定	山谷争議団事件 （東京高判S63. 4. 1）
タイプ4	自動 マニュアル 動画	連続	不特定	不特定	あいりん地区事件・民事 （大阪地決H6. 4. 27）
タイプ5	マニュアル 動画	連続	特定	不特定	国公法事件* （東京地判H18. 6. 29）
タイプ6	マニュアル 動画	連続	特定	特定	防犯ビデオ同一性識別 （最二決H20. 4. 15）

* 東京高裁H22.3.29逆転無罪判決。最高裁H24.1.27無罪判決維持（刑集66巻12号1337頁）

ずっと撮っているみたいなのはタイプ5です。

国公法違反事件では裁判所は、長期撮影を任意捜査として適法だとしています。この事件では捜査官が11名、ほぼ1ヵ月、ビデオカメラを4台ないし6台用意して毎日その人が対象になっている人が朝出かけてから帰るまで、ずっと追跡していました。一部違法判断が出ているのですが、それはチラシを取りに共産党の地区の事務所に入った部分が思想信条の自由を脅かすということで、その部分の撮影については違法だとされたんですが、それ以外は長期の撮影をしていても適法だとしました。

撮影は尾行の際に行われていることから、公道上で行動しているところの被告人を撮影しただけとして、プライバシーの合理的な期待を認めませんでした。この事件では、開示された証拠から大規模なビデオ監視がされていたということがわかっています。たった1人をのべ180人で尾行撮影していたようです。具体的にどういう機器が使われていたかを見ると、名だたる日本を代表するITメーカーの製品を警視庁は使っているということがわかります。

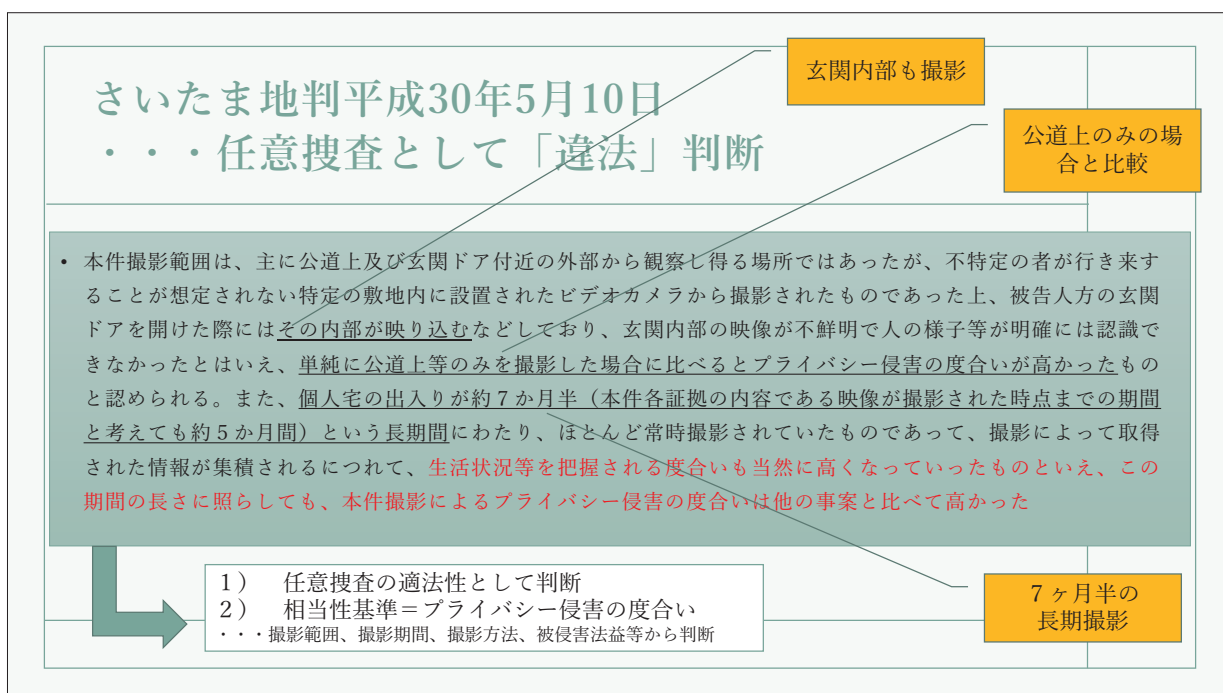
そうした中、最近さいたま地裁で、長期期間監視は違法とするという判断が出ました。任意処分として適法な範囲を越えて違法だとされました。7ヵ月半にわたって玄関内部が中まで見えるような、公道を挟んだ私人宅からずっと撮影していたというケースです。生活状況等を把握される度合いも当然に高くなっていた、その撮影期間の長さにも照らしてもプライバシー侵害の度合いは他の事案と比べて高いとして違法判断が出ています。長期撮影について違法判断が出たの

