

警察政策学会資料 第100号  
平成30（2018）年4月

# 警察におけるカメラ画像の活用と課題

警察政策学会  
管理運用研究部会

## まえがき

本資料は、平成30年3月19日にグランドアーク半蔵門において開催された、警察政策学会（管理運用研究部会）フォーラム「カメラ画像の活用と課題」における星周一郎（首都大学東京都市教養学部法学系教授）、木村伊量（国際医療福祉大学大学院特任教授・前朝日新聞社長）両氏と松尾庄一（管理運用研究部会幹事・元近畿管区警察局長）の報告とフロアとの質疑応答の結果をまとめたものである。

なお、当日の録音を起こした原稿を基に、後日、各報告者が若干の追加及び修正を行い、また、読者の便宜上、適宜、小見出しをつけたことを前もってお断りする。

平成30年4月

松尾庄一



## 目次

開会あいさつ<野田 健>.....	1
-------------------	---

### 基調報告

捜査におけるカメラ画像の活用と課題<星 周一郎>.....	3
-------------------------------	---

### 報告1

超監視社会をどう生きる——公益とプライバシーとのはざまで<木村伊量>.....	17
付録 当日配布のハンドアウト.....	27

### 報告2

ソフトターゲットテロ防止におけるカメラ画像の活用と課題<松尾庄一>.....	32
付録1 当日配布のレジュメ.....	38
付録2 「ネットワークカメラシステムに関する法的諸問題」(配布資料) .....	41



## 開会挨拶

野田 健 管理運用研究部会長

本日は、管理運用研究部会として「カメラ画像の活用と課題」と題するフォーラムを行うことにしましたが、開会に当たり、所感を述べたいと思います。

私が平成 11 年に警視総監になったころは、犯罪の凶悪化であるとか国際化、広域化というようなことが大きな課題でした。警視庁では、最近では 5 件とか 6 件というレベルですが、特別捜査本部事件が当時は 30 件ぐらいありました。特に、東京都内でも新宿の歌舞伎町あたりはひどく、毎年のように殺人事件の特別捜査本部が作られていました。

こういう状況でしたから当時の石原都知事と一緒に年末警戒の視察・督励で現場へ行き、町の住民のお話を聞かせていただきました。その中である人が「歌舞伎町の大変ひどい治安状態を是非よくしてもらいたい」というようなことを話されたことから、都知事が記者会見で「歌舞伎町は日本で一番治安が悪いところなんだ」という話をしました。ところが、その記事を読んだ人から「その犯罪をなくすのがあなたの仕事でしょう」という投書があったため、都知事から「警視総監、何とか考えてくれ。多少お金はかかってもいいから」と言われました。

そこで私は、「歌舞伎町というのはそんなに広くないから、50 カ所ぐらいにカメラをつけてそれを録画する。それに、指名手配された人物がうろうろしているという実態もあるから、できれば顔認証で、それを探し出すことができないか」と考えました。実施に当たっては、顔認証は当時のテクノロジーでは難しくて実現しませんでした。その他にも障害がいくつかありました。例えば、歌舞伎町から新宿警察署までは画像を即時に送るために通信会社の既存の回線を借りればいいと考えていたのですが、当時は、通信ケーブルが山手線の大ガードを越えていないから、追加で 3 億ぐらいの予算を特別につけてもらって始めました。

運用を開始するといろいろなことがありました。たとえば、あるとき暴力団風の男がタクシーの運転手を捕まえて警察署に来て、「歩いていたら、このタクシーの野郎が俺をはねたんだ」と言うんですね。それで、現場の録画画像を見ると、実はタクシーがぶつけたのではなくて暴力団風の男が蹴っ飛ばしている状況が見事に映っていて、それは違うだろうというので、申告してきた男を検挙したことがありました。また、あるとき暴力団同士で日本刀を持って大立ち回りがあったのですが、警察官が行ったときに、日本刀を持っているほうが何かやったのではないかと思うのですけれども、これも録画画像を見ると違っていたのです。実は、日本刀を持ち出したのは相手方で、斬りかかったところ真剣白羽取りをやられて奪われたことが分かりました。つまり、警察官が行ったときに日本刀を持っていたのは被害者で、相手側が日本刀を持ち出し、斬りかかってきたということでした。

これらは、カメラを設置して録画することの直接的な効果でしたが、毎年のように歌舞伎町では殺人の特別捜査本部が作られていたのに、カメラを設置して録画するようになったら発生しておきませんので、重要凶悪な事件を防止するにも非常に効果があったと思います。何か事が起きたときには、その状況がどこかのカメラに映っているということで、計画的な犯罪は避ける効果

があるのではないかと思います。

先ほども述べたように歌舞伎町のカメラシステムは顔認証機能はありませんが、最近、顔認証システムで怪しげな者を見つけ出すということが、いろいろなところでかなりできるようになりました。「見当たり捜査」といって、指名手配になっている者の写真をじっと睨んで頭に刻んで、繁華街を歩いている群衆の中から見つけて捕まえているお巡りさんもおりますから、カメラ 50 台で見て、それで機械的に「これは指名手配されている人間ではないか」というアラームが出てくれば非常にいいのではないかと。できれば歌舞伎町のシステムを更新するときに、そういう機能を持ったカメラシステムになってほしいと期待をしております。

ただし、カメラ画像の警察活動での活用はいろいろな問題もありますので、本日は、フォーラムということで皆さん方にもぜひ御理解をいただいて、問題点があれば問題点を解消するし、いいことについてはさらに使っていくというようなことができればいいのではないかと考えております。

## 捜査におけるカメラ画像の活用と課題

星 周一郎（首都大学東京都市教養学部法学系教授）

司会（松尾庄一） まず、首都大学東京都市教養学部法学系教授の星周一郎先生に、「捜査におけるカメラ画像の活用と課題」というテーマで、基調報告に続き講演をいただきたいと思います。

