

データ駆動型捜査時代の規律方法 ：令状主義との訣別？

2021年7月22日
JILIS 連続講演会

指宿 信（成城大学法学部）
Makoto Ibusuki©2021

1

Agenda

はじめに

1. レイヤー 1 : 最下層（民間協力）での情報収集
2. レイヤー 2 : 中間層（任意捜査）での情報収集
3. レイヤー 3 : 最上位層（強制捜査）での情報収集
4. 新たな規制枠組みの必要

<付録> GDPR 2019年十分性認定は果たして「十分」か？

まとめ

はじめに

「他人が自分についての情報を得る方法は二つしかない
ー モニタリング／監視か、検索・検索を通じてだ。」

ローレンス・レッシング
『C o d e』
(2001、翔泳社) 258頁より



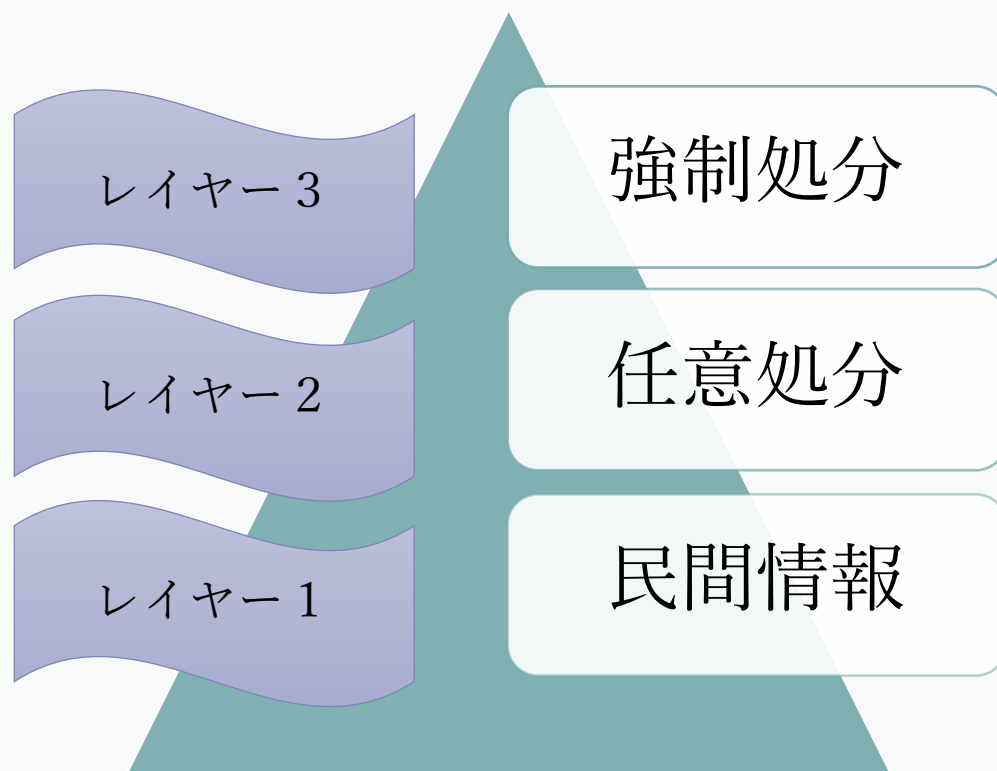
すなわち、
電子化、オンライン化された社会では、
モニタリング／監視には情報の「ターゲティング」と「追跡」が必要になる
検索・検索には情報の「収集蓄積」と「ブラウジング」が必要になる

つまり、
個人情報（データ）の保護とは、「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」を規制することと同義である

電子化問題への視座：1

- 電子化・オンライン化は捜査の文脈では「データ駆動型捜査手法」の問題である
- 捜査から公判の情報収集で、見逃されているデータ取得後の保護（事後規制）
- 電子化問題の特徴・・・情報処理過程になぞらえると、
 - ✓ インプット段階の**大規模化**（多様な入手経路、一元化、個人情報の利用、多様なデータ）
 - ✓ 処理段階の**不透明化**（アルゴリズムの検証不可能性）
 - ✓ アウトプット段階の**不公正化**（保管廃棄・アクセス権・他機会利用）
- 事前規制の時代は終わったのか？
- 事後規制にはどのような方法があるのか？

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）

レイヤー1

1、最下層（民間協力）での情報収集

具体例：捜査関係事項照会

1. 捜査関係事項照会とは
2. 根拠条文
3. 利用実態
4. 明文規定のない代表的な任意捜査
5. 明文規定のある任意捜査
6. 解釈と課題



詳細については、
JILIS講演会
2019年6月15日
指宿「捜査関係事項照会っ
て何だ？」参照のこと
[https://www.jilis.org/events/
2019/2019-06-15.html](https://www.jilis.org/events/2019/2019-06-15.html)

捜査関係事項照会とは

刑事訴訟法(昭和23年法律第131号)第197条第2項の規定による **捜査関係事項照会**は、**公務所又は公私の団体(以下「公務所等」という。)**に**報告義務を負わせるものである**ことから、当該公務所等は報告することが国の重大な利益を害する場合を除いては、当該照会に対する回答を拒否できないものと解される。また、同項に基づく報告については、国家公務員法等の守秘義務規定には抵触しないと解されている。しかし、照会先である公務所等に対し、強制力をもって回答を求めることができないことから、回答に伴う業務負担等、相手方に配慮した範囲内において行うものとする。

別記様式
様式第48号(刑訴第 197条)

文書番号	第	号
管理番号	第	号

捜査関係事項照会書

年 月 日

殿

警察署

司法

㊟

捜査のため必要があるので、下記事項につき至急回答願いたく、刑事訴訟法第 197条第2項によって照会します。

記

照 会 事 項

【照会警察署の所在地】〒

【担当者氏名】

(電話)

)

出典：愛媛県例規集平成12年1月21日 例規捜一第1号
○捜査関係事項照会書の取扱いについて

根拠条文

- 刑事訴訟法 197 条
- 捜査については、その目的を達するため必要な取調をすることができる。但し、強制の処分は、この法律に特別の定のある場合でなければ、これを行うことができない。
- **○2 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。**
- ○3 検察官、検察事務官又は司法警察員は、差押え又は記録命令付差押えをするため必要があるときは、電気通信を行うための設備を他人の通信の用に供する事業を営む者又は自己の業務のために不特定若しくは多数の者の通信を媒介することのできる電気通信を行うための設備を設置している者に対し、その業務上記録している電気通信の送信元、送信先、通信日時その他の通信履歴の電磁的記録のうち必要なものを特定し、三十日を超えない期間を定めて、これを消去しないよう、書面で求めることができる。この場合において、当該電磁的記録について差押え又は記録命令付差押えをする必要がないと認めるに至ったときは、当該求めを取り消さなければならない。
- ○4 前項の規定により消去しないよう求める期間については、特に必要があるときは、三十日を超えない範囲内で延長することができる。ただし、消去しないよう求める期間は、通じて六十日を超えることができない。
- **○5 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。**

利用実態について（１）・・・元警察幹部・元検察官の証言

- コンビニエンスストアの防犯カメラ映像、携帯電話の通信記録、銀行口座の明細、戸籍謄本、学校の成績など、国民のプライバシーに関わるあらゆる情報を、警察は本人に知られることなく、容易に入手している・・・警察では多くの場合、刑事訴訟法１９７条の「捜査関係事項照会」という手続きが使われる。捜査に必要な事項について他の役所や民間企業、団体に報告を求めることができるという規定だ。**形式は任意だが、事実上は強制だ**

➤ 原田宏二氏（元北海道警釧路方面本部長）毎日新聞2014年5月9日「情報技術の発展とプライバシー」

- ・・・・対象となる犯罪には何ら制限がないので、捜査のために必要であれば、世間を賑わす特異重大事件から軽微な事件に至るまで、オールマイティーに使うことができる。問合せを受けた**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。**犯罪捜査という公的な目的によるものである上、断っても後日令状で事務所を搜索され、差押えをされるばかりか、その対応に社員が割かれ、事務もストップさせられるのが関の山だからだ。

➤ 前田恒彦氏（元検事）のブログより

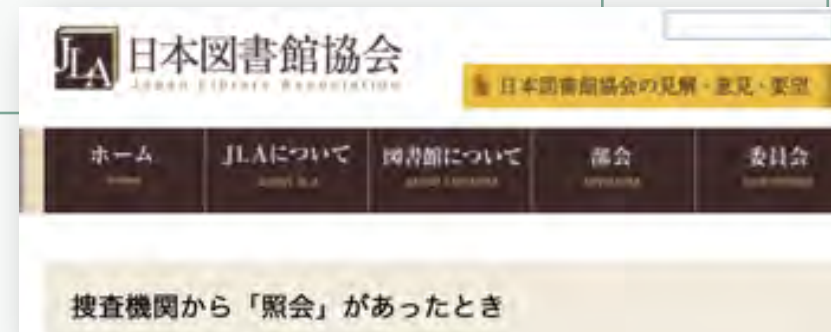
➤ <https://news.yahoo.co.jp/byline/maedatsunehiko/20160525-00058016/>

利用実態について（２）・・・企業アンケート調査による実態

- 「捜査上有効なデータ等へのアクセス方法等一覧表」（最高検察庁法科学専門委員会作成）
- メタデータ：データ等名称・概要、入手可能なデータ等の内容、保存期間、保有先・問い合わせ窓口・照会先、照会方法、照会・差押等に当たっての留意事項、その他参考事項、備考
- 掲載企業：主要航空会社、鉄道・バス会社、電気・ガス会社、ポイントカード発行会社、クレジットカード会社、消費者金融、携帯電話会社、コンビニ、スーパー、家電量販店、ドラッグストア、パチンコ店、遊園地、アパレル、居酒屋、劇団、映画館、ガソリンスタンド、カラオケ店、インターネットカフェ、ゲーム会社
- 共同通信社社会部取材班が２９０社にアンケート
- 回答例：カードなどの利用履歴（７８社）、氏名・生年月日、住所（７２社）、電話番号（６１社）、銀行口座（１９社）、メールアドレス（１５社）、家族情報（３社）その他、店内防犯カメラ画像やレシート情報

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、搜索差押令状を要求する



（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しるべき行政の客体側の個人的秘密をも含む」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）。