はおそらくこれが初めてのケースだろうと思います。

では海外では、こうした長期撮影をどうやって規律しているのかということですが、アメリカの場合、連邦は立法で規制しています。令状を取らなければなりません。

Nシステムについてはどう捉えていたかを見てみましょう。こちらでも国家賠償請求訴訟で争われています。裁判所は、車両は公道を走っているんだから外部から簡単にナンバーを見ることが可能である、だからそういう情報についてはプライバシーの期待はありません、公権力に対して秘匿されるべき情報ではないし、そもそもこのナンバーのデータは後で消去されるし、目的外に使用されることはないの、違法とはいえない、そういう判断をしました。

何度も申し上げますけれども、撮影というのは被処分者からすると撮られているのがわかりませんから、連邦の法執行機関がすべての長期撮影を、令状を取ってやっているとは私は思わないです。事後規制もありませんから、法令遵守状況、コンプライアンス状況は確認できません。現在、州レベルでは判例によって規制すべきかどうか分かれています。連邦と同じように修正4条の侵害、つまり捜索・差押えにあたっては令状を必要とするという修正4条要求は不要という否定論の立場の判例と、いや当たる、目視とは一緒に考えられないという肯定論とで分かれています。最高裁判決は出ていませんので、まだこの決着はついていないという状況です。ただし立法による規制も、今申し上げたように、事前規制ですから、日本と同じようにどれぐらい大量の監



視撮影をしていますが、事後的にはコントロールできないということです。

顔認識技術の問題

さて、長期監視はターゲット特定型の撮影ですが、ターゲットを特定しない網羅型の撮影はどうか。これが今、世界中で問題になっている顔認識、AIを利用した顔認識技術の問題です。皆さんが属されている会社でもこういった技術を開発、あるいは提供されているのではないかと思います。全国の警察で防犯カメラ映像やSNSの顔データと、前歴者の顔写真データベースを照合するシステムが運用されています。けれども問題が多い。どこからデータを収集するのか。データ保有者はデータ提供義務を負うのか。顔データは個人情報保護法で保護されないのか。データ保有者はデータ提供者に通知義務を負わないのか。照合する目的はいったい何か。誰が照合する権限を有するのか。

こういった点が一切不明です。不明のまま、これが稼働しているということです。

顔認識技術を利用した捜査に関して、諸外国にどんな規制動向があるかを見てみましょう。偶然ですが、この講演の依頼を受けてから世界中で怒涛のような動きがありました。先月、6月ですが、アメリカ、イギリス、カナダ、欧州で顔認識技術の捜査利用に関する厳しい指摘が相次ぎました。まずは米国。6月に米国議会に対する報告、Report to Congressional Requestersが出ました。20の連邦機関が顔認識技術

を利用している、ということです。そのうち14機関が法違反者を特定するためにこの技術を利用している。クリアビュー社を利用する機関が多いです。クリアビュー社というのは、顔認識・AI技術で最も大きなマーケットを持っていると言われている企業です。FBIは独自に4,000万人の顔写真データを保有しているそうです。その報告ですが、12の法執行機関に対して、その利用実績の追跡をきちんとしろ、どういふふうに使っているのか、また、個々の利用については評価制度を導入しろ、すなわち事後規制が必要、と指摘しました。

次にカナダを見てみましょう。プライバシー委員会というところが報告しています。日本と違ってプライバシー委員会は公的部門も監督対象にしていますから、クリアビュー社の顔認識技術を使った連邦警察(RCMP)の捜査に対してプライバシー保護法(Privacy Act)に違反すると警告がありました。クリアビュー社は、この警告によると、30億件のカナダ人の顔情報を同意なく収集している、ということです。プライバシー保護法によれば、カナダの政府機関は第三者が違法にカナダ人から収集した個人情報を利用することを禁じているのです。だから、カナダ議会は、第三者が情報を収集する際に法律を遵守することを確実にさせるよう政府機関に義務付ける法改正を行わなければダメだと報告しています。

イギリスでも去年(2020年)からこの顔認識技術をめぐる判例が出て、控訴院から欧州人権規約第8条に違反するという判決が出たため、大きな議論を呼んでいました。とうとうこの6月に、データ保護規

例：顔データの捜査活用

- ・ 2021年3月から全国の警察で防犯カメラ映像やSNSの顔データと、前歴者の顔写真データベースを照合する「顔認証システム」の運用開始

- * どこからデータを収集するのか？
- * データ保有者はデータ提供義務を負うのか？
- * 顔データは個人情報保護法で保護されないのか？
- * データ保有者はデータ提供者(個人)に通知義務を負わないのか？
- * 照合する目的は何か？
- * 誰が照合する権限を有するのか？

The screenshot shows a Yahoo! Japan news article. The headline is '捜査に顔認証、全国の警察で 3月から運用開始' (Face Recognition for Investigation, Nationwide Police Search from March). The article is dated 2020/9/13 (September 13, 2020) and is 6:00 PM old. It has 12 shares. The article text states that nationwide police have started using a face recognition system to cross-reference surveillance camera footage and SNS photos with a database of photos of suspects. It mentions that the system was started on September 12th. The article also notes that the system can identify individuals with similar facial features to the suspect's name or criminal record, and that it has been used in the past to identify suspects. It also mentions that the system has been used to identify suspects in the past. The article is from KYODO.