なお、先生は、警察学論集の第70巻（2017年）11月号に「防犯カメラ、ドライブレコーダー等による撮影の許容性と犯罪捜査、刑事司法における適法性の判断」ということで論文を掲載されております。これを読みまして、本日のフォーラムを企画した次第です。

### はじめに—本日の講演テーマについて

ただいまご紹介をいただきました、首都大学東京の星と申します。本日は、どうぞよろしくお願いたします。

私のほうからは、「捜査におけるカメラ画像の活用と課題」ということで、最初に簡単にカメラの設置状況についてお話をさせていただいた後、カメラ設置の法的な根拠はどこに求められるのか、について考えたいと思います。それから、近時の大きな変化なのですが、かつてのアナログの不鮮明な映像からデジタルの非常に鮮明な映像に変わってきたことにより、画像に個人情報該当性が認められるようになってきました。ここをどう考えるべきなのかについてお話ししたいと思います。あともう1つ、防犯カメラを設置・運用する場合に、プライバシーに対する影響が懸念される、ということがよく言われます。その場合の、プライバシーに対する影響というのは具体的に何であるのか、どこまでの利用が許容されるのか、そういったようなお話をさせていただきます。その後、捜査でのカメラ画像の利用、それから証拠としての利用、その他について簡単にお話をさせていただくという形にしたいと思っております。

### カメラの設置状況

まず警察によるカメラの設置状況を見てみましょう。先ほど野田会長のお話にもございましたが、警察がみずから設置しているカメラの数も非常にふえてきておりまして、2017年3月現在で、数にして1,715台、都道府県ですと28都道府県という形になっております。警察白書にこの統計数値が載るようになってから、台数ベースで10倍になっています。

ただ、もちろん、それを上回る民間設置の街頭カメラがあるわけです。それを数えるのは、既に困難なぐらい数がふえております。今から6年ほど前に日経新聞で、300万台以上あるのではないかという報道がされたことがありますけれども、この数値も何に基づいているのかは、記事を読む限りは、ちょっとよくわからないところがあります。

諸外国の例も若干見てみましょう。

イギリスは、かつて防犯カメラ先進国でして、2014年の数値ですけれども、590万台という数値が報じられたことがあります。ただ、これもその12年前の2002年には、425万台という推



計値が出ておりましたので、そこからいきますと、イギリスは既に、数から言えば飽和状態になっているのかもしれませんが。あとは映像の質といいますか、あるいは利用の仕方という問題に、議論のステージが移ってきていると言えるかもしれません。

アメリカも何台あるのか見当がつかないのですが、これも古い数値ですけども、ウォールストリートジャーナルが、2004年に2,900万台という数値を報じたことがありまして、3,000万台という数がしばしば言われる時代がありました。

それから、「意外」、というよりは、「やはり」、というふうに言ったほうがいいかもしれませんが、近年に急増しているのが中国です。2017年暮れに、イギリスBBCが、1億7000万台のカメラが中国の街頭にあり、さらに3年後には、4億台になるのではないかという報道をしております。ただ、これらは「街頭に設置されているカメラ」ということであって、必ずしも防犯を目的としたものには限りません。特に、中国は顔認証を決済手段に使うという形で街頭に置かれているカメラも非常にふえているようです。ですから、設置カメラを何の目的で使うのかということが、今後問題になってくるということもあると思います。

以上が、街頭カメラの設置状況です。

## カメラ設置の法的根拠

次に2番目の議論であるカメラ設置の法的根拠について、話を日本に戻したいと思います。街頭設置カメラの法的性質を考える上で、まず、いかなる法的根拠に基づいてカメラの設置・運用ができていのでしょうか。これは、民間部門のものと公的部門が設置するもので明らかに違ってあります。

### (1) 民間部門設置カメラの設置根拠

まず、民間部門ですと、要するに民法上の権利です。所有権であるとか賃借権といった民法上の使用権に基づく——さらに、これは昔、公安労働事件でよく問題になったのですが、施設の中の秩序維持という、「施設管理権」という概念が判例で認められているわけですが、その判例の考え方に基づいて、財産の保全であるとか従業員やお客さんの安全といったようなものを管理する「施設管理権」というものに基づいていると考えられます。

### (2) 公的部門設置カメラの設置根拠

これに対して、公的部門が設置しているカメラはどうなのかといいますと、例えば地方自治体が設置しているものを例に取りますと、これは2つあります。いずれにしても自治事務といいますか、地方自治体が行う事務の一環として行われるわけですが、その中でも、1つは、いわゆる箱物ですね。市役所の庁舎ですとか、〇〇市民会館の安全の維持といったようなものに関しては、いわゆる公物管理権という概念が行政法学にあるわけですけども、この公物管理権の一環として、カメラの設置・運用がされていることになります。かつては固有事務と呼ばれていたものです。これに対しまして、例えば通学路の安全ですとか河川管理といったようなものにカメラを設

置して運用するのであれば、これはかつての行政事務と呼ばれるものですが、やはり、自治事務の一環として行われていると考えることができます。

警察の場合も、街頭設置のものは2つのパターンが考えられるかと思います。1つは、人間によるパトロールに代替するものとしての街頭設置カメラ、犯罪予防などを目的とする行政警察活動の一環としてのカメラの設置根拠についてですが、これは警察法2条に求められます。警察法2条の定める「警察は、個人の生命、身体及び財産の保護に任じ、犯罪の予防、鎮圧及び捜査、被疑者の逮捕、交通の取締その他公共の安全と秩序の維持に当たることをもってその責務とする」という警察の責務規定に照らして行われていることとなります。先ほどの1,715台のカメラというのは、こういった考え方に基づいて設置・運用されていると考えられるわけです。

それ以外に、特定の犯罪のために、例えば犯罪者がアジトにしているのではないかとこの人の出入りを見るために、臨時にカメラを設置するという場合もあり得るかと思います。それは捜査の一環という形になりますので、その撮影が任意処分にとどまるのであれば、刑訴法197条にいう「必要な取調」として、強制処分に当たるのであれば、刑訴法218条の定める検証の一環として検証令状に基づいて、それぞれ行ってください、ということになります。捜査用に設置したカメラに関して、それが直接争われた最高裁判例はありませんけれども、任意処分であれば捜査比例の原則に基づいて、検証に当たるようなものであれば検証令状を取って行ってくださいということですね。