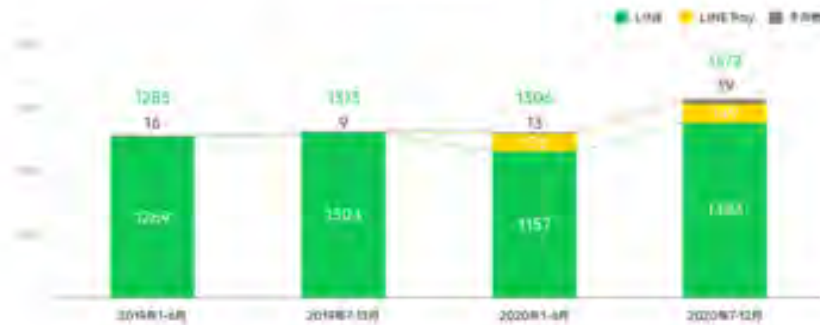
単純に言えば、「警察からの照会に緊急性が認められるか否か図書館で判断する。緊急性がなければ、照会状による提供は断る。警察はそれでも情報がほしければ、搜索差押令状を裁判所に請求して出してくる（任意捜査から強制捜査に）。」ということになります。

捜査機関は1～2日で裁判所から搜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。

捜査機関からのユーザ情報開示・削除要請

開示・対応件数



2020年7-12月の要約



要請件数

7/22/21の要請が受け付けました。



対応の割合

7/22/21の要請に対して75%の対応が完了しました。



対象回線数

7/22/21の要請に対して対象が特定された回線数は1,234件です。



捜査機関

7/22/21の要請に対して80%の捜査機関からの対応が完了しました。

利用実態について（4）

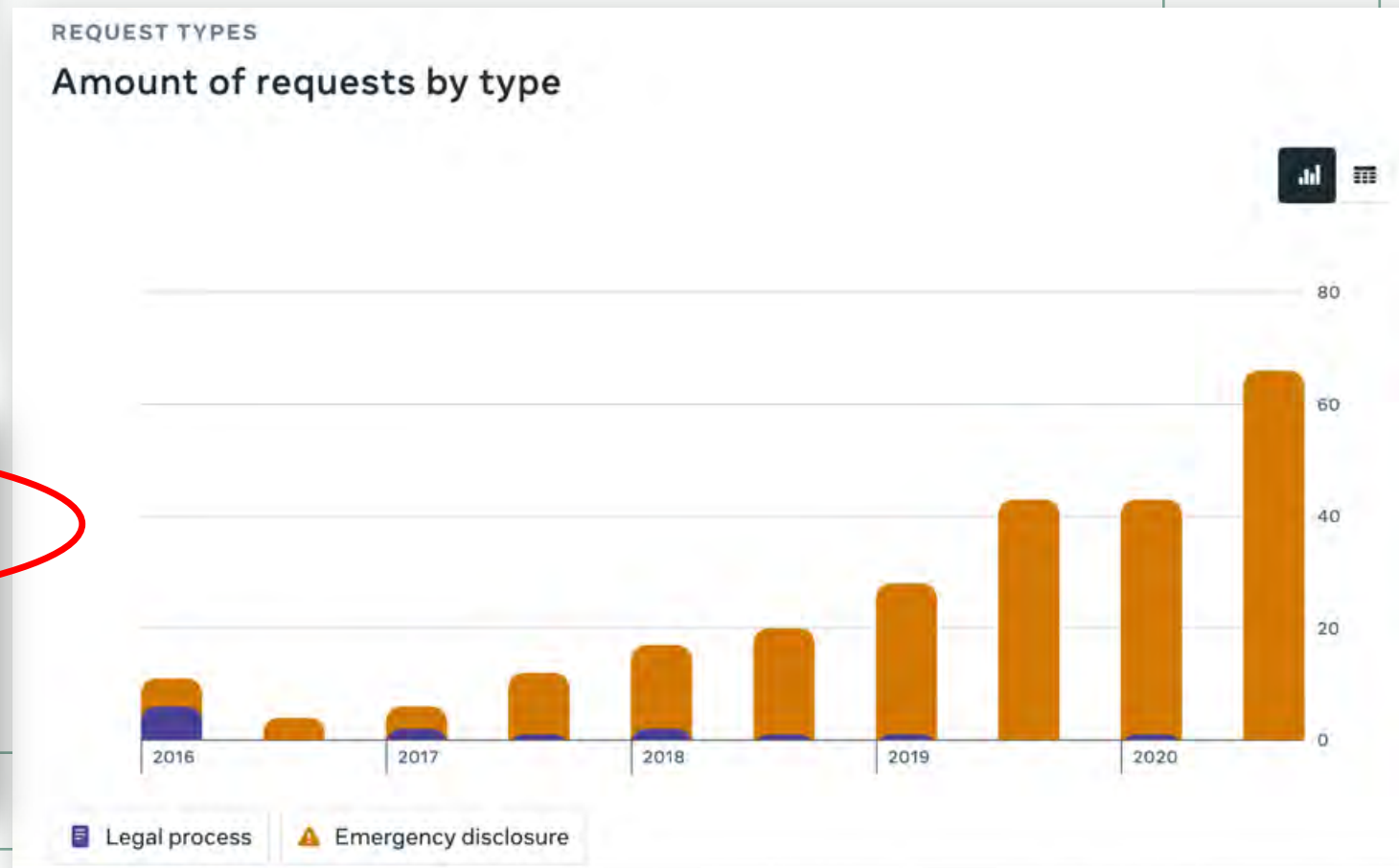
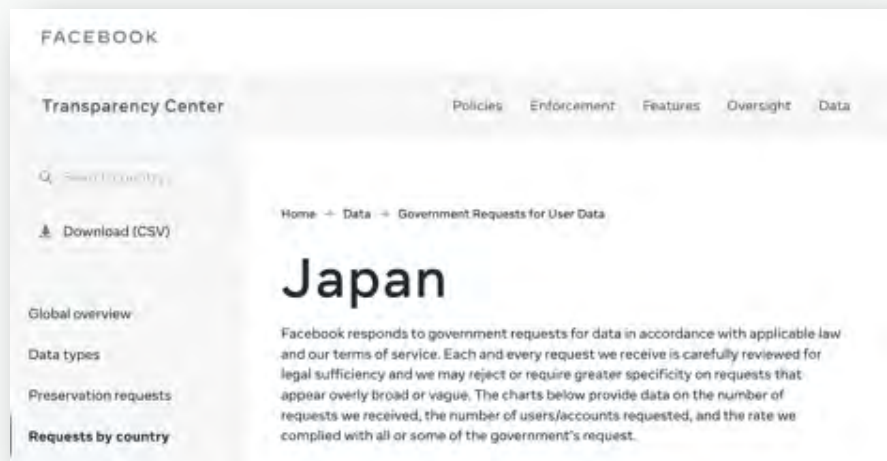
・・・企業の透明性レポートに見る実態：1

LINEの例

- 日本における捜査関係事項照会の内訳はLINE Payに関する対応（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



解釈と課題

- 任意捜査の範疇とされるが、実態は無規制
- 対象
 - 公務所：国家機関、地方自治体の機関、裁判所、検察庁、警察も含む
 - 団体：法人格の有無を問わない。個人と同視されるものは含まない
- 報告義務：（通説）原則として報告すべき義務を負うが直接的に強制する手段・方法はない。報告しても、国家公務員法・地方公務員法などの規定による守秘義務には反しない。
- 報告の内容：条文上「必要な事項」。具体的限定なし。（弁護士）客観的事項に限るべき（捜査実務）意見やその他の情報まで得ようとする場合がある

【問い①】 守秘義務に反しないとはいえ他の法令との抵触があるのではないか？

【問い②】 何が「必要な事項」に当たるかを誰が決めるのか？

【問い③】 照会先の選定について誰が決めるのか？

【問い④】 照会業務のコストは誰が負担するのか？

【問い⑤】 照会手続は記録化され、事後的に検証できるのか？

捜査関係事項照会書 平成 24 年 月 日 株式会社トリニティー 代表取締役 兼 佐 田 隆 雄 氏 愛知県 豊 田 市 司法書士 佐 田 隆 雄 氏 司法書士 佐 田 隆 雄 氏 照会のため必要があるため、下記事項につき照会させていただきます。御事柄に法第 197 条第 5 項によって照会します。 照 会 書 照会事項は、() に入力してください。 1. 照会事項 2. 照会事項 3. 照会事項 4. 照会事項 5. 照会事項 6. 照会事項 7. 照会事項 8. 照会事項 9. 照会事項 10. 照会事項 なお、みだりに本照会に関する事項を漏らさないよう、刑事訴訟法第 197 条第 5 項によって求めます。 法 官		照会事項は、() に入力してください。 1. 照会事項 2. 照会事項 3. 照会事項 4. 照会事項 5. 照会事項 6. 照会事項 7. 照会事項 8. 照会事項 9. 照会事項 10. 照会事項
【照会照会事項の所在地】 〒 467-0000 名古屋市中区千代田 1-1-1 千代田ビル 10 階 1001 号室 佐田隆雄事務所 【担当氏名】 新 宮 昭 彦 電話 052-942-0110(内線)		照会事項は、() に入力してください。 1. 照会事項 2. 照会事項 3. 照会事項 4. 照会事項 5. 照会事項 6. 照会事項 7. 照会事項 8. 照会事項 9. 照会事項 10. 照会事項

なお、みだりに本照会に関する事項を漏らさないよう、刑事訴訟法第197条第5項によって求めます

【問い⑦】全ての照会書中に定型文化されているのは、適正性・合理性を欠くのではないか？

【問い⑧】 情報提供を求められた公務所・団体には本人への通知義務があるのではないか？

【問い⑨】 保秘要請の必要性・妥当性を誰が
チェックできるのか？

【問い⑩】 全て「捜査の秘密」で正当化可能か？

利用実態について（６）・・・スマホゲームの利用履歴を位置情報把握に使用

スマホゲーム、捜査に利用か GPSで個人位置把握

ツイート

810

シェア0

2019年1月14日 朝刊

捜査当局がスマートフォンゲームの運営会社を通じ、衛星利用測位システム（GPS）機能を使って事件関係者の位置情報を取得している可能性が高いことが分かった。検察の内部文書に取得方法を詳細に示した記載があり、当局が捜査上必要な場合に企業などに令状を示さず報告を求める手続き「捜査関係事項照会」で取得できるとされていた。

大手携帯電話会社から当局が位置情報の提供を受ける際は、令状が必要とされているため、ゲーム会社を通じる手法が「抜け道」になり得る。GPSを巡っては、二〇一七年三月の最高裁判決が深刻なプライバシー侵害を指摘し、令状なく端末を取り付ける捜査手法を違法と認定した。当局が実際にゲーム会社から取得していれば、問題性の高い取り扱いと言える。

内部文書に記載されているゲーム運営会社は三社。いずれも自社のホームページに「政府機関からの要求で個人情報を開示することがある」などと記している。

この文書は共同通信が入手した、検察内部で共有されているリスト「捜査上有効なデータ等へのアクセス方法等一覧表」。リストによると、対象者のメールアドレスや氏名、住所、携帯電話番号などを三社に伝達すると、運営会社はそのユーザーが使うスマホの位置情報を提供する。