< 海外参考事例 4 >

顔認識技術を利用した捜査に 関する諸外国の規制動向

2021年6月、
米・加・英国、欧州で
顔認識技術の捜査利用に
関する厳しい指摘が
独立した機関から
相次いだ！

12/21/2021

46

GAO

United States Government Accountability Office
Report to Congressional Requesters

June 2021

FACIAL RECOGNITION TECHNOLOGY

Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks

『顔認識技術：連邦法執行機関はプライバシー
と他のリスクに適切なアセスメントをせよ』

米国

- ・ 2021年6月 米国議会報告文書
- ・ 20の連邦機関が顔認識技術を利用
- ・ 14機関が法違反者を特定するために顔認識技術を利用（FBIは一機関で6つのシステムを保有、国防省は2つのシステム保有）
- ・ クリアビュー社を利用するのは10機関、Vigilant Solution社が5機関
- ・ FBIは4000万人の顔写真を保有
- ・ 勧告：12の機関に対して、そうした技術の利用実績を追跡すべき、かつ、その利用について評価制度を導入すべき

12/21/2021

47

制局は公共空間でのライブの顔認識技術使用について、規制当局はその使用について、合法的な目的を確立すべき、法的根拠を明らかにすべき、手続条件を把握すべき、条件に合致しているかどうかを確認し、必要性やターゲットの選定について運用の合理性を把握すべき、そして事後規制を明確にすべきだと指摘したのです。

最後は欧州です。この4月に欧州議会が公共空間におけるAIを使った個人情報の収集を規制するという方針を打ち出しました。これは日本のメディアにも大きく報道されていましたが、6月になって、EDPB

（欧州データ保護会議）とEDPS（欧州データ保護監察機関）が合同でこの議会の方針を歓迎するとともに、AIを利用した顔認識技術による公共空間での個人情報の収集を中止するよう勧告したのです。こちらは全然報道されていないと思います。こちらのほうがはるかに重要です。

以上の、米・加・英・欧州の動きからの示唆は次のようなものです。個人情報収集した法執行機関に対する監督・調査・評価権限を持った独立した機関やメカニズムがちゃんと存在しているということがこれらからわかります。利用されている個々の（顔認識）

カナダ

- ・ 2021年6月、プライバシー委員会がクリアビュー社の顔認識技術を使った連邦警察(RCMP)の捜査はプライバシー保護法(Privacy Act)に違反すると警告
- ・ クリアビュー社は30億件のカナダ人の顔情報を同意なく収集している
- ・ プライバシー保護法は、カナダの政府機関が、第三者が違法にカナダ人から収集した個人情報を利用することを禁じている
- ・ カナダ議会は、第三者が情報を収集する際に法律を遵守することを確実にさせるよう政府機関に義務付けるための法改正を行う

ページ
12/21/2021

Office of the Privacy Commissioner of Canada / Commissariat à la protection de la vie privée du Canada

Search:

For individuals For businesses For federal institutions Report a concern OPC actions and decisions About the OPC

Home → OPC News → News and announcements

News release

RCMP's use of Clearview AI's facial recognition technology violated Privacy Act, investigation concludes

Canadian privacy regulators release draft guidance on police use of FRT; launch consultation with stakeholders in L to establish clearer rules, potentially new laws

NOTE: A teleconference for journalists will be held this morning. See details below.

GATINEAU, QC, June 10, 2021 – The RCMP's use of facial recognition technology (FRT) to conduct hundreds of searches of a database compiled illegally by commercial enterprise is a violation of the Privacy Act, an investigation has found.

In a Special Report to Parliament, the Office of the Privacy Commissioner of Canada (OPC) shared its findings regarding the RCMP's use of Clearview AI, a technology company that was itself the subject of a previous OPC investigation. The OPC, along with its provincial and territorial counterparts, also announce the launch of a public consultation to help establish clearer rules and consider whether new laws are desirable.

Clearview AI was found to have violated Canada's federal private sector privacy law by creating a databank of more than three billion images scraped from internet websites without users' consent. Clearview users, such as the RCMP, could match photographs of people against the photographs in the databank.