このように、設置根拠が、設置主体によって、法的にいろいろ考えられるということになるわけです。

以上が、まず設置の根拠についての議論です。

## 映像の個人情報該当性と利用の許容性

### (1) 映像の個人情報該当性

次に、設置して、映像を撮って、それを録画してハードディスクやSDカードに保存していくということになりますと、それは、設置根拠があるカメラから撮影した映像なのだから、いかなる場合でも自由に使えるのでしょうか。そうではなくて、特に、先ほどもお話したように、映像の解像度が非常にクリアになってきていることを勘案する必要があります。そうしますと、撮影状況、画角などにもよりますが、かつては直ちに個人識別性が認められないような映像が主であったわけですが、それが鮮明なデジタル画像に置きかわってきたのです。

そうすると、どう考えるべきことになるのでしょうか。かつて「主流」だった不鮮明なアナログ映像ですと、民間が持っている間は個人情報には基本的にあたらないことになる。個人情報該当性というのは、その映像自体から個人識別ができる場合と、他の情報と突き合わせて容易に個人が識別できる場合に認められるわけです。そうしますと、民間ベースでは、なかなか容易には個人識別ができないので、個人情報には当たらない。でも、個人識別性がなければ捜査に使えないのではないですか、という疑問も生じます。そのとおりでして、警察が押収して、警察の捜査力をもって他の情報と突合すれば、個人情報該当性が認められるわけです。アナログ映像は、個

個人情報ではないけれども、個人情報に当たり得るものという位置づけを私はしていたのです。

しかし、デジタルの高精細の映像が主流となった現在は、最初から個人情報に当たるもの、したがって、個人情報保護法の適用対象になると考えるべきだということになります。

## (2) 個人情報としての映像利用の許容性

そうしますと、一般向けの講演なんかでこういう話をしますと、「えっ、個人情報に当たるの。じゃ、もう使えなくなっちゃうの?」という反応が、やはりあるんですね。ただ、これは明らかに誤りであって、個人情報保護法イコール「個人情報利用禁止法」ではないのです。

個人情報を使う場合には、一定のルールに基づいて扱ってくださいというのが個人情報保護法なわけです。個人情報保護法自体、非常に抽象的でわかりづらい法律なのですが、若干誤解含みなどところはあるかもしれませんが、あえて単純化しますと、個人情報を扱う場合には、まず利用目的を特定してください。それで、その特定された利用目的の範囲内でのみ利用してくださいということです。さらに、個人情報を取得する場合に、偽りその他不正の手段を使ってはだめですよ。あと利用目的を、原則として本人に通知してください。ただ、取得の状況から明らかな場合には個別の通知は不要です。あと「個人情報だから教えられません」、よくある場面ですね。それは個人情報が個人情報データベースを構成する「個人データ」になりますと、第三者提供について厳しい制約がかかるわけです。基本的に、本人の同意がなければ第三者に提供してはいけません。

この枠組みさえ守れば、個人情報保護法上、個人情報は何ら問題なく使えるということになります。ですから、防犯目的という目的を設定して、その防犯の目的のためだけに使うということであれば、個人情報にあたる映像でも、個人情報保護法上は、何ら問題は生じないわけです。

## 防犯カメラとプライバシー

### (1) プライバシー概念の意義

次に4番の防犯カメラとプライバシーというところに移りましょう。

防犯カメラの設置に当たっては、「個人情報保護法との整合性が懸念される」みたいな言い方は、まだあまりしないです。「プライバシーに対する影響が懸念される」という言い方は、良く聞きます。それでは、プライバシーとは何なのでしょう。

既に市民権を得た法的な概念であるプライバシー権ですが、実は、国会が制定した法律の中に「プライバシー」という言葉は一言も出てきません。あえて言えば、特別養護老人ホームの設置基準なんかで、プライバシーに配慮したサービスの提供をしてくださいという厚生労働省の省令ですとか、そういったような省令レベルで若干出てくるだけです。

それでは、法的根拠の全くない概念なのかというと、そうではなくて、法的ヒエラルキーの一番上のところ、憲法13条に根拠があるんですね。「すべて国民は、個人として尊重される。生命、自由及び幸福追求に対する国民の権利については、公共の福祉に反しない限り、立法その他国政の上で、最大の尊重を必要とする」。個人としての人格権の尊重、その一環としてプライバシー

の保護。「プライバシーが守られていない」イコール「個人として尊重されていない」ということになるわけです。ここに根拠が求められることになる。非常に抽象的なんですね。

さらに、これは法学の領域では必ずお話することですけれども、プライバシー権概念には大きく2つの内容がある。御承知のように、19世紀末、アメリカで最初にプライバシー権というものが生じてきたときには、今で言えば一部の週刊誌みたいなものですが、イエロージャーナリズムに対する対抗として、私生活をむやみに暴かれない権利があり、それによって個人が尊重されるべきだという主張でした。1人で放っておいてもらう権利、静穏プライバシー権という言葉もします。それが、特に20世紀後半、情報化社会の進展に伴って、自分の情報は適正に使われるように、ちゃんとコントロールするという考え方が生まれました。自己情報コントロール権、あるいは情報プライバシー権とも言いますが、このように、プライバシー権の中身自体も、時代によって変わってきている。ですから、議論が非常に見えにくいのです。憲法学では、プライバシーというものをどう捉えるべきなのかというのは、百家争鳴の状況なわけです。