スマートフォンゲーム会社を通じた位置情報取得のイメージ



JILISの提案(2020年3月)

4. 1. 4 要配慮個人情報等の機微情報について

個人情報保護法は、要配慮個人情報については、その取扱いによっては差別や偏見を生じるおそれがあるため、特に慎重な扱いが求められる個人情報を類型化したものである。

また、購買履歴や取引履歴等は、要配慮個人情報を推知させる情報を含み得るものである。

捜査機関への報告内容に、これらの情報が含まれる場合には、捜査関係事項照会に対して、より慎重に判断を行うべきである。

4. 2 令状の有無

捜査関係事項照会は、任意処分である。他方で、強制処分について、捜査機関は、令状を取得しなければならない(上記3. 1ご参照)。したがって、事業者は、強制処分について、裁判所より搜索差押許可状等による令状が発付され、当該令状の提示を受けた場合にのみ、開示等を行わなければならない。そのため、本来は強制処分にあたる捜査について、事業者は、捜査関係事項照会に応じるべきではない。

4. 3 通信の秘密

捜査関係事項照会がなされた場合において、電気通信事業者には通信の秘密を保護すべき義務があり(電気通信事業法第179条、有線電機通信法第9条、第14条第1項)、通信の秘密に属する情報(通信内容のほか、通信当事者の住所・氏名、発受信場所及び通信年月日等通信の構成要素並びに通信回数等通信の存在の事実の有無を含む。)については、令状なくして、捜査機関に提供してはならない。

したがって、通信の秘密に属する事項については、捜査関係照会に応じるのは適切でない。

* 捜査関係事項照会への業者の対応に慎重な姿勢

* 理由＝捜査関係事項照会には事前規制も事後規制も存在せず
保秘要請が含まれていて、個人情報の保護の観点から、当該情報の提供者に対して負うべきコンプライアンスを果たせない可能性がある

<海外参考事例 1>

英国における街頭監視撮影の規律

監視検査官制度(Surveillance Commissioners)

The screenshot shows the official website of the Office of Surveillance Commissioners (OSC). The header is teal with the OSC logo and name on the left, and a search bar on the right. A dark navigation bar below the header contains links: Welcome, Home (highlighted), About us, How we work, Advice and guidance, OSC Procedures and Guidance, and Contact us. The main content area is white. On the left, under a 'Home' breadcrumb, is a large 'Home' heading followed by a paragraph about the OSC's role in overseeing covert surveillance. Below this is another paragraph about the OSC's independence and funding. At the bottom left is a paragraph about the aim of the OSC. On the right, under a 'Useful links' heading, is a list of links: RIPA 2000, RIP(S)A, Police Act 1997, Protection of Freedoms Act 2012, Statutory instruments, Codes of practice, and RIPO.

OSC Office of Surveillance Commissioners

Search

Welcome Home About us ▾ How we work ▾ Advice and guidance ▾ OSC Procedures and Guidance Contact us

Home

Home

The Office of Surveillance Commissioners is responsible for overseeing the use of covert surveillance by designated public authorities based in the UK, and by the Police and Customs operating within the [Sovereign Base Areas of Cyprus](#). We do not oversee the intelligence or security services.

The OSC is judge-based and entirely independent of Government and all other public authorities. Its modest budget is funded by the Home Office but the Home Office has no control over how it carries out its functions.

Our aim is to provide effective and efficient oversight so that the conduct of covert activities by public authorities is human rights compliant in accordance with the following legislation, from which our authority is derived:

Useful links

- [RIPA 2000](#)
- [RIP\(S\)A](#)
- [Police Act 1997](#)
- [Protection of Freedoms Act 2012](#)
- [Statutory instruments](#)
- [Codes of practice](#)
- [RIPO](#)

監視検査官の任務

- 対監視監督委員(surveillance commissioners)

- 侵入捜査の承認
- 家屋侵入の承認
- 法的特権侵害に関する事項の取り扱い
- 捜査機関のオンサイトビジット（訪問査察）

主として**事前規制**

- 対監視査察官(surveillance inspector)

- 戦略・政策・手続きの制定
- 訓練計画の立案
- 内部監査、質的保障
- 監視捜査技術基準の制定
- パフォーマンス測定、分析報告
- 他機関との協調
- リスクアセスメント
- 取得情報の保存、審査、破棄に関する規定

主として**事後規制**

イギリスにおける関連法例・ガイドラインの変遷

- 1998年データ保護法

- 公的分野及び民間分野における個人データ取扱全般を規律
- 監視カメラで取得される個人データも保護対象

- 1998年犯罪・秩序違反法

- 2000年 ICO（情報検査官オフィス）によるCCTV実務規範策定

- 2008年 実務規範改訂

- 2012年自由保護法

- 監視カメラシステムを規制
- 内務大臣による監視カメラ実務規範の策定義務
- SCC（監視カメラ監督官）の設置（内務大臣任命）

- 2013年 監視カメラ実務規範策定

- 地方自治体や警察設置のカメラのみが対象。民間は対象とせず
- 民間設置カメラは依然ICOの実務規範に基づく

- 2014・2015年 ICOがCCTV実務規範改訂

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



[Departments](#) [Worldwide](#) [How government works](#) [Get involved](#)
[Policies](#) [Publications](#) [Consultations](#) [Statistics](#) [Announcements](#)



**SURVEILLANCE CAMERA
COMMISSIONER**

[Surveillance camera code of practice](#)
[Self assessment tool](#)
[Recommended standards for the CCTV industry](#)
[Third party certification scheme](#)



5 September 2017 — News story

Surveillance Camera Commissioner and Information Commissioner sign MoU

Today (5 September) Tony Porter, Surveillance Camera Commissioner, and Elizabeth Denham, Information Commissioner, have published a revised memorandum of...

2013年 監視カメラ検査官実務規範



Home Office

**Surveillance Camera Code of Practice
Pursuant to Section 29 of the
Protection of Freedoms Act 2012**

• 実務規範による監視カメラ12原則

- ① 特定目的
- ② プライバシー侵害と正当化根拠の考慮
- ③ 透明性の確保（情報提供と不服申し立て）
- ④ 法的責任と説明責任
- ⑤ 明確な準則・政策・手続
- ⑥ 妥当な保管期間
- ⑦ 保管映像・情報へのアクセス制限
- ⑧ 運用者の義務（法令遵守）
- ⑨ 無権限使用の禁止
- ⑩ 効果的な審査と監査の導入
- ⑪ 合法目的と必要性
- ⑫ データベースとのマッチングに関する正確性



Surveillance cameras

This page explains how Transport for London, including its operating subsidiaries, use personal data collected via Closed Circuit Television (CCTV) and Automatic Number Plate Recognition (ANPR) camera systems across London's transport network.

- ▼ Camera systems we operate
- ▼ Why we operate cameras
- ▼ Camera locations
- ▼ Length of time we keep personal data
- ▼ Keeping personal data secure
- ▼ Sharing personal data
- ▼ London's buses
- ▼ Docklands Light Railway
- ▼ London Overground
- ▼ Trams
- ▼ TfL Rail
- ▼ Taxis and private hire vehicles
- ▼ External guidelines and best practice
- ▼ Accessing your personal data
- ▼ Raise a concern

ロンドン交通局
ホームページ
監視カメラのコーナー

自身のデータへの
アクセスについて



Access your data

Under the Data Protection Act 1998 you are entitled to ask to see any personal information that we hold about you. This page explains how to make a 'Subject Access request' to TfL.

[▼ Oyster or contactless journey history](#)[▼ Taxi and Private Hire licensing](#)[▼ Congestion Charge and Low Emission Zones](#)[▼ Traffic enforcement and monitoring cameras](#)[▼ London Underground CCTV cameras](#)[▼ Santander Cycles](#)[▼ TfL's Customer Contact Centre](#)[▼ TfL job applications and staff records](#)[▼ TfL Pension Fund](#)[▼ Dial-a-Ride](#)

個人情報保護法に
に基づく
個人からのデータ
アクセス権を保障

レイヤー 2

2、中間層（任意捜査）での情報収集

明文規定のない代表的な任意捜査一覧

- 内偵・聞き込み・尾行・張り込み*
- 写真撮影（最高裁大法廷昭和44年12月24日）
- 自動速度取締装置（最高裁昭和61年2月14日）
- おとり捜査（最高裁平成16年7月12日）
- 動画撮影（最高裁平成20年4月15日）
- Nシステム（東京高裁平成21年1月29日）
- DNA情報の収集（最高裁平成20年4月15日、東京高裁平成28年8月23日）

* 犯罪捜査規範（国家公安委員会通達）

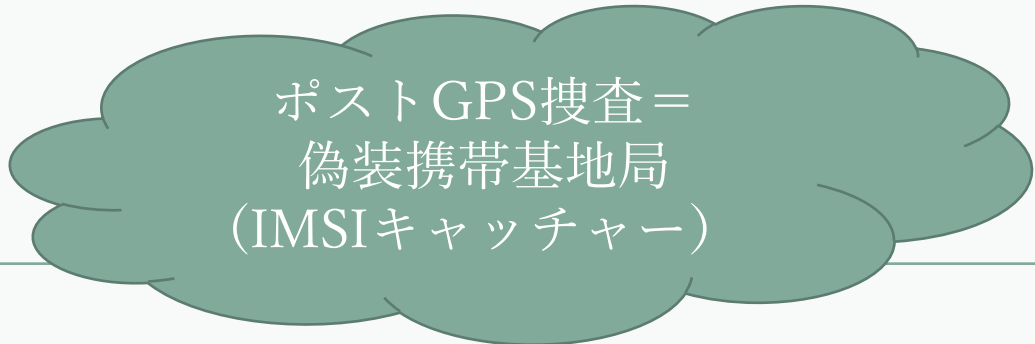
第101条 捜査を行うに当つては、聞込、尾行、密行、張込等により、できる限り多くの捜査資料を入手するように努めなければならない。

レイヤー2（任意処分）をめぐる問題状況

- 各種データ（音声、映像、位置、行動履歴）収集は広範囲に任意捜査（令状による事前規制なし）によって収集されてきた
- 保秘により明らかにされない手法も存在する（＝規制の必要性すら認識されず）
- 最高裁も長年、任意捜査としての3要件（必要性、緊急性、相当性）に当てはめて適法判断を続けてきた（＝事前規制なし）
- 学説も公道上を舞台としたデータ収集について任意処分説に立ち実態について検討を深めていない（＝事前規制の必要性すら認めず）