48

技術内容、利用目的、利用方法、収集されているデータの性質などが評価されています。プライバシー保護法令の遵守状態や危険性などのリスク評価もされています。ただ、事前規制が必要とされているわけではなくて、むしろ事後規制が提唱されているのが特徴です。日本では、公共空間での顔認識（生体認証）技術利用について、法執行機関が関わる場合について、誰が評価・監督するのかという疑問が出てきます（JR東日本による導入について批判的に考察したものとして、以下参照。「監視カメラで全乗客の顔を判別」JR東日本の出所者検知システムはどこに問題があったのか」PRESIDENT Online（2021年10月29日）<https://president.jp/articles/-/51210?page=1>）。

以上のレイヤー1とレイヤー2をまとめてみます。イギリスなどでは街頭監視撮影について事前・事後の規制があります。今日ご紹介したように顔認識技術の利用について2021年に入って規制方向が明確に出されています。それ以外の国では、捜査機関による個人情報収集については、まず令状取得という事前規制が進んでいるということもわかります。これに対して日本には、法執行機関による個人情報収集について外部の独立した査察・調査・評価機関が存在しないという問題があります。日本には、多くの情報収集捜査が無令状で実施されていて、事前規制も、外部評価もありません。いわゆる「任意処分説」、すなわち情報収集やデータ駆動型捜査は任意処分だと考えている学説は、任意・強制的の区別に指針を示してはいますが、具体的にどうやってそうした収集を

規制するのか、長期撮影があってもその撮影がこの基準に合致しているかどうかを誰がどのように判断するのかという枠組みについて何も提案していません。

レイヤー 3—強制捜査

それでは、最上位層（強制捜査）での情報収集について入ります。レイヤー3です。このレイヤーを考える最高の素材として、有名なGPS位置情報取得捜査を例に挙げたいと思います。これは当初任意捜査として実施されていました。この捜査手法が明るみに出たのは2004年、愛媛県警の内部文書がインターネットに流出した時です。有名なWinnyの暴露ウィルスに引っかかって、県警の警察官のパソコンのデータがインターネットに流出し、そこにこのGPS発信装置を取り付けて位置情報を取得するという捜査手法が文書として存在していたわけです。このスキャンダルを受けたかどうかはわかりませんが、2006年に警察庁がGPS発信装置を用いた位置情報取得捜査に関する内部通知を発出しました。もっとも、この通知が発出されたということも秘匿されていました。ずっとあとになって、これからご紹介するGPS捜査を違法と争った事件が出てきてからこの通知が出ていたことがようやくわかったんです。ずっと下って2017年3月、今から4年前に最高裁大法廷で、憲法35条という個人の私有物を搜索したり、私邸を搜索したりするには令状が必要だという有名な条項ですが、この憲法35条違反だという判決が出ます。GPS捜査

任意処分説を支持した学説例

- GPSを用いた捜査が、態様によっては、重大なプライバシー侵害を伴うが、「GPS的なツール」にもその機能において種々なものが考えられ、さらに得られた情報の使用目的・管理方法も様々なものが考えられる。多数の国民の重大な法益にかかわる犯罪の十分な嫌疑がある場合に、**緊急やむを得ない場合には、許される場合を認めざるを得ない。**
- 「GPS捜査一般が強制処分か否か」というのではなく、機器の性能のバラツキや機器使用態様の差異を踏まえた上で、どのような要件を備えれば適法となるのかが見えてくるような判断が必要であろう。

前田雅英「広域窃盗事犯の尾行とGPSを用いた追跡捜査」 WLJ判例コラム 73号(2016))

12/21/2021

58

この事件では
最長7ヶ月監視して
いたのに、緊急性は
問題ですか？

に令状が必要で、そして既存の令状ではできないから新しい立法を作りなさいという、15名全員一致の判決です。これは皆さんご存じだろうと思います。

まず、このGPS捜査が当初任意捜査として行われていたということ、そしてこの警察の考え方を支持していた学説があることを紹介したいと思います。GPS捜査は、任意でやっていいんだ、事前規制も事後規制もいらない、という学説が多数だったのです。

その中のひとつをご紹介します。「『GPS的なツール』にもその機能において種々なものが考えられる」として一律に規制するのに反対する見解です。いったいどういうツールがあると考えているのかということ明らかにせず、「得られた情報の使用目的・管理方法も様々なものが考えられる」などという。問題はそうした位置情報捜査を事前にチェックしたり、事後的にチェックしたりしなくていいか、という点です。「緊急やむを得ない場合には、許される場合を認めざるを得ない」というのですが、実際に大法廷判決の事案は、7ヵ月間にわたって位置情報を取得していたんです。全く緊急やむを得ない事態ではありません。どのような要件を備えていれば適法となるのか裁判所が個別の事案で判断すればいいという、つまり、これまでの任意捜査に対する最高裁判所の考え方の延長でやればいい、と考えていたのが任意処分説です。けれども、今回、大法廷はきっぱり違う考え方を取ったということです。任意捜査では当然無理で、強制処分としても無理で、令状だけではコントロールできないと言っているわけです。強制処分説どころか、立法必要説まで進んだのです。