ただ、街頭設置カメラとの関係で言いますと、これも古いものですが、大阪地裁が、平成6年に示した見解が参考になります（大阪地判平成6年4月27日判時1515号116頁）。これは、みだりに個人の情報の取得を許さず、みだりに取得した情報の公表・利用を許さず、もって個人の人格的自律・私生活の平穏を維持する、これがプライバシーの利益であると定義しております。要するに、むやみやたら撮影されない。撮影された映像をむやみやたらと使われない。そうすれば安心して暮らせることになるということです。あえて言えば、この最初の、「みだりに情報の取得を許さない」というのが静穏プライバシー権とニアリーイコール、「みだりに情報の公表・利用を許さない」、すなわち、適正に使ってくださいというのが自己情報コントロール権と、対応すると言えば対応するわけですが、こういったようなことを考えていくべきだとされています。

## (2) 個人情報保護とプライバシー保護との関係

そうしますと、次に、この個人情報保護とプライバシーの関係はどういう関係に立つのが問題になってきます。個人情報保護に関しては、先ほども若干お話したように、ごく簡単に言えば次の4点に気をつけて下さい、ということです。個人情報に当たる映像については、①利用目的を特定してください。②設定した利用目的の範囲での利用にとどめてください。③適正な取得をしてください。原則として本人通知してください。④個人データについて第三者提供には厳しい制限があります。

これを守ればOK、ということなのですが、ちょっと例を挙げて、例えば隣人トラブルでよくちよくあるのですが、隣人監視目的、嫌がらせ目的でカメラを、相手先の玄関先に、あるいは庭とか家の中が映るような形でカメラを設置して撮影するという場合について、個人情報保護法との関係を考えてみましょう。まず、①利用目的を特定してくださいということです、隣人監視目的です。②利用目的の範囲での利用にとどめてくださいということで、隣人監視目的だけで利用します。③適正な取得・原則本人通知してくださいということです、本音は嫌がらせです

から「正々堂々」撮影しますし、本人にも通知します。④個人データの第三者提供には本人の同意がない限りしてはいけません、わかりました、第三者提供しませんよ……。そうすると「あれ、個人情報保護法上は、この使い方もOKなんですか？」。

実は、個人情報保護法は、この本人への通知ということで、隣人監視目的での利用ということであれば、本人がやめてくださいとあって、こういう使い方がされないことを期待しています。ですので、個人情報保護法自体も、こういうことを積極的に認めているわけではないのですが、実は、個人情報保護法はミニマムスタンダードなんです。いわば個人情報を扱う際の無色透明の器を用意しているだけであって、その器の中にどういう液体を入れるのか、おいしいスープを入れるのか、からの煮汁を入れるのか、それは何も規定していないのですね。

ところが、こういった利用の仕方については、本人も「嫌だ」と当然言うわけですし、我々の常識としても、こういう利用の仕方は許されないと判断します。その判断を支えるのがプライバシーの考え方なのです。つまり、こういう利用というのは、プライバシーの不当な侵害に当たるから許されないのです。個人情報保護法が守られていなければ、それはプライバシーを侵害するような使い方にも当たることになるわけです。しかし、実は、個人情報の保護とプライバシーの保護というのは、必ずしも次元を同じくしない、異にする概念なんです。それでは、プライバシー保護の仕組みがどこに求められるかということ、そういう使い方は、民法90条の定める公序良俗違反になります。それによって、相手に対して精神的苦痛を与えたのであれば、民法709条の不法行為にあたります。なぜ公序良俗に反するのですか、他人の権利・利益を侵害したことになるのですか。それは、憲法13条の保障しているプライバシーの利益を不当に侵害したからなんですよ、という構造になっているわけです。ですから、ここが、議論が複雑になる1つのポイントです。

### (3) 許容限界を画するプライバシー概念の曖昧性

さらに厄介なのが、この、最終的に利用の許容範囲を定めるプライバシー概念自体がはっきりしないのです。先ほど、プライバシー概念は、法的には2つの概念、静穏プライバシー権と情報プライバシー権があるというお話をしたのですが、それぞれのプライバシー権の中身自体も変わっていくのです。

その典型を示すのが、グーグルのストリートビューです。ちょうど10年前、2008年に日本でサービスが開始された当初は、波紋を巻き起こしました。自分の家が勝手に撮られて、無断でインターネット上に載る、これは、とんでもない話です、と。一部の単位弁護士会、福岡県弁護士会ですけれども、そこは、即刻の中止を求めるという弁護士会としての声明を出したぐらいですし、総務省の中でも研究会を立ち上げて、こういったようなことは許されるのか、検討をしました。それで最終的には、撮影カメラの位置を2.45 mから2.05 mに下げるとか、ぼかしを入れてくださいといった要請に対する窓口を設けるとか、幾つかの修正はされましたけれども、今このサービスに対して根本的に文句を言う人は、ほとんどいなくなりました。みだりの情報取得、みだりの情報の公表・利用にあたるのではないかという懸念が、この10年間で、それは「みだりに」

ではないですよ、不当なプライバシー侵害には当たらない、というように、評価が変わったわけです。

さらにもう1つ、数年前に読売新聞が、池袋の大型書店の対応を報じたことがあります。本は、やはり今高いものですから、それを万引きして行って、特に専門書ですが、それを8割ぐらいの値段で出すとあっという間に売れる。新品同様だというようにアマゾンなんかのマーケットプレイスにも出ていますけれども、その中に贓物が紛れている可能性もあるのですが、それに手を焼いたその大型書店が、万引き常習犯の来店をチェックするために顔認証機能を入れました。ところが、それはおかしいじゃないかと批判的な記事が読売新聞に出て、「書店ですよ。書店で客の行動監視なんかをしたら、その人の思想・信条・趣味嗜好がわかってしまうではないか。とんでもないプライバシー侵害ですよ」という批判も生まれました。でも、それを言うんだったら、アマゾンはどうなんですか。同一IDを使っている限り、アマゾンは正確な情報を完璧に把握しているのです。それについては誰も文句を言わない。現実空間ではだめなものが、サイバー空間だとOKなんですよ。この差の合理性というのは、どこにあるのでしょうか。