< 海外参考事例 2 >

スティングレイをめぐる米国の動き



ポストGPS捜査＝
偽装携帯基地局
(IMSIキャッチャー)

“スティングレイ”とは？

：偽装携帯基地局(Cell Cite 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
- もともとは軍・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「スティングレイ」（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

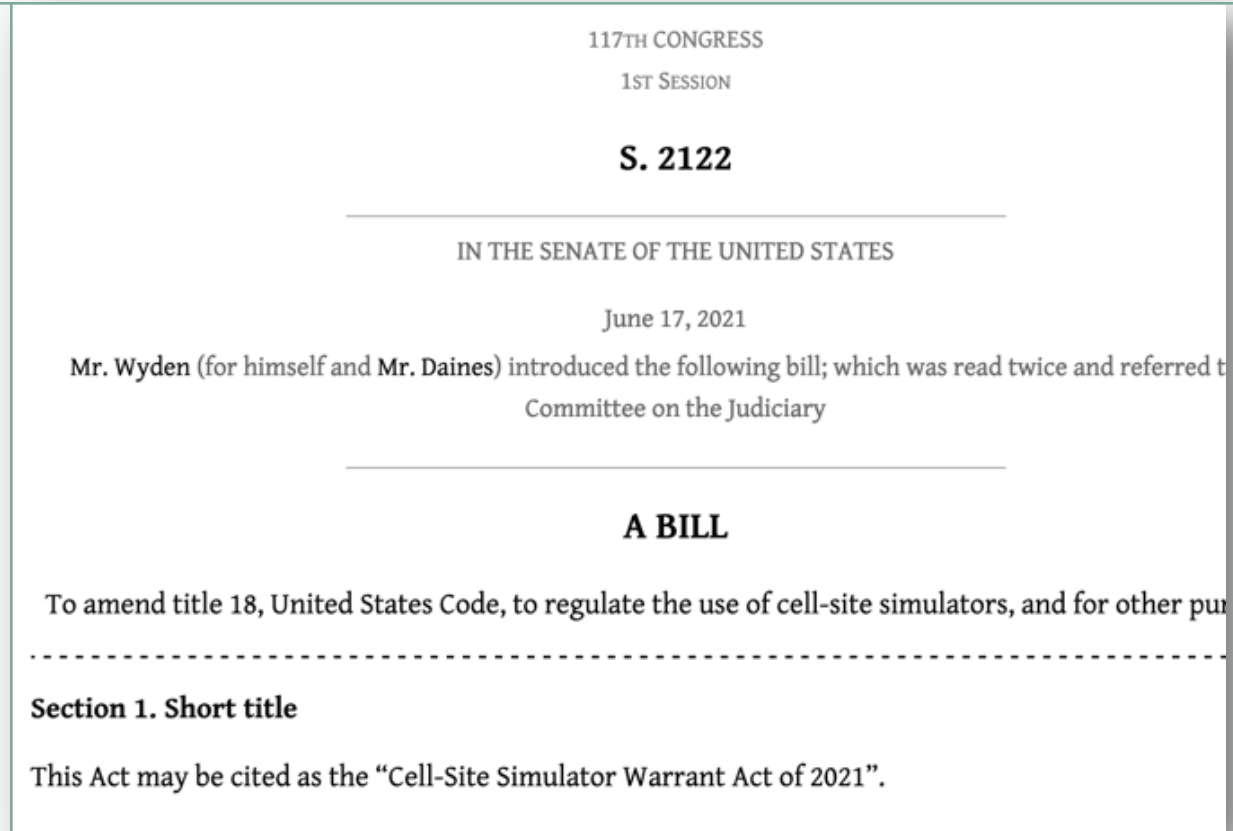
* International Mobile Subscriber Identity の略



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「スティングレイ」」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
 - 7/2 ✓ 開示要請のある場合



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

レイヤー2に関する小括

1. 任意処分説は、「データ駆動型捜査手法」の本質・特性を捉えていない
2. 強制処分説も、データ取得後規制に無関心で事前規制万能説
3. 立法必要説でも、データ取得後規制に十分な留意がされていない

レイヤー2の限界事例：その1

長期撮影をめぐる

- 長期撮影がなぜ問題か？

1. 目的や手法が多岐にわたる法執行機関の撮影行為を任意処分で正当化するが、要件や正当化理由が混乱（次&次々スクリーン参照）
2. 警察には大量の撮影機材が集積されていて、外部から全く規制なく実施されていること（2019年法とコンピュータ学会シンポジウム参照。『法とコンピュータ』誌39号収録。近刊）
3. 事前規制の社会的便益損失論者の中には、尾行とGPS捜査を比較して後者に「深刻な実害が生じる」ことを指摘するが、尾行と同じ捜査手法とされている内偵・張り込みにおいて撮影を伴った場合の「害悪」の深刻さが検討されていない

長期間撮影に関するわが国の裁判例

- 網羅的（無差別）撮影方式
 - ✓ Nシステム適法判決（民事裁判）
- 定点的撮影方式
 - ✓ あいりん地区撮影訴訟（民事裁判）
- 対象者長期撮影・・・ターゲット特定方式but犯罪実行後の証拠収集
 - ✓ 最二決平成20年4月15日 映像同一性識別目的（刑事裁判）
- 対象者長期撮影・・・ターゲット特定方式 but 犯罪実行前監視
 - ✓ 国公法違反事件（監視長期撮影、本人の刑事裁判で弁護側証拠）
 - ✓ さいたま地裁（監視長期撮影、第三者の刑事裁判で検察側証拠）

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S 4 4. 1 2. 2 4)
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S 6 1. 2. 1 4)
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S 6 3. 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H 6. 4. 2 7)
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H 1 8. 6. 2 9)
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H 2 0. 4. 1 5)

* 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）

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**公道上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

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、バッグ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、通常のパフォーマンスのビデオカメラで撮影したものに過ぎず、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

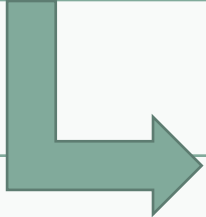
公道上での撮影
がプライバシー
の期待を減殺

さいたま地判平成30年5月10日 ・・・任意捜査として「違法」判断

玄関内部も撮影

公道上のみの場合と比較

- 本件撮影範囲は、主に公道上及び玄関ドア付近の外部から観察し得る場所ではあったが、不特定の者が行き来することが想定されない特定の敷地内に設置されたビデオカメラから撮影されたものであった上、被告人方の玄関ドアを開けた際にはその内部が映り込むなどしており、玄関内部の映像が不鮮明で人の様子等が明確には認識できなかったとはいえ、単純に公道上等のみを撮影した場合に比べるとプライバシー侵害の度合いが高かったものと認められる。また、個人宅の出入りが約7か月半（本件各証拠の内容である映像が撮影された時点までの期間と考えても約5か月間）という長期間にわたり、ほとんど常時撮影されていたものであって、撮影によって取得された情報が集積されるにつれて、生活状況等を把握される度合いも当然に高くなっていったものといえ、この期間の長さにも照らしても、本件撮影によるプライバシー侵害の度合いは他の事案と比べて高かった

- 
- 1) 任意捜査の適法性として判断
 - 2) 相当性基準＝プライバシー侵害の度合い
・・・撮影範囲、撮影期間、撮影方法、被侵害法益等から判断

7ヶ月半の
長期撮影

<海外参考事例 3>

米国における長期撮影の規律に関する論争

長期監視撮影をめぐる規律方法

立法による規制

- 連邦捜査規則 4 1 条
 - United States v. Falls, 34 F. 3d 674, 1994 U.S. App. LEXIS 24528(8th Cir. 1994) 修正 4 条（の要請）を満たし、かかる監視が規則 4 1 条によって許容され、かつ、その要件に合致する場合に地裁は令状を発付できる

事前規制（令状）
方式
による規制

判例による規制

- 否定論（修正 4 条侵害なし）
 - United States v. Houston, 813 F.3d 282, 288–90 (6th Cir.2016) 10 週間にわたる監視撮影は修正 4 条違反ではない
- 肯定論（修正 4 条侵害あり）
 - United States v. Vargas, No. CR-13-6025-EFS, at 20(E.D. Wash. Dec. 15, 2014) 6 週間にわたる私邸の庭のビデオ撮影監視は、プレインビューと同視できず修正 4 条違反に当たる

レイヤー 2 の限界事例

： その 2 顔認識・AI利用の問題

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？

YAHOO! ニュース IDでもっと便利に新規取得
ログイン 7/25（日）は「ふるさと納税」で+5%

検索バー: [検索] | Q

トップ 速報 ライブ 個人 オリジナル みんなの意見 ランキング 有

主要 国内 国際 経済 エンタメ スポーツ IT 科学 ライフ 地域

捜査に顔認証、全国の警察で 3月から運用開始

2020/9/13(日) 6:00 配信 12  





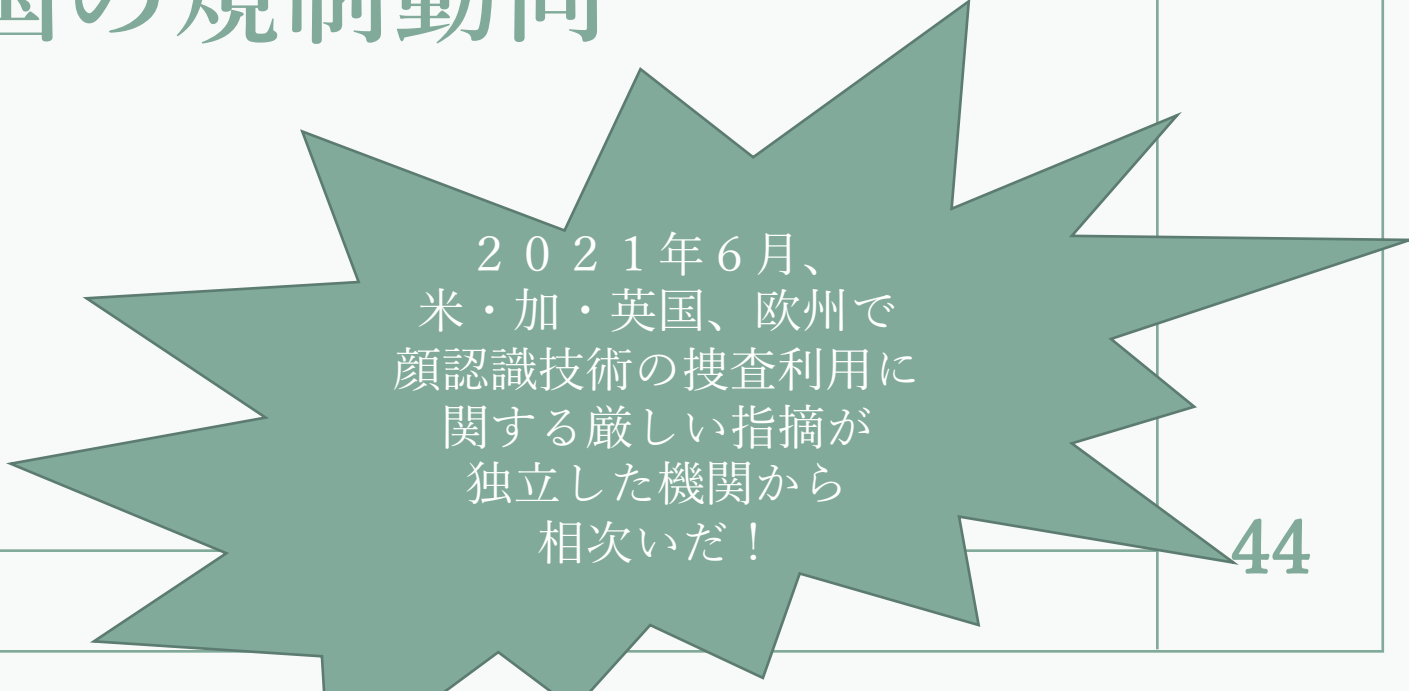
警察庁が入る中央合同庁舎2号館=千代田区霞が関

全国の警察が今年3月から、犯行現場などの防犯カメラや、事件に関連する会員制交流サイト（SNS）などの顔画像を、過去に逮捕した容疑者の顔写真データベースと照合する「顔認証システム」の運用を始めたことが12日、警察庁への取材で分かった。