では、GPS位置情報の取得方法にどういうものがあるか。基本的には次の4つしかありません。まず、大きく装着型と非装着型に分かれます。装着型というのは対象、ターゲットにGPSを記録する装置を付けて記録しますが、送信機能が付いているか付いていないかでわかれます。非装着型というのは、アクセス型といってターゲットの通信を中継している基地局の情報を取る方法と、インストール型というマルウェア、スパイウェアをインストールして位置情報を抜き取る方法があります。この4つしかないと考えられます。任意処分説はそのどれもきちんと詰めて検討していない。大法廷判決の事案で問題となった装着型の送信装置付きだけ任意処分のできるのか、他はどのようなかも不明です。おそらくこうした技術的な方法も知らないで論じているのではないかと思います。今回問題になったのは送信型の装着型GPSの場合ですが、大法廷は立法必要だと言った。他の手法も当然同様だと私は考えます。

警察は任意処分で行っていましたから、裁判所に「こういう機器をリースをします」とか「この車に付けます」という事前審査を受けていません。「移動追跡装置運用要領」という警察庁が作った内規に則って行われなければならないということになっていました。そこには「移動追跡装置を使用した捜査を任意処分として実施するに当たっては、その適正確保に遺漏のないように」という記載があります。つまり「保秘要請」です。どういうことかということ、位置情報を捜査で得たとしても、犯罪者が犯行現場に行っていたということがわかって、裁判所の逮捕状や

要領における使用要件

3 使用要件

任意捜査を行うに当たり移動追跡装置を用いるについては、次の各号に定める要件を満たさなければならないものとする。

- (1) 次に掲げる犯罪の捜査を行うに当たり、犯罪の嫌疑、危険性の高さなどにかんがみ速やかに被疑者を検挙することが求められる場合であって、他の捜査によつては対象の追跡を行うことが困難であるなど捜査上特に必要があること。

ア [REDACTED]

イ [REDACTED]

- (2) 犯罪を構成するような行為を伴うことなく、次に掲げる物のいずれかに取り付けること。

ア [REDACTED]

* 対象犯罪限定
* 非代替性要件

* 犯罪回避義務

同旭川地裁判決

「本件GPS捜査にあたっては、私物である本件ロガーが用いられている上、これが本件要領にいう移動追跡装置に該当することは明らかと言ふべきであるにもかかわらず、犬伏警部は、これについて**正式な手続き履践せず**に**使用していた**というのであって、この点も本件GPS捜査の違法性を高めている」

搜索差押え令状の請求にこの事実を用いてはならない。また、報道発表でも触れない。さらに検察官にも送致しないということです。大法廷判決の事案の一番の裁判でGPS捜査をやっていたことが明らかになって、初めて出てきたんですね。おそらくGPS捜査が争われた公判立会検事たちは、自分の扱っている事件で警察がGPS捜査をやっていた事実を知らなかったと思われます。

2019年に、これは大法廷判決のあとのことですけれども、旭川地裁がこの保秘要請について、令状主義の精神に反するという厳しい指摘をしました。つまり、データ駆動型捜査手法というのは、警察がこういった情報統制を図る傾向が顕著に見られます。外部的な統制を受けないことがデータ駆動型捜査の重要なポイントだと考えられているようです。

続いて、諸外国でGPS捜査をどうやって規律しているのかということで、合衆国、イギリス、ドイツ、フランス、オーストラリアを見てみたいと思います。

詳しくは、私が編著で出した『GPSとプライバシー保護』（現代人文社、2018）の一番後ろに細かい表が出ていますが、これはその抜粋版です。国によって事前規制か事後規制か、あるいは両方必要になっています。さらに、位置情報捜査の対象犯罪の特定があるかないか。実施要件としてどういうものがあるか。実施期間はどれぐらいか。被処分者へ事後告知があるかどうか。異議申し立て手続があるか。記録媒体の保存期間はどれぐらいか。廃棄や破棄の規定はあるか。査察制度はあるか。捜査実施報告義務が

あるか。いろいろな要件や手続きは国によってまちまちです。けれども、いずれの国もきちっと法律で定めているところが、大事なポイントでしょう。こうした規定、規制を持っていなかったは先進国では日本だけです。だから、大法廷が立法必要だという全員一致の判断を出したのも当然です。

他国のGPS捜査で行われているような事後規制を日本でやっているのは、唯一「通信傍受法」です。通信傍受は傍受された人に事後的に告知されて、記録消去要請ができたり、不服申し立てができるということになっています。当然ですが通信傍受は強制処分です。

GPS捜査最高裁大法廷の判決を見てみましょう。先ほどから何度も申し上げているように、任意捜査ではできない、令状がないとできないといっています。そして、事前規制がまず必要だとします。さらに事後規制も必要だということです。ただ、情報取得の後の情報蓄積については何も言っていません。事前審査で令状が必要だとは言っていますが、事前審査の限界も指摘しています。たとえ令状を出しても、裁判官による令状請求の審査を要することとされている趣旨を満たすことができないおそれがある、と。位置情報を取っていいという令状があったとしても、どれぐらいの期間・頻度で検索しているかということは事前には規制できませんから、事後的に確認・検証するしかない。これは通信傍受とよく似ています。だから立会いとかー今は通信傍受は立会いなしの方法も導入されましたー犯罪と関係のない通信が傍受されていないかをチェックする事後規制があるわけ