もう少し言うと、家に鍵をかけ忘れて、あるいは店に鍵をかけ忘れて、金庫に鍵をかけ忘れて現金を取られた。現金は「窃取」されます。ところが、ネット上で、いろいろ重要な情報を蔵置しているサーバーにセキュリティホールがあって、サイバー攻撃を受けて情報を取られた。これは情報の「流出」「漏洩」とされて、管理者のほうが悪いんです。現実空間で鍵をかけ忘れてるのは、たしかに無用心ですけれども、鍵をかけ忘れていたら中へ入って現金を取っていったい、なんて価値観にはならないはずなのに、サイバー空間なら、なぜか攻撃を受けたほうが悪いんです。プライバシー概念の前提となる社会の意識は、かくも不合理なものなんですね。ですから、限界線を引くのが難しいのです。

## 捜査でのカメラ映像の利用

### (1) 街頭防犯カメラの設置根拠とその映像の利用

前置きの話が長くなりましたけれども、以上を踏まえた上で、警察におけるカメラ画像の利用というものが、どこまで許容されるのかということをもう一度考え直してみたいと思います。

まず、カメラ画像の取得、映像の取得ということを考えていきたいと思いますが、1,715台の、警察がみずから設置した街頭カメラからの映像の取得は、先ほども言いました、カメラの設置・利用については警察法2条の犯罪の予防・鎮圧に当たるという警察の責務の一環として行われます。ただ、法的な根拠があるからといって、いかなる利用も許されるのかというと、もちろんそうではない。その限界はあるわけですが、それは実は、昔から言われていた警察比例の原則です。利益侵害の程度と達成しようとする目的とのバランスを考えて、そのバランスがとれていなければ不当なプライバシー侵害に当たる、ということですね。そうしますと、先ほどの大阪地裁平成6年判決が示した、①目的の正当性がありますか、②設置の必要性はありますか、③設置状況に妥当性はありますか、④設置・使用に効果がありますか、⑤使用方法の相当性がありま

すか、こういうものを考えていって、これをクリアするのであれば、警察比例の原則から許容されるカメラの設置・利用になる、同時に、不当なプライバシー侵害には当たらない、という形になってきます。

次に、何もなければその映像は2週間なら2週間、1カ月なら1カ月で捨てていくわけですが、何か捜査に使える映像が出てきたということであれば、そこから映像を引き出します。それについても捜査比例の原則ということで、設置自体が任意にとどまっていますから、そこからの映像の引き出しも任意処分にとどまるわけですが、片方で捜査の必要性、犯罪の重大性ですとか証拠としての必要性がどの程度あるのか、もう一方で、被侵害利益に対する程度はどれぐらいあるのか、どういう状況が映っている映像なのか、その両者の比較衡量から許容範囲が決まることになってきます。一般の任意捜査の許容限界と全く変わらないという形になります。

## (2) 捜査目的でカメラの設置と利用

捜査目的で設置するカメラからの取得についても同じです。個人の意思を制圧し、身体・住居・財産等に制約を加えないような対応での行動、あるいは公道から見える範囲での撮影ということであれば、いわば実況見分としての撮影という形になってきます。それで東京地裁平成17年の判決（東京地判平成17年6月2日判時1930号174頁）は、連続放火事件の被疑者ではないかと疑われる者の自宅ですとか、あるいは幾つか駐車場の撮影は、適法だとしています。東京高裁平成19年の判決（東京高判平成19年8月7日（高検速報平成19年280頁）は、これも強盗被疑事件で非常に重い事件ですが、アジトとして使われているのではないかという家の玄関先を撮影したところ、これは証拠としての必要性は薄い、このような捜査までする必要はない、捜査の必要性は低いという形で違法だとされたものがあります。やはり捜査比例の原則による適法性判断という形になってきます。

これに対して、住居の中ですとか、通常外から見られない、プライバシーに対する合理的な期待が認められるところを撮影するというのであれば、「検証」として許容されるのかが問題となります。これは正面から争われたものではありませんが、有名なX線検査についての最高裁平成21年の判例（最決平成21年9月28日刑集63巻7号868頁）、これは検証令状を取ってやってくださいという判断を示したものですが、この考え方が恐らく妥当することになるだろうと思います。

## (3) 民間部門設置カメラからの映像の取得

それから、圧倒的に多くは、民間に設置されているカメラから取得するという場合であると思いますが、この場合にも、やはりカメラの管理運用者から任意提供を受ける場合であれば、刑法197条の必要な取り調べの一環として行うことができるという形になります。その場合に、私の所属している大学もそうなんですが、捜査関係事項照会を出してください、そうであれば出しますよとよく要請をします。学生が粗相をしたりして、こういう学生はいませんかという照会が警察からあった場合に、捜査関係事項照会を出してくださいとお願いするのです。ただし、本来は、

相手方が任意に応じない場合に捜査関係事項照会をかければ、強制性があるとまでは言いませんけれども、相手方に強く「出せ」と求めることができるというものですが、今は証拠がわりに使われていますね。データを提供した側が、後から、例えば学生のデータを提供した場合に親から苦情を寄せられて、「何でうちの息子の個人情報を出したのだ」というふうに言われた場合に、「いや、警察から言われたんですよ」という証拠文書として残してほしいという、ちょっと本来の使い方とは違う使い方がされるようになってきています。

そうしますと、今、大阪府警と市町が設置しているカメラとの間で、役場が開いている間は役所の職員の立ち会いのもとで映像を引き出すのですが、夜間・休日、急速を要する場合には先に映像を出してしまって、後から捜査関係事項照会を出します、という運用方法について協定を結んでいます。「それはおかしいじゃないか」みたいな議論もあるわけですが、少なくとも、市町により任意処分にとどまる形で設置されているカメラの映像について、市町のほうがOKですと言っているのであれば、これは問題ない運用であることとなります。映像について、仮に第三者提供制限の制限にかかるのでは、ということであれば、その例外として認められる法令事項にあたります。刑訴法 197 条の警察による捜査の一環として行うものです。