顔の特徴が類似している人物の氏名や犯歴といった情報が即座に判明し、既に捜査に活用されている。一方、プライバシーの侵害につながる懸念があり、運用実態の公開などを求める声も出そうだ。

< 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！

June 2021

FACIAL
RECOGNITION
TECHNOLOGYFederal 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

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べき

7/22/21

The screenshot shows the official website of the Office of the Privacy Commissioner of Canada. The header includes the organization's name in English and French, along with a search bar. The main navigation menu lists various sections: For individuals, For businesses, For federal institutions, Report a concern, OPC actions and decisions, and About the OPC. The breadcrumb trail indicates the current page is 'Home > OPC News > News and announcements'. The headline of the news release is 'RCMP's use of Clearview AI's facial recognition technology violated Privacy Act, investigation concludes'. Below the headline, there is a sub-headline: 'Canadian privacy regulators release draft guidance on police use of FRT; launch consultation with stakeholders in bid to establish clearer rules, potentially new laws'. A note mentions a teleconference for journalists. The main body of the text, dated June 10, 2021, from Gatineau, QC, states that the RCMP's use of facial recognition technology (FRT) to search a database compiled illegally by a commercial enterprise is a violation of the Privacy Act. It also mentions a Special Report to Parliament and a public consultation to establish clearer rules and consider new laws. The text concludes by stating that Clearview AI 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.

英国

- 2020年8月、控訴院は個人の同意なく顔情報を収集するライブ顔認識技術利用が欧州人権規約第8条に違反するとの判決*
- 2020年12月、監視カメラ検査官からライブ顔認識技術利用に関するガイダンス発行
- 2021年6月、データ保護規制局は公共空間でのライブ顔認識技術使用について、規制当局は使用の合法的な目的を確立し、法的根拠を明らかにし、手続条件を把握し、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しなければならない。





EUROPEAN COMMISSION

Brussels, 21.4.2021
COM(2021) 206 final
2021/0106(COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS

{SEC(2021) 167 final} - {SWD(2021) 84 final} - {SWD(2021) 85 final}

EXPLANATORY MEMORANDUM

欧州

- 2021年4月、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方針を示す（左）
- 2021年6月、EDPB（欧州データ保護会議）とEDPS（欧州データ保護監察機関）が合同で議会の方針を歓迎し、AIを利用した顔認識技術による個人情報の収集を中止するよう勧告

米・加・英・欧州からの示唆

- 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・メカニズムが存在している
- 利用されている個々の（顔認識）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る
- 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がされている
- ただし、事前規制が必要とされているわけではなく、むしろ米国では事後規制が提唱されている
- 日本では、誰が公共空間での顔認識（生体認証）技術利用について－特に法執行機関の利用について－評価・監督するのか？

レイヤー 1 / レイヤー 2 のまとめ

英国は街頭監視撮影について事前・事後規制あり

英米加欧州では、顔認識技術の利用について2021年
に入って規制方向が明示された

各国で捜査機関による個人情報収集について「令状取
得」（事前規制）が進む

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

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、外部評価もない

学説（任意処分説）は、任意・強制の区別に指針を示し
ても具体的規制方法の考え方を提示せず

レイヤー 3

3、最上位層（強制捜査）での 情報収集

GPS位置情報取得捜査

I. 当初、任意捜査としてGPS捜査を開始

- 2004年、愛媛県警の内部文書がインターネットに流出。GPS発信装置を用いた行動確認を実施していることが明らかに
- 2006年、警察庁、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発出
- 2013年、福岡県警によるGPS捜査発覚
- 2014年、大阪府警のGPS捜査発覚。その後各地の刑事裁判で争われる
- 2015年6月、大阪地裁による初めての強制処分説、違法判断
- 2016年3月、大阪高裁、任意処分説、適法判断
- 2017年3月、最高裁大法廷、憲法35条侵害を認め、強制処分＝立法必要説へ

任意処分説を支持した学説例

- G P S 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可能性を孕むが、「G P S 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。
- 「G P S 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G P Sを用いた追跡捜査」 WLJ判例コラム 73号(2016))

任意処分説を支持した学説例

いったいどんな
ものですか？

- G P S 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可能性を孕むが、「G P S 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。
- 「G P S 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G P Sを用いた追跡捜査」 WLJ判例コラム 73号(2016))

任意処分説を支持した学説例

どんな目的で、
どのように管理
しているのです
か？

- G P S 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、「G P S 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。
- 「G P S 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G P Sを用いた追跡捜査」 WLJ判例コラム 73号(2016))

任意処分説を支持した学説例

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？

- G P S 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、**「G P S 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。**
- 「G P S 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G P Sを用いた追跡捜査」 WLJ判例コラム 73号(2016))

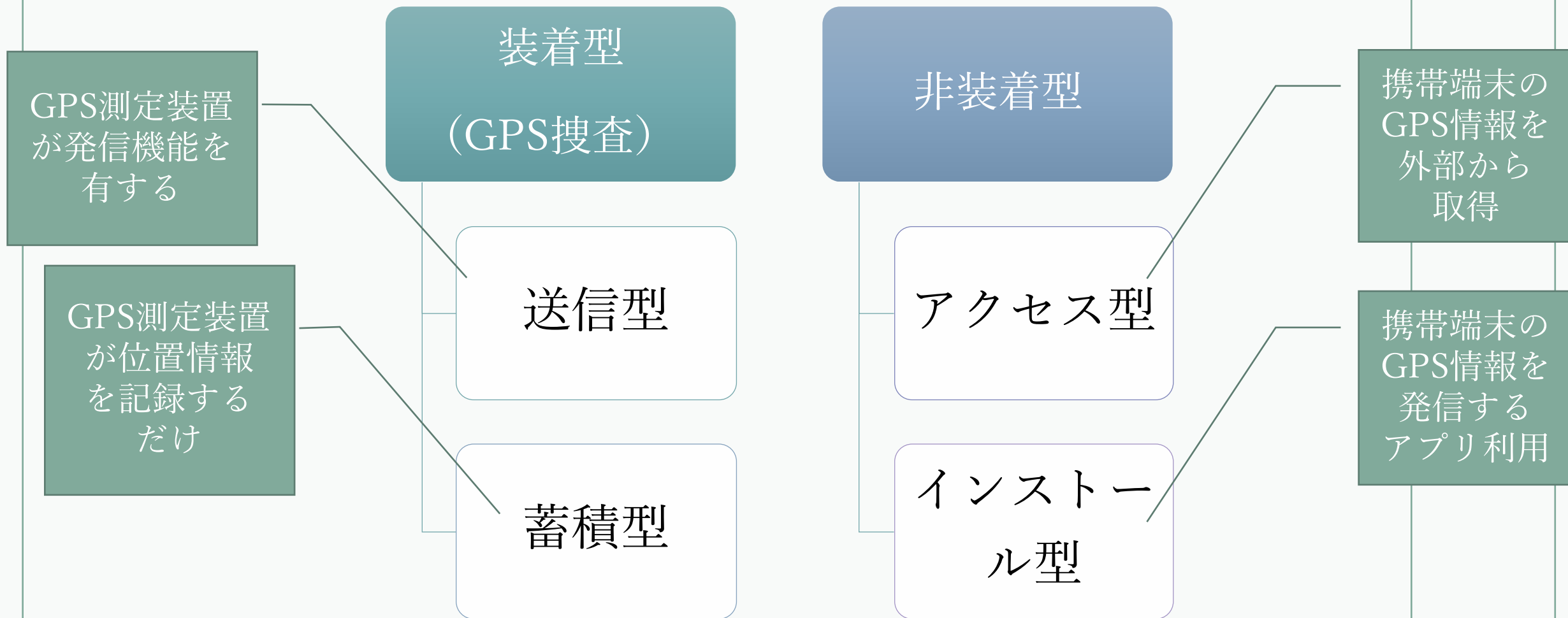
任意処分説を支持した学説例

- G P S 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孕むが、「G P S 的なツール」にもその機能において種々なもの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。大き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、許される場合を認めざるを得ない。
- 「G P S 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。

大法廷は
立法に委ねると
しました。
令状でGPSの利用方法
まで規律できないと
しました

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

GPS位置情報取得方法の分類



出典：指宿信編著『GPS捜査とプライバシー保護』（現代人文社、2018）
から抜粋

装着型（送信型）・・・発信装置装着

- GPS発信装置装着に対象者の承諾なし
- 非代替性要件（運用要領*）
- 警察本部捜査主管課長の承認（運用要領*）
- 一週間に一回以上の進捗状況報告（運用要領*）
- 装着は車両下部ないし内部で位置情報発信の認識困難
- 移動時に身体と同一化
- 公道が中心。だが、私有地や道路上以外にも駐停車する。
- バッテリー交換のためアクセスの必要

* 移動追跡装置運用要領（平成18年6月30日）
警察庁刑事局企画課長発出（次スクリーン参照）



装着型に関する 警察庁2006年通知

取	扱	注	意
原議保存期間5年 (平成23年12月31日まで)			
警察庁丁刑企発第184号 平成18年6月30日 警察庁刑事局刑事企画課長			

移動追跡装置運用要領の制定について

見出しの要領を別添のとおり定めたので、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されたい。

なお、移動追跡装置を用いた捜査を実施することの適否については、本要領を踏まえつつ、個別具体の事案に即して十分な組織的検討を経た上で厳格に判断されるべきものであり、疑義がある場合には警察庁の当該事件捜査主管課に協議することとされたい。