事前審査の限界を指摘する

データ駆動型捜査手法について
事前審査（令状方式）では収集
する範囲を統制
できない可能性を指摘

- 仮に、検証許可状の発付を受け、あるいはそれと併せて捜査を受けて行うとしても、GPS捜査は、GPS端末を取り付けた対象車両の所在の検索を通じて対象車両の使用者の行動を継続的、網羅的に把握することを必然的に伴うものであって、GPS端末を取り付けるべき車両及び罪名を特定しただけでは被疑事実と関係のない使用者の行動の過剰な把握を抑制することができず、裁判官による令状請求の審査を要することとされている趣旨を満たすことができないおそれがある

12/21/2021

71

4、新たな規制枠組みの必要

- 個人に関わる情報（データ）に関する「セキュア」な法整備を！
- レイヤー1、レイヤー2に対する事前規制（令状方式）の導入が必要
- レイヤー3に対する事後規制（告知・通知、不服申立て、監査査察）の導入が必要

事後規制

告知・通知

不服申立て

監査査察

12/21/2021

73

です。位置情報の取得の場合もそういう必要があることを大法廷は指摘しました。これは大法廷がよく書いたなと思います。つまり、事前規制が必要だと言いつつ、その事前規制の有効性について限界があるということを指摘したのです。

レイヤー3をまとめたいと思います。事前規制の方式は、今見たように令状主義、令状によって規制するという限界がGPS捜査によって明らかになってきました。有体物の場合は不要なものを差し押さえないように事前に明示しやすいし、事後的にもチェックしやすい。ですが、データの場合はほぼ不可能です。

「データ駆動型捜査」の規律はどうあるべきか

最後のパートに行きたいと思います。新たな規制枠組みが必要という主張です。特にレイヤー1とレイヤー2に対しては事前規制が必要で、レイヤー3に対しては事後規制が必要になります。その事後規制については、情報を取得されたという告知・通知、それから本人からの不服申し立て手続の整備、外部・第三者の監査・査察の導入が不可欠だと考えます。

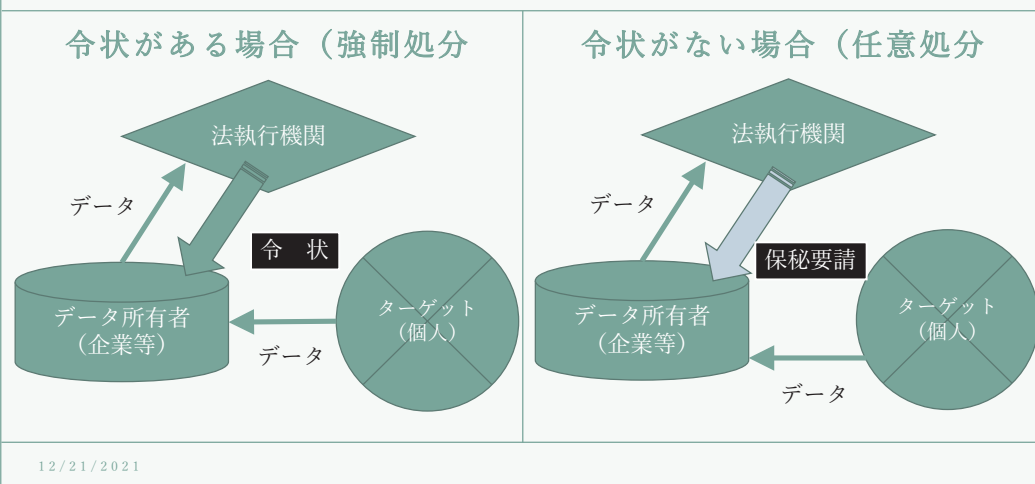
では日本におけるデータ駆動型捜査の規律状況を

国連麻薬及び犯罪対策局「重大・組織犯罪捜査における電子監視に関する現在の実務」（2009）による監視手法の分類

音声監視 (Audio surveillance)	映像監視 (Visual surveillance)	追跡監視 (Tracking surveillance)	データ監視 (Data surveillance)
電話盗聴	隠しカメラ	GPS位置情報取得	インターネット利用履歴 (クッキー情報) スパイウェアによる監視
インターネット音声会話 盗聴(VOIP)	車両搭載カメラ	携帯端末位置情報追跡	携帯端末追跡
屋内盗聴(盗聴機器使用)	身体装着カメラ	RFIDによる追跡	キーストローク監視
	赤外線透視	生体情報による監視	
	街頭監視カメラ		
通信傍受法	検証許可状	新たな立法	保全要請 搜索差押令状