これに対して、相手方が提供に応じないということであれば、搜索差押許可状に基づく強制処分を押さえるしかない。非常に古いものですが、國學院大學映研フィルム事件という非常に有名な判例（最決昭和 44 年 3 月 18 日（刑集 23 卷 3 号 153 頁））がありますけれども、この考え方が妥当するという形になります。

#### (4) 捜査目的での映像の取得に関するその他の問題点

あと、民間撮影映像からの取得については、ストリートビューの映像を捜査に利用するという場合もあると思います。これも、先ほど少しお話ししました。ストリートビューの映像自体、現在は不当なプライバシー侵害には当たらないのだというコンセンサスが得られているわけですし、すでに公表されている映像なわけですから、それを捜査に使うということによって新たな法益侵害が生ずるとは基本的には考えられないと思います。

これに対して、メディアが撮影した映像ですと、これは報道の自由、取材の自由との比較衡量を考える必要がありますので、若干難しい問題が出てきます。報道の自由は表現の自由に資するもので非常に重要なものですし、その前提をなす取材の自由との関係もあります。ただ、取材の自由に関しては「一定程度の尊重が求められる」という位置づけで、やはり捜査の必要性という公益目的との比較衡量で、一定の制約も認められます。有名な博多駅事件（最決昭和 44 年 11 月 26 日刑集 23 卷 11 号 1490 頁）、日テレ事件（最決平成元年 1 月 30 日刑集 43 卷 1 号 19 頁）、TBS 事件（最決平成 2 年 7 月 9 日刑集 44 卷 5 号 421 頁）というものがありますけれども、その枠組みの中で許容される場合であれば使えるという形になるかと思います。

また、ドライブレコーダーからの映像の取得はどうなのでしょう。ドライブレコーダーも、今は映像が非常にクリアになってきていますので、基本的には個人情報に当たる映像を撮っているという形になると思います。そうしますと、利用目的の特定ということであれば、交通関係な



んですね、通常は。ですから、交通事故での証拠映像として使うのであれば、本来の、特定された利用目的の達成に必要な範囲での利用という形になるわけです。しかし、それをそれ以外の犯罪捜査にも、いわば移動する街頭防犯カメラとして使うことができるかという問題が出てきます。実は、個人情報保護法自体が、特定された利用目的以外での利用も一定の範囲で認めています。その典型的なものが、法令に基づく場合です。法令に基づく場合には、例外として本来の利用目的以外の目的でも使えるという形になってきますので、警察の捜査として許容される範囲であれば提供できるという形になります。

ただし、プライバシー侵害の程度のいかんは、より厳しく評価されるとも考えられますので、捜査についての公益目的はどれぐらいあるのか、それと被撮影内容との比較衡量という形で判断されます。名古屋高裁の平成17年の判決（名古屋高判平成17年3月30日裁判所ウェブサイト）は、近隣のホテルで起こった私文書偽造事件に関するものです。偽名で宿泊するという、一定の公安事件によくあるものですが、その捜査のために、本人が間違いなくそのあたりにいたということを、ホテルのそばのコンビニエンスストアの映像からとってきた。コンビニエンスストアのカメラというのは、利用目的は、本来は店内の防犯のためなので、それ以外の目的に使えるかが争われたのですが、比較衡量の観点からこれは許されると判断されました。あと、有名な三浦和義のものですけれども、彼が自宅近くのコンビニで万引きをした。その映像が報道で流されるなどしたということで、三浦和義が損害賠償を求めて訴えた事件があります。東京地裁平成22年の判決（東京地判平成22年9月27日（判タ1343号153頁）は、報道には万引きの警鐘という公益目的があるので、それは許容されます、ということで適法な利用だとしました。けれども、このコンビニエンスストアにカメラを納入した設置会社が、「うちが納入したカメラで三浦和義の万引きの場面を捉え、捕まえることができました」と、その映像を宣伝に利用した。そういった商用での利用は許されません、公益目的がありませんと判断し、その部分に関しては違法だという形で損害賠償を認めています。

こういったような形で、利用の許容範囲というのを個別の文脈ごとに判断していくしかないわけです。

#### (5) 生体認証機能の利用可能性

そうしますと、先ほど顔認証機能について野田会長からお話がありましたけれども、顔認証機能の利用というのをどういうふうにか考えるべきなのか。個人情報保護法のレベルとプライバシー保護の観点からのレベルと2つのレベルで考えますと、顔認証機能付のシステムを入れるか入れないかによって利用目的である防犯目的、例えば店頭での防犯目的でカメラを設置した場合、それはプレーンのシステムであっても、認証機能がついているシステムであっても、変わらないことになります。特定された利用目的は変わりません。では、何が変わってくるか。利用目的達成に必要な範囲での利用にとどまると言えるのでしょうか。店頭での万引き防止のために顔認証機能付のシステムを使うことが必要な範囲と言えますか。こういった解釈問題として、個人情報保護法のレベルでは問題になってきます。具体的には、個人情報保護法16条1項の解釈、行政機

関であれば行政機関個人情報保護法3条2項の解釈問題です。では、必要な範囲での利用として許されるのですか、許されないのですか。その許容限界を定めるのは、プライバシーに対する社会一般の理解ということになります。データベース登録者への利益影響の評価ですとか、あるいはデータベースへの登録基準ですとかシステムへの理解によるのだと思います。

先ほど、大型書店での話をしましたけれども、店に入ってくる大多数のお客さんに関しては、顔認証のためのデータ登録はしないわけです。しても無意味なわけです。来店客全員に反応させてみても、店がてんでこ舞いになるだけです。万引きの常習性が疑われる者についてのみだけ登録することによって、必要なアラートを立てて警戒をすることができる、そういうシステムです。そうであれば、大多数の人にとってみれば、プレーンのカメラシステムとプライバシーに対する影響は全く変わらないのですね。そういうシステムに対する理解というのが、まだまだ得られていない。こういったようなものについての理解が得られれば、恐らく顔認証機能の利用に対する理解というものも深まっていくだろうというように考えられるかと思います。