要領における保秘要請

5 保秘の徹底

移動追跡装置を使用した捜査の具体的な実施状況等については、文書管理等を含め保秘を徹底するものとし、特に次の事項に留意する。

- ・
- ・
- ・

* 令状請求に用い”ない”
* 報道発表でも触れ”ない”
* 検察官にも送致し”ない”

2019年3月29日旭川地裁判決「本件要領が保秘の徹底を求めている点は、GPS捜査に対する司法審査を困難にする運用を招来しており、それ自体、令状主義の精神に反するきらいがある」

データ駆動型捜査手法には、このような徹底した情報コントロール化を図る傾向が顕著に見られる

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

イ

- (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

- * 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」

< 海外参考事例 5 >

諸外国の位置情報捜査規制の 枠組み

(US, UK, 独, 仏, 豪)

* 2017年段階の状況

出典：指宿信編著『GPS捜査とプライバシー保護』（現代人文社、2018）
から抜粋

	米国（メイン州）	イギリス	ドイツ	フランス	豪州(NSW州)
事前・事後の規制	事前（令状審査） 事後（本人告知）	事前（警視以上の許可）	事前（長期の場合、令状審査）事後（本人告知）	事前（令状審査）	事前（令状審査） 事後（オンブズマン査察）
対象犯罪・保護利益等	制限なし	国家安全保障、犯罪抑止、国家経済利益、安全、公衆衛生、脱税等	重大な犯罪	生命・身体犯については3年以上の罪、それ以外は5年以上の罪	制限なし
実施要件	相当の理由	必要性、相当性	犯罪の重大性、補充性	必要性	犯罪の蓋然性、必要性、相当の理由
実施期間	10日間	3ヶ月（通常・書面申請） 72時間（緊急・口頭申請）	短期監視（最大2日） 長期監視（3月）	検察官許可（15日間） 裁判官許可（1ヶ月） 特殊事案で4ヶ月	90日以内
被処分者へ告知	3日以内（90日以内の延長可）	—	あり	—	—
異議申し立て	—	審判所(Tribunal)による審査	—	あり	—
記録媒体の保存	—	終了後3年間保存	あり	あり	あり
記録媒体の破棄廃棄	—	あり	あり	あり	あり
記録保管状況に対する査察	—	あり	—	—	あり
捜査実施報告義務	あり（裁判所。裁判所は議会に）	あり	—	あり	あり
記録の秘匿化	—	あり	—	あり	あり
情報流用	—	—	他事件利用可	—	禁止

--	--

事後規制の例

：通信傍受法における記録消去要請、不服申立てとデータ消去命令

- 29条（傍受記録の作成）：3 第一項に規定する記録は、第二十四条第一項後段若しくは第二十六条第二項の規定により記録をした記録媒体又は第二十五条第三項の規定により作成した同条第一項の記録媒体の複製から、次に掲げる通信以外の通信の記録を消去して作成するものとする。
- 33条（不服申立て）：3 裁判所は、前項の請求により傍受又は再生の処分を取り消す場合において、次の各号のいずれかに該当すると認めるときは、検察官又は司法警察員に対し、その保管する傍受記録（前条第六項の規定により傍受記録とみなされたものを除く。以下この項において同じ。）及びその複製等のうち当該傍受又は再生の処分に係る通信及びこれと同一の通話の機会に行われた通信の記録並びに当該傍受の処分に係る一時的保存をされた暗号化信号の消去を命じなければならない。

GPS捜査最高裁大法廷判決との比較

- GPS捜査の位置付け＝「合理的に推認される個人の意思に反してその私的領域に侵入する捜査手法」「個人の意思を制圧して憲法の保障する重要な法的利益を侵害するもの」「刑訴法上、特別の根拠規定がなければ許容されない強制の処分に当たる」「令状がなければ行うことのできない処分」
- 適正手続の担保手段＝「第三者の立会い，事後の通知等様々なものが考えられる」「捜査の実効性にも配慮しつつどのような手段を選択するかは，刑訴法197条1項ただし書の趣旨に照らし，第一次的には立法府に委ねられている」

2017年3月15日最高裁大法廷判決

- GPS捜査の位置付け＝「合理的に推認される個人の意思に反してその私的領域に侵入する捜査手法」「個人の意思を制圧して憲法の保障する重要な法的利益を侵害するもの」「刑訴法上、特別の根拠規定がなければ許容されない強制の処分に当たる」「**令状がなければ行うことのできない処分**」
- 適正手続の担保手段＝「第三者の立会い，事後の通知等様々なものが考えられる」「捜査の実効性にも配慮しつつどのような手段を選択するかは，刑訴法197条1項ただし書の趣旨に照らし，第一次的には立法府に委ねられている」

事前規制（令状
必要説）を
採用したけれど
も。。

2017年3月15日最高裁大法廷判決

- GPS捜査の位置付け＝「合理的に推認される個人の意思に反しての私的領域に侵入する捜査手法」「個人の意思を制圧して憲法保障する重要な法的利益を侵害するもの」「刑訴法上、特別の根拠がなければ許容されない強制の処分に当たる」「令状がなければ行うことのできない処分」
- 適正手続の担保手段＝「**第三者の立会い，事後の通知等様々なものが考えられる**」「捜査の実効性にも配慮しつつどのような手段を選択するかは，刑訴法197条1項ただし書の趣旨に照らし，第一次的には立法府に委ねられている」

事後規制についても言及あり！
通信傍受法を参考にしている。
だが、情報保管や保護には言及なし

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令状を受け、捜査令状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

レイヤー3のまとめ

- 事前規制方式（令状主義）の限界がGPS捜査によって明らかになってきた
- 事後規制方式（記録消去・事後通告・不服申立て等）が導入されているのは通信傍受法のみ
- わが国では、様々な監視・情報収集手法（データ駆動型捜査の端緒、次スクリーン参照）のうち、強制処分として法令で位置付けられているものが非常に少ない

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、監查查察）の導入が必要

事後規制

告知・通知

不服申立て

監查查察

前提：
日本における
データ駆動型捜査の規律状況まとめ

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	生体情報取得監視	
	街頭監視カメラ		

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

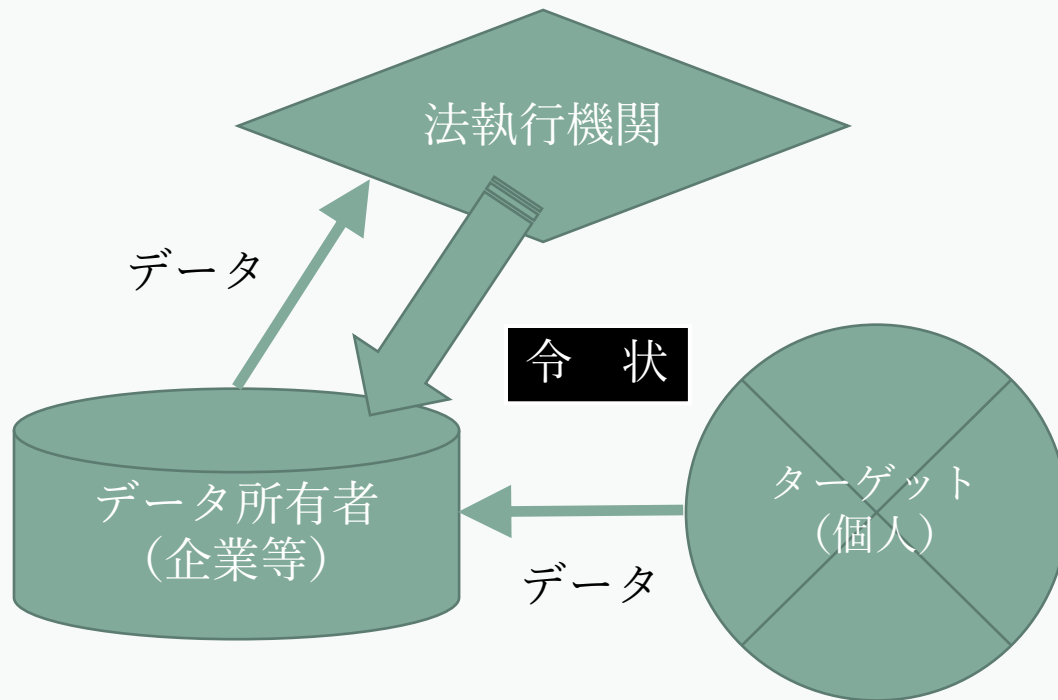
国連麻薬及び犯罪対策局「重大・組織犯罪捜査における電子監視に関する現在の実務」（2009）による監視手法の分類

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	生体情報取得監視	
	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

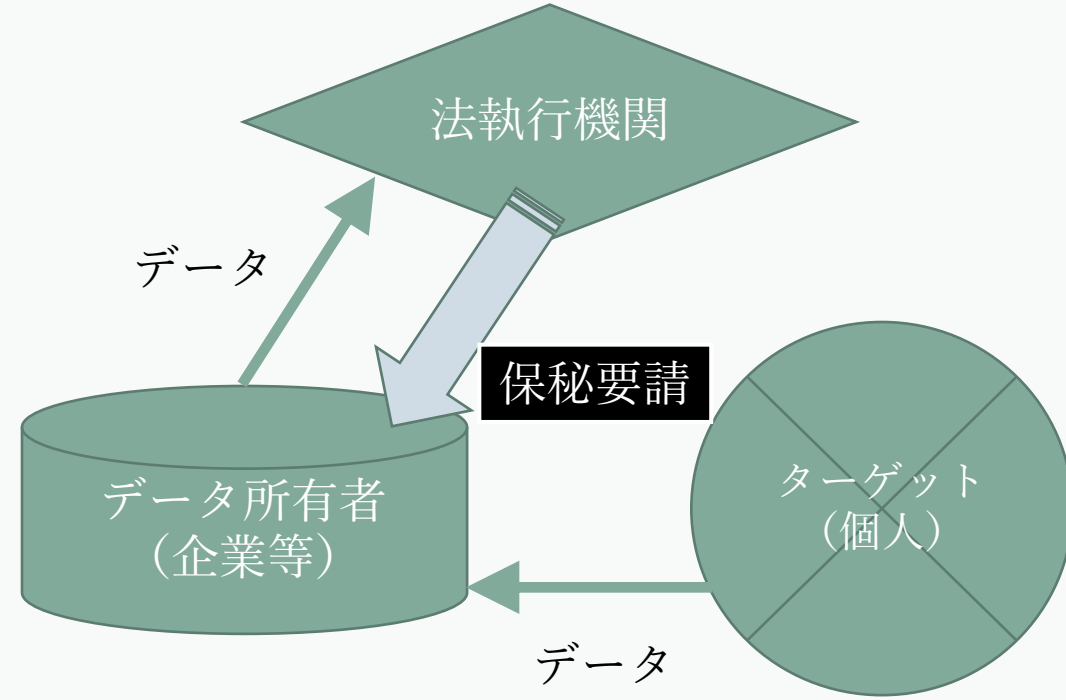
出典： United Nations Office on Drugs and Crime (UNDOC)
Current practices in electronic surveillance in the investigation of serious and organized crime2009