出典：United Nations Office on Drugs and Crime (UNDOC)
Current practices in electronic surveillance in the investigation of serious and organized crime 2009

令状がある場合とない場合のデータの流れ



12/21/2021

78

まとめてみましょう。まず、国連が出している監視手法の分類を参考にします。国連の分類によると、監視というのは音声監視、映像監視、追跡監視、データ監視の4つです。それぞれ、具体的な手法がその下に例として挙げられています。音声監視だと電話盗聴とかインターネット音声会話盗聴とか屋内盗聴とかです。

これらについて日本でどういう規律があるかということを見たのが次のスライドです。電話盗聴については通信傍受法がありますし、GPSについては新たな立法をしろという判決があったわけです。映像監

視の赤外線監視については、配送物、宅配便の中身についてX線で捜査機関が撮影して、その映像をもとにその配送先の居宅の搜索差押許可状を取っていましたが、その疎明資料となっているX線の撮影についても検証許可状でやらなければいけないという判例が10年ほど前に出ました。これがあらゆる赤外線撮影に適用できるかどうかは不明ですが、そういう強制処分の必要を示した最高裁の判断も出ています。全体を見ていただいたらわかるように、規制があるのは少ない。今回大法廷からGPSを立法しなさいと言われているんですが、法執行機関としてはもう犯

(1 3 5)

警察は「独立した審査を受けている」

• Third, also within the executive branch the Prefectural Police is subject to independent supervision. This includes in particular the Prefectural Public Safety Commissions established to ensure the democratic administration and political neutrality of the police (108). These commissions consist of members appointed by the Prefectural Governor with the consent of the Prefectural Assembly (109) and are composed of citizens with no public servant position in the police in the five preceding years and have a security of office (in particular only dismissal for good cause) (109). According to the information received, they are not subject to instructions, and thus can be considered as fully independent (110). As regards the tasks and powers of the Prefectural Public Safety Commissions, pursuant to Article 38(3) in conjunction with Articles 2 and 36(2) of the Police Law they are responsible for "the protection of [the] rights and freedom of an individual". To this effect, they are empowered to "supervise" (111) all investigatory activities of the Prefectural Police, including the collection of personal data. Notably, the commissions "may direct the [P]refectural [P]olice in detail or in a specific individual case of inspection of police personnel's misconduct, if necessary" (112). When the Chief of the Prefectural Police (113) receives such information, he or she becomes aware of a possible case of misconduct (including the violation of duties), (s)he has to promptly inspect the case and report the inspection results to the Prefectural Public Safety Commission (Article 56(3) of the Police Law). Where the latter is not satisfied, it may designate one of its members to review the status of implementation. The Prefectural Public Safety Commission is satisfied that the incident has been adequately dealt with.

独立した都道府県公安委員会が監督。個人の権利や自由の保護に責任を負っている

公安委員会は、個人情報の収集を含む都道府県警察のあらゆる捜査活動について監督する権限を与えられている

罪者や犯罪組織に知られているので、立法を作っても意味ないという感じで、法制化されていません。

続いて、令状がある場合とない場合でデータの流れがどう違うかを見てみましょう。

上のひし形は法執行機関です。左側がデータ所有者、企業の方々はこちらになるわけです。捜査のターゲットになるのが丸のマークです。データは、個人からデータの所有者（企業等）へ提供されます。強制処分の場合、令状がある場合は法執行機関は令状でデータ所有者に対してデータを取ってくる。任意処分の場合、たとえば捜査関係事項照会などは保秘要請のうえでデータを取ってくるというのがこの図の説明です。こうした場合、ターゲットは自分が（情報を）取られたということがわかりません。仮に、通信傍受のように「あなたの通信を傍受しました」という告知があれば、被処分者も知ることができて、不服申し立てもできるわけです。あるいはデータ所有者（企業等）がデータ提供者（私人）に告知をすれば、認識できるわけです。データ所有者は、透明性レポートなどによって、警察に協力したことを外部に事後的に明らかにしています。個々のデータ提供者については告知していません。ですので、個人情報（データ保護）の観点からすると、透明性レポートでは不十分でしょう。令状がない場合も、法執行機関がもし本人に告知していれば、自分が情報を取られたということがわかるわけです。点線が告知を示しています。この告知があれば不服申し立てをして争うことができます。

しかし、こういった仕組みがそもそも発動できない

のが、今の日本のデータ取得捜査の実態だということです。

最後に、一昨年出ましたGDPRの十分性認定についてお話しします。日本の公的部門、法執行機関によるデータの収集について2019年1月23日に十分性認定がされたわけです。その認定は果たして十分かという問題提起を最後にしたいと思います。

この十分性認定に先立って、2018年の段階で、欧州委員会から日本の法執行機関による個人情報の収集・管理・保護については疑問があるということが公式に提示されました。これに対して日本側から回答があり、それを受けて十分性認定が出ました。本報告ではその十分性認定が果たして十分かという疑問を提示します。