## 映像の証拠利用

カメラ映像の証拠利用については、簡単に言及させていただきたいと思います。証拠価値、映像の信用性ということに関して言いますと、やはりビジュアルというのは、人間にとっての訴求力が非常に大きいです。インパクトが非常に大きいですし、最近は裁判所でも、「防犯カメラ映像はないんですか」みたいなことをいって検察官に立証を促す、といった話もあると聞いています。確かに、インパクトが大きいイコール真実を映しているということにはなるのですが、そこに誤解を生ずるような映像があった場合に、その誤解が「真実」になってしまうという両刃の剣でもあります。

やや古い判決ですけれども、不鮮明なアナログ時代のもので、風体が似ている者がコンビニエンスストアのATMで盗んだカードを使って行った。「おまえだろう」ということで捕まえて、起訴までしたのですが、映像を分析してみたら別人だということがわかったという事案があります（金沢地判平成22年9月1日判例集未掲載）。耳の形がどうみても違う。こういう他の情報との突合が大事になります。これは有名な事案ですが、ガソリンスタンドで、盗んだカードを使ってガソリンを入れた人がいた。ところが、ガソリンスタンドのカメラ映像の上に映り込ませたメタデータ、何時何分に映したのかのメタデータの時間が間違っていたがために、そこにたまたまスポットはまってしまった別人を、犯人として誤認逮捕し、起訴までしてしまった。この人は、その直後にETCを使って高速道路に入っていて、それと突合しますと、明らかにこんな短時間では移動できない、これは、絶対別人なはずだということがわかったわけです（大阪地判平成27年6月15日LLI/DB:07050331参照）。やはり、他の客観証拠の突合、相対化の必要性というものをいま一步、ぜひ意識していただきたいと思います。

逆に、映像データによって証言の信憑性も判断することはできます。今まで間接証拠というのは、証言の組み立てなどでやってきたわけですが、人間の証言ほど、記憶ほど、当てにならないものはないわけですね。これは、GPS捜査についてインパクトを与えた最高裁判決が出たのと

同じ日に大阪地裁で出た判決の事案ですけれども、痴漢の事案について、被害者はこの人が犯人だと言っている。ところが、映像を見ると、その人は明らかに離れたところにいる。その人が犯人であるとは思えないという形で無罪判決が出た（大阪地判平成 29 年 3 月 15 日 D1-Law.com 判例体系：28251741）ということもあります。

## 今後の課題—まとめに代えて

最後、管理運用部門でのことを考えますと、やはりテロ対策ですとか警備の問題、事象警備の問題への対応が必要となりますね。特に最近、渋谷でのハロウィンですとか年越しカウントダウンみたいなもの、この警備というのは非常に大変なわけです。東京ドームでイベントがあるということであれば、最大でも 4 万 5000 人ですよ、何時ごろこうなりますよ、ということがわかりますから、警備計画は立てやすいわけです。ですが、こういう自然発生的な事象については非常に把握するのが大変で、どういう警備をすればいいのかというのが大変になってくるわけです。そうしますと、人出の予測・把握というものに、ふだんの防犯カメラ映像が使えないでしょうか。あるいは人流の把握に関しても同じです。例えば、こういったような利用ですと、個人識別性は要らないんですね。「数」が必要になってくるわけです。あるいは、「流れ」が必要になってくるわけです。そうであれば、非識別加工情報ですとか統計情報としての利用が考えられます。非識別加工情報ないしは匿名加工情報というのは、個人との対応関係はあるのだけれども、それが誰なのか常識ではわからないというレベルに匿名加工しているものです。統計情報というのは個人との対応関係も全くなくなるものです。そういった個人識別性のない画像情報を、ツイッターなど、SNS 上での「渋谷に集まろうぜ」という言葉の頻出度合いと突合するみたいな形でやっていくということであれば、恐らく許容されることとなります。少なくとも個人情報保護法上は、非識別加工情報になれば、本人の同意がなくても自由に使えるわけですので、こういう利用も可能という形になります。ただ、やはり最終的には、そういった利用に対する世間の理解が得られるのかが重要ですね。

時間がなくなってきたので、一言だけ最後に申し上げますと、世間の理解が得られるかどうか、という問題を考える場合、何でストリートビューが最初にあれだけ懸念されたのが、この 10 年でこれだけ受容されるようになったのか、その分析が参考になると思います。

ストリートビューのおもしろいところは、防犯システムとに大きな違いがあって、撮られた人も何が撮られたのかわかるということなんですね。自分の家がどういうふうに映っているのか確認できる。それを見たら、「大したことない映像じゃないか。こういう程度のものなのか」と確認ができるわけです。あともう 1 つの特徴が、皆さんも使えるということなんですね。メリットを得られるシステムなのです。プライバシー侵害の程度がそれほど大きくなくて、それをはるかに上回る便益がある、ベネフィットがあるのだ、そういう理解が得られると、不当なプライバシー侵害だという評価ではなくなるわけです。

あと、以上のことが誰でも把握できるという、システムの透明性があるということです。透明性の問題は、なかなか防犯システムの場合は難しいところもあるわけですが、どういうシステムで、どういう形で運用するのか、それに対する丁寧な説明と理解が得られるかどうか。そ

ういうシステムによって、皆さんの安全が守られるんです、という理解が得られるかということが大事になってくるのではないかと私自身は考えております。

以上、雑駁な話ではございますけれども、私のほうからの基調講演は以上とさせていただきますと思います。御清聴いただき、ありがとうございました。(拍手)

## 質疑応答

### マスメディアが撮影し、放映した画像の捜査上の扱いについて

メディアにいらっしゃった方をお隣にして、なかなかお話しづらいところもあるのですが、確かにおっしゃられたとおり、少なくとも、既に放映されているもの、あるいはインターネット上に載っているものであれば、それはオープンになっているわけですから、必要な取り調べという形で警察が集めることは、本来的にはできるはずです。