令状がある場合とない場合のデータの流れ

令状がある場合（強制処分）

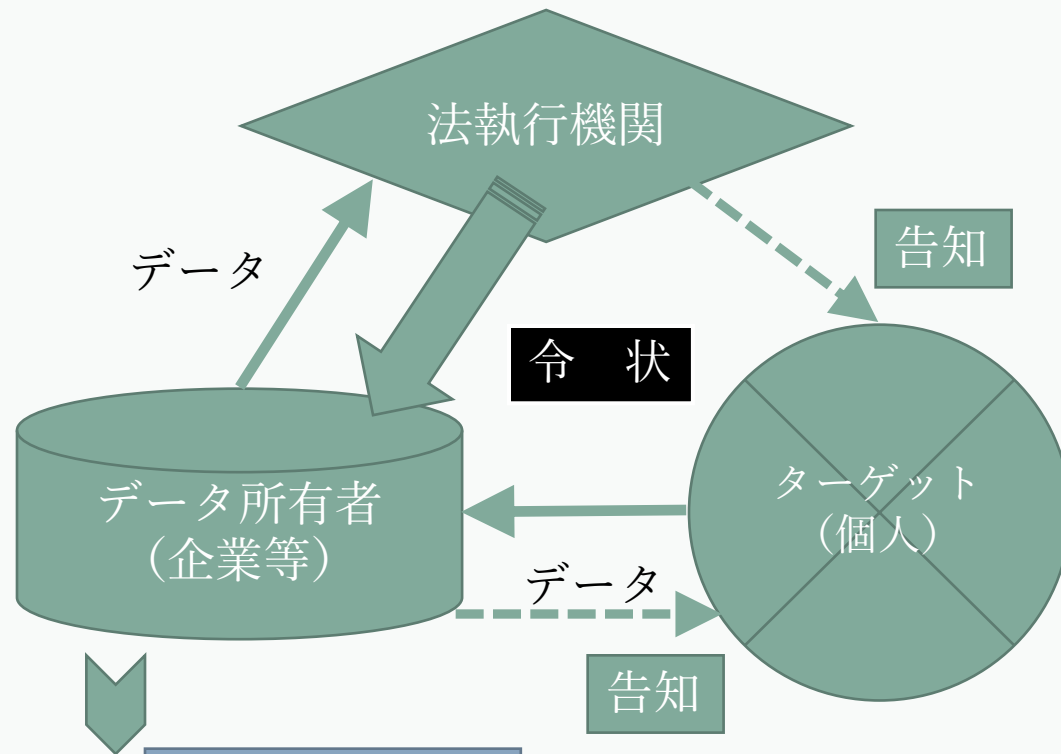


令状がない場合（任意処分）

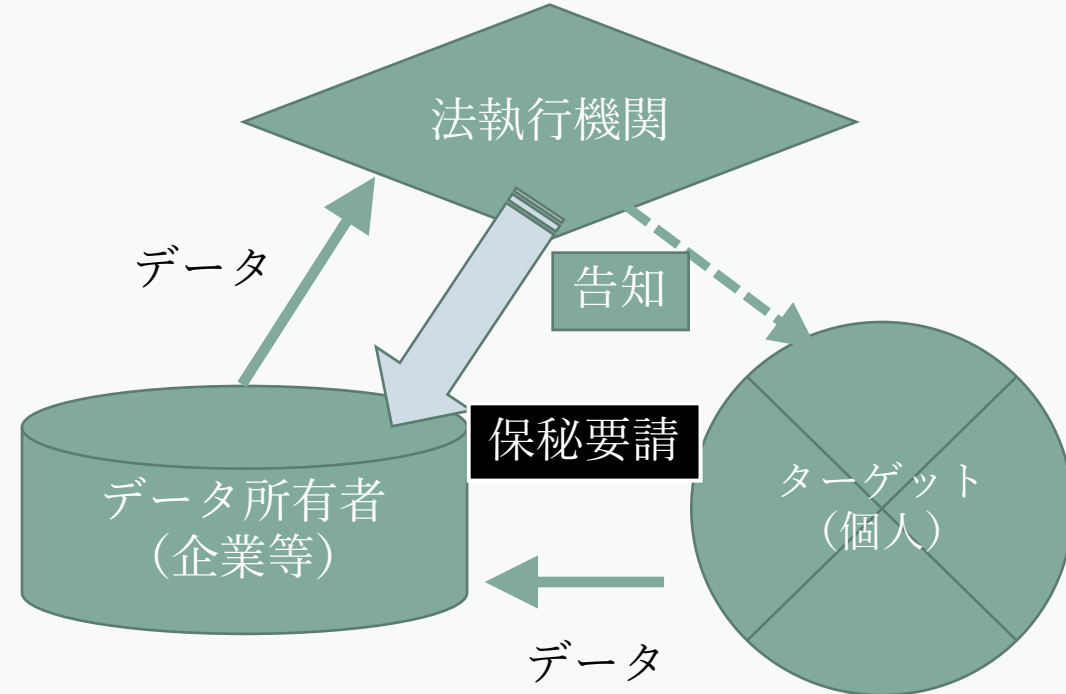


告知・通知があればターゲット（個人）は知りうる

令状がある場合（強制処分）

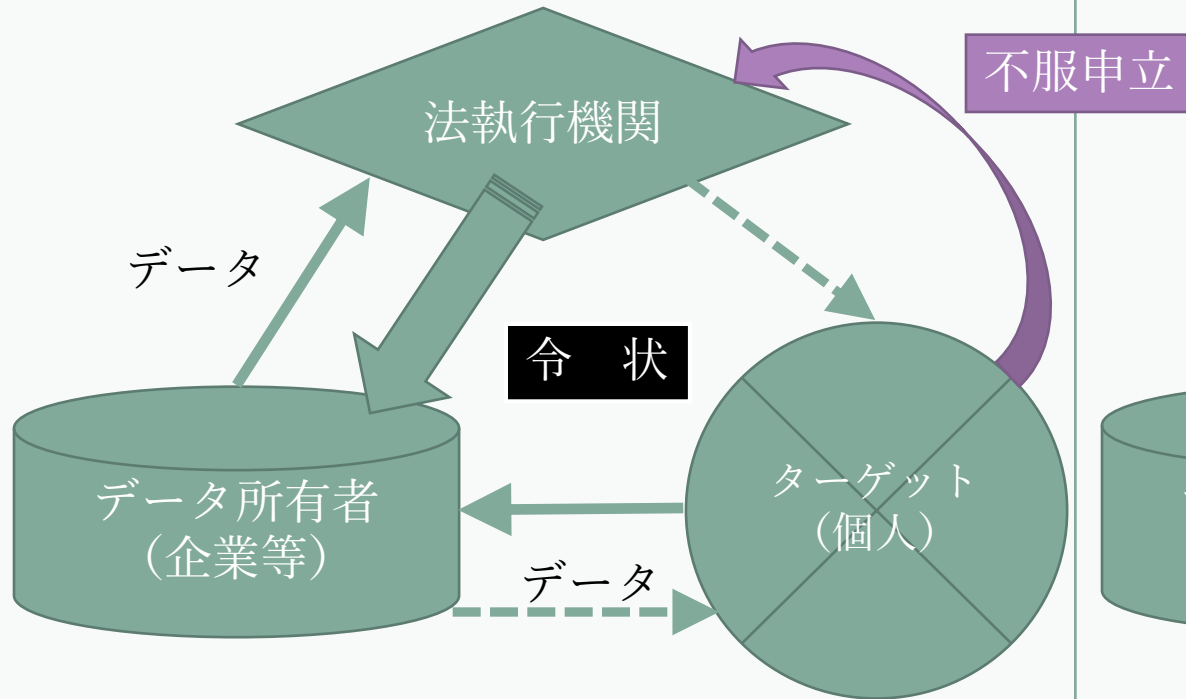


令状がない場合（任意処分）

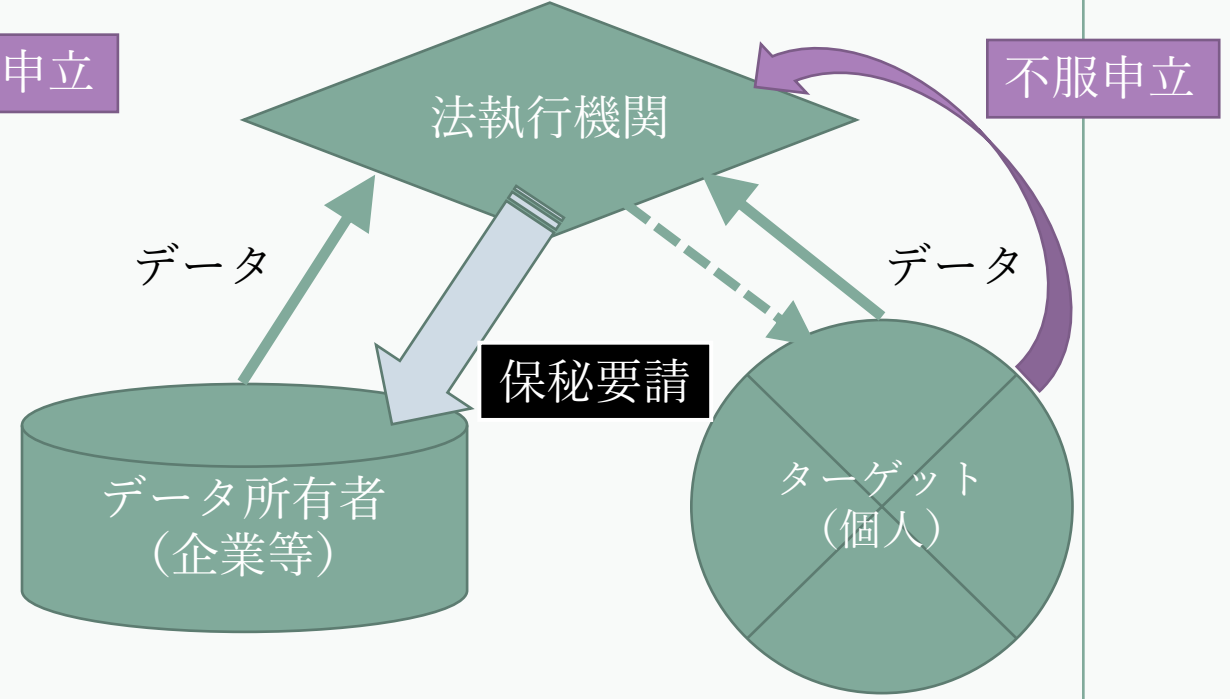


不服申し立てがあればターゲット（個人）は争いうる

令状がある場合（強制処分）



令状がない場合（任意処分）



現行法の例：
搜索差押や勾留については準抗告手続
通信傍受については不服申立て手続

日本のデータ駆動型捜査における 事前・事後規制の状況

捜査の性質	強制処分			任意処分		
捜査手法	通信傍受	インターネット利用履歴	基地局情報	捜査関係事項照会	位置情報取得【違憲判断】	【参考】DNAデータ取得
事前規制	あり（令状）	あり（令状）	あり（令状）	なし	なし	なし
事後規制						
監督機関	なし	なし	なし	なし	なし	なし
事後通知	あり	？	？	なし	なし	なし
不服申立	あり	なし	なし	なし	なし	なし
監査査察	なし	なし	なし	なし	なし	なし
実施報告	あり	なし	なし	なし (透明性レポートのみ)	なし	なし