まず、裁判所による十分な事前審査があると第132パラグラフで言っています。搜索・差押えでの情報収集は、裁判官によって厳格な「十分な根拠」基準に基づいて事前に審査されているから大丈夫だと言っています。これは、はかなくもGPS大法廷判決が、令状による事前審査方式ではいかなる位置情報がどの程度取得されたかを統制できないと、明白に指摘していました。それを知りながらこんな回答をしている。

国政調査権によって監督を受けているから大丈夫だと第134パラグラフには出てきます。国会が国政調査権を発動して、通信傍受実績に関する国会報告があるというふうに言っているわけです。しかし、個々の強制捜査で収集された個人情報の管理を独立して監督する権限はないでしょう。あくまで、去年はこ

のぐらいの実績がありましたよという報告を受けているだけです。だから、これも誤りです。

第135パラグラフでは、警察は「独立した審査を受けている」というふうに言っています。けれども、その審査をする「都道府県公安委員会」、Prefectural Public Safety Commissionsが監督して個人の権利や自由をきちんと守っているとの認定については、そんな実態はありません。今日は時間がないので省略しますが、各都道府県の公安委員会の議事録を見ても、警察が収集した個人情報についての報告は行われていません。議事録にそういった記載がないんです。ないにもかかわらずどうして独立した審査を受けていると言えるのか。先ほどGPS捜査任意処分説の論者として、日大の前田雅英先生の評釈を挙げたのは意味があります。前田先生は東京都の公安委員会の委員ですから、警視庁の行うこうしたデータ駆動型捜査手法について、今回の「十分性認定」に言わせると、監督する立場にあるはずで。私が確認したところ、都公安委員会がそうした審査を行った形跡はありません。これは、十分性認定としては不十分です。

第136パラグラフに総務省が監督していると出ているんですが本当でしょうか。今日ご出席の官庁の方、総務省の方が一度でも警察の個人情報収集について総務省が指導した実績があるとご存知であれば教えていただきたいんですが、寡聞にして知りません。これも十分性認定としては十分ではないでしょう。

まとめ

我が国のデータ駆動型捜査については、レイヤー1、レイヤー2、レイヤー3のいずれについても改善が必要だと思います。まず、レイヤー1・レイヤー2のターゲットを特定した、たとえば長期間撮影、こういうものについては事前の規制が必要です。レイヤー2の網羅的情報収集、誰かはわからないけれどもとにかく全部集めておくというような情報収集活動については、事後規制が必要だと思います。そこでは独立した

第三者機関によるチェックが行われなければならないと思います。レイヤー3、強制処分によって収集されたデータの保管やアクセス状況について、これは事前に、一応強制処分ですから、令状審査が行われているわけですが、取ったデータはどうなっているのか、どう使われているのか、いつ廃棄されるのかといった点について、監査・査察をする独立した第三者機関が必要だと思います。

以上、駆け足でしたけれども、最後にまとめておきたいと思います。日本では、データ駆動型捜査に関わり、レイヤー1（民間協力）からレイヤー3（強制捜査）に至るまで、通信傍受を別にして事後規制が存在しないし、収集した情報に対する統制は外部的にも内部的にも行われていない。GDPRに関して、法執行機関による個人情報保護の枠組みに関する「十分性認定」に関わって事前・事後の規制や、取得状況に対する監督が果たされているという日本国の回答には十分な根拠がない。GPS捜査に関する大法廷判決にもかかわらず、事前・事後規制の双方で法整備を懈怠している立法府・行政府には、個人情報保護につき立法不作為の過失責任がある、と私は考えます。

今日お話ししたようなことは、いろんなところに、この25年、四半世紀ぐらい書いてきました。GPS捜査については一冊の本が出ていますのでこちらをご参照いただきたいのですが、あれについてはあれを読んでください、これについてはこれを読んでくださいと、取材に来た記者にいちいち言うのが面倒くさいので、本にまとめることにしまして、今年度中には成文堂から『電腦空間と刑事手続』というタイトルで出版し、ブラウジングしやすいように皆さんに提供できる予定です。その節はご購入いただければと思います。

以上となります。ご清聴ありがとうございました。

==

本稿は2021年7月11日(日)～22日(木)に開催された第5回情報法制シンポジウムでの講演を基に作成したものです。

成城大学教授

指宿 信（いぶすき・まこと）

成城大学法学部教授。鹿児島大学法文学部教授、立命館大学法科大学院教授などを経て2009年より現職。刑事訴訟法、法情報学を専門とする。近著として、編集委員『刑事司法を考える・全7巻』（岩波書店）、編著『GPS捜査とプライバシー保護』（現代人文社）など。元・情報ネットワーク法学会副理事長、現・法と心理学会理事長。近刊として、『電腦空間と刑事手続』（成文堂・2022）を予定。