< 付録 > GDPR2019年十分性認定 は果たして「十分」か？

19.3.2019

EN

Official Journal of the European Union

L 76/1

COMMISSION IMPLEMENTING DECISION (EU) 2019/419

of 23 January 2019

pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information

(notified under document C(2019) 304)

(Text with EEA relevance)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) ⁽¹⁾ ('GDPR'), and in particular Article 45(3) thereof,

After consulting the European Data Protection Supervisor,

1. INTRODUCTION

Opinion of the Board (Art. 70.1.s)



Opinion 28/2018

**regarding the European Commission Draft Implementing
Decision**

on the adequate protection of personal data in Japan

Adopted on 5 December 2018

- 2018年10月、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・保護について十分性認定に関わる疑念が公式に提示される
- 個人情報保護法が警察が収集した個人情報を対象外にしていることへの懸念
- 捜査関係事項照会による個人情報収集プロセスの不透明性を指摘

2019年1月、十分性認定へ



- COMMISSION IMPLEMENTING DECISION (EU) 2019/419 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information
- URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.076.01.0001.01.ENG&toc=OJ:L:2019:076:TOC

裁判所の十分な事前審査がある

(132)

- First, in all cases where electronic information is obtained by means (search and seizure), the police has to obtain a warrant (see recital 121). Therefore, the collection in those cases will be checked ex ante by a judge, based on a strict "adequate cause" standard.

搜索差押での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、事前審査される。

理由：

GPS捜査大法廷判決が、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確に指摘している

国政調査権によって監督を受けている

(134)

- Second, according to Article 62 of the Constitution, each House of the Diet may conduct investigations in relation to the government, and may compel witnesses, and/or the production of records. Those powers are further detailed in the Diet Law, in particular Chapter XII. In particular, Article 104 of the Diet Law states that "public agencies and other parts of the government" must comply with a House or any of its Committees for the production of reports and records necessary for consideration of investigation." Refusal to comply is allowed only if the government provides a plausible reason found acceptable by the Diet, or upon issuance of a formal declaration that the production of the reports or records would be "gravely detrimental to the national interest" (106). In addition, Diet members may ask written questions to the Cabinet (Articles 74, 75 of the Diet Law), and in the past such "written inquiries" have also addressed the handling of personal information by the administration (107). **The Diet's role in**

国政調査権の発動、
通信傍受実績に関する
国会報告がある、と。
個々の強制捜査で収集され
た個人情報管理の
を独立して監督する
権限はどこに？

7 / 22 / 2021 **supervising the executive is supported by reporting obligations, for instance pursuant to Article 29 of the Wiretapping Act.**

警察は「独立した審査を受けている」

(135)

- Third, also within **the executive branch the Prefectural Police is subject to independent review**, which 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 (at least half of them must be citizens with no public servant position in the police in the five preceding years) and have a security of tenure (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 a direction or /herself becomes aware of a possible case of misconduct (including the violation of police 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 properly handled.

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！

総務省が監督している

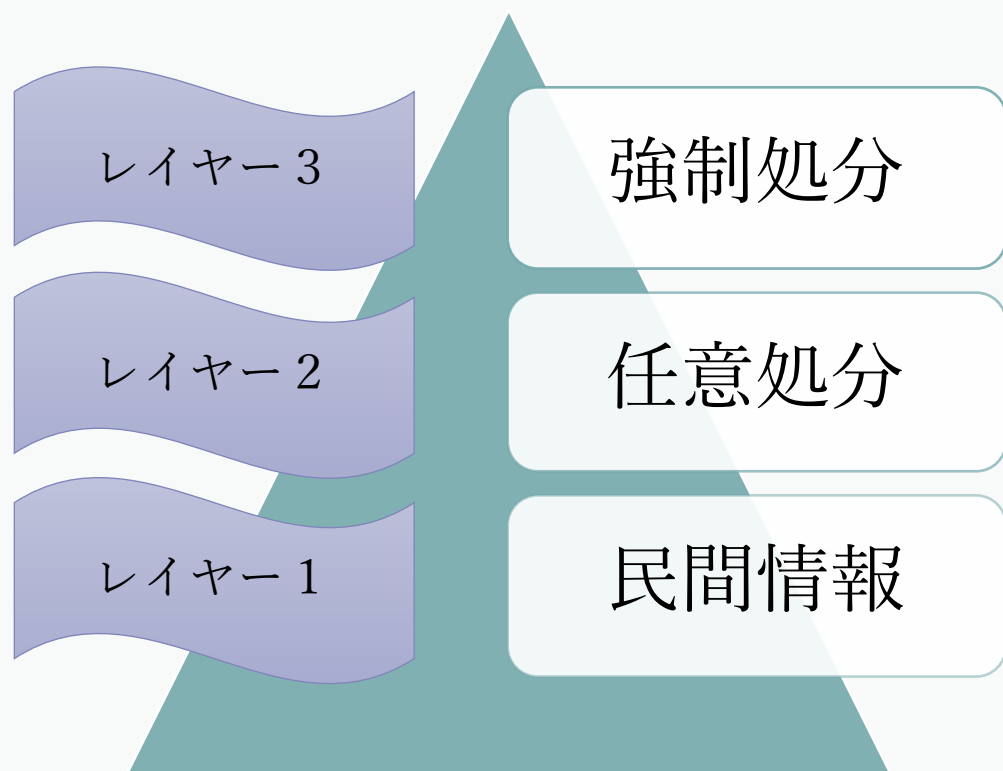
(136)

総務省が行政機関の
個人情報取り扱いに関す
る責任を負っていて、説明
を求め、意見を付すことが
できる

- In addition, with respect to the correct application of the APPIHAO, the **minister or agency head (e.g. the Commissioner General of the NPA) has enforcement authority, subject to the supervision by the Ministry of Internal Affairs and Communications (MIC)**. According to Article 49 APPIHAO, the MIC "may collect reports on the status of enforcement of this Act" from the heads of Administrative Organs (Minister). That oversight function is supported by input from MIC's 51 "comprehensive information centres" (one in each Prefecture throughout Japan) that each year handle thousands of inquiries from individuals (114) (which, in turn, may reveal possible violations of the law). Where it considers this necessary for ensuring compliance with the Act, **MIC may request the submission of explanations and materials, and issue opinions, concerning the handling of personal information by the concerned Administrative Organ (Articles 50, 51 APPIHAO).**

まとめ

レイヤー毎の規制方向のあり方



- レイヤー1・レイヤー2のターゲット特定型監視・情報収集には事前規制（令状等）方式を導入すべき
- レイヤー2の網羅的情報収集には、第三者機関による事後規制（監査・査察等）方式を導入すべき
- レイヤー3の強制処分によって収集されたデータの保管・アクセス状況について第三者機関による事後規制（監査・査察等）方式を導入すべき

- 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せず、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「充分性認定」につき、わが国では事前・事後の規制、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する立法府・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

関連研究業績：その1

拙編著『GPS捜査とプライバシー保護：位置情報取得捜査に対する規制を考える』（現代人文社、2018）p. 2-12

「ハイテク機器を利用した追尾監視型捜査：ビデオ監視とGPSモニタリングを例に」『鈴木茂嗣先生古稀祝賀論文集（下巻）』（成文堂、2007）p. 165-186

「GPS利用捜査とその法的性質：承諾のない位置情報取得と監視型捜査をめぐって」法律時報87巻10号 p.58-64（2015）

「アメリカにおけるGPS利用捜査と事前規制」季刊刑事弁護85号p.89-95（2016）

「追尾監視型捜査の法的性質：GPS利用捜査をめぐる考察を通して」刑事弁護の原理と実践（美奈川成章先生・上田國廣先生古稀祝賀記念論文集）（現代人文社、2017）

「GPS捜査と個人のプライバシー——平成29年最高裁大法廷判決まで・その意味・その後」法とコンピュータ36号 p. 3-13（2020）

「GPS捜査事件最高裁大法廷判決を振り返る～法理論と法実務のクロスオーバー」成城大学法学部創立40周年記念論文集（2019、信山社）p.127-144

「判例解説「7ヶ月半に及ぶ撮影についてプライバシー侵害の度合いが強いとして証拠排除した事例」新・判例解説Watch刑事訴訟法 No.4（2019）



2018, 現代人文社

関連研究業績：その2

Preparation
for
publication

電腦空間
と
刑事手続

「これが国際通信盗聴網「エシュロン」だ！」法学セミナー 539号p.57-61 (1999)

「インターネット盗聴ソフト「カーニボー」の正体」法学セミナー 556号p.47-50 (2001)

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「スティングレイ」法学セミナー60巻11号p.1-4 (2015)

「Apple vs FBI問題を考える」法学セミナー 61巻7号 p.5-8 (2016)

「変わる捜査の対象：モノからデータへ（法律時評）：サイバー刑事法制の諮問を契機として」法律時報75巻7号p.1-3 (2003.6)

「越境するデータ、越境する捜索—域外データ取得をめぐる執行方式に関する欧米の立法動向」Law and Technology No.82 p.45~57 (2019)

「越境捜索を適法とした令和3年2月1日最高裁決定」Law and Technology No.91 p. 41~45 (2021)