ただ、理屈を言いますと、それでもやはりメディアの方が抵抗されるのは、取材元が、メディアで放映する分にはいいけれども、おれは警察が嫌いだから、警察の捜査に使われるのならしゃべらないよという人が出てきかねない。そうすると、取材の自由が制約されるではないかというところを恐らく懸念されていると思うのです。そこで報道の自由、取材の自由と公益目的との比較衡量という形になってくるかと思えます。

ですから、一律に禁止されるというものでも、一律に許容されるというものでもなくて、比較衡量という非常に曖昧なマジックの中で、これぐらいの証拠化であれば利用可能であろう、あるいはメディアのほうも、これが使われることは当然の前提として放映しているのだろうというようなことが推測できるのであれば、それは十分可能だし、それが直ちに違法収集証拠に当たるといったことはないだろうと考えております。

ライブ映像の捜査への利用ですが、少なくとも、ブロードキャストという形で公開の放送で流される映像であれば、捜査への活用は十分可能であると、私は思います。捜査という文脈でいいますと、街頭で警察官が見ているのか、捜査機関そのものでないにせよ、公開で放送される映像としてモニターを通じて見ているのと、プライバシーに対する影響は、基本的には変わらないと思います。そうであれば、そういった映像を使うこと自体は問題にならないでしょう。

それを顔認証機能と組み合わせた利用については、個人情報保護法上は「目的達成に必要な範囲での利用」といえるのであれば、これも問題ないはず。これも、すでに指名手配等、一定程度以上の嫌疑のある者の照合データを使うような場合には、強制処分性を基礎づける法益侵害もないので、任意捜査として許容される程度の影響にとどまるといえるという面と、犯罪の重大性や嫌疑の程度などとの比較衡量に基づく捜査比例の原則で許容されるかどうかの判断がなされることとなります。それが同時に、個人情報保護法の「目的達成に必要な範囲での利用」にあたるという判断を基礎づけるものになる、というように考えております。

### 国民が撮影した画像のテレビ放映とプライバシーの関係について

これもメディアに関係する話ですので、なかなかお話しづらいところはあるのですが、

私自身の問題関心からいきますと、先ほどの三浦和義の事件が興味深いですね。カメラの設置会社が自分のところの宣伝にあの映像を使うのはだめだけれども、メディアが使うのはいいよ、というのはぎりぎりの線です。やはり、本来の利用目的というのは、店内の防犯ということであれば店内の防犯のみに使うものであって、メディアがそう簡単に使うというのをそんなに許してしまっていていいのかなと、逆に疑問は感じます。

ただ、確かに知る権利みたいなものがあるわけですね。捜査との関係でいきますと、初動段階で余り知られていないほうが捜査にとっては適切といたしますか、捜査の妨げにならないかとか、いろいろな問題もあると思うのですけれども、今おっしゃったように、事件が起こると、現場付近の防犯カメラ映像を警察とメディアが取り合いをしているという、何かとんでもない状況になっている。知る権利があるとはいえ、メディアが何でそんなに強いのかな、と思うところも少なくはないです。やはり、比較衡量の天秤の針の置き方というのを少し考える必要がある状況にあるのかな、というふうに思っています。けれども、ちょっと私の狭い知見では、そこを正面から論ずることは、表現の自由というのがかかわってきて難しい、議論しづらいところもあって、それほど盛んな議論はされていないのではないかと認識しています。曖昧な答えで申しわけないのですけれども、そんな気がしております。

#### 補足発言

やはりネット関係の話ですね。ネットメディアの関係というのは、やはりこれから厳しくなっていくのだろうなと。ネット社会になって、ある意味、情報の秩序だった整理というのが、確かにできなくなってきている。そういう中で、我々の価値観みたいなものも、過剰に、しかも一時的にしか反応しないネット世論みたいなものに、どんどん振り回されていくということになりかねない状況がある。その中において、先ほども言いましたように、もともと合理性に乏しい面もあるプライバシー概念の中で、最大公約数を求めていくのがどんどん難しくなっていくようにも思います。

そうしますと、本日は防犯カメラの利用という形での情報の扱いということだったわけですが、どのような情報が、どこまで利用できるのかということが、やはりグレーゾーンが逆に広がっていくことになると思うのですね。グレーゾーンが広がっていく中で、これはグレーだから踏み込まないでおこうということで済むのであれば、それでよいのですが、先ほどからありますように、それで本当に我々の生活の安全・安心が守られるんですかというところが出てきますよね。ですから、どこまで踏み込むのか、そして踏み込む際に、どういう手順で踏み込んでいって、ある一定の批判はあったとしても、やはりこれだけの利益があるのだから、こういう使い方は認めてくださいよと、そういう方向性の議論は、少しこれから真剣に考えていかないといけないと思います。従来のやり方では、難しいかもしれない。片方で犯罪予防といいますが、それに対する国民の期待といたしますか、それを求める声も非常に大きいわけですので、そこのバランスのとり方がますます難しくなっていくのだろうな、という感じがしております。

## 超監視社会をどう生きる——公益とプライバシーとのほざまで

木村伊量（国際医療福祉大学大学院特任教授・前朝日新聞社社長）

司会（松尾庄一） 木村先生は、約3年前まで朝日新聞社の社長を務めていましたが、訳あって辞任しまして、現在はフリージャーナリストとして活躍しています。それに加え、アカデミズムのほうにも手を伸ばしており、日本だけでなく米英の大学で研究したり、教鞭をとったりするなど多角的な活動をされています。

その活動の1つが、国際医療福祉大学大学院特任教授として、社会人向けに文明史を論ずる講座、通称、乃木坂スクールを開講しました。それを受講しましたが、このテーマが、「我々人類はどこから来て、どこへ向かうのか」という大変雄大なもので、また内容もすごくて、毎週1回、90分の講義を前期15回、1～2カ月休みをとった後に後期15回、都合、30回1人でこなされたということで、ここら辺にもまた超人的な能力をうかがい知ることができるわけであります。その中で、「カメラ社会における公益とプライバシーとの関係」につきまして、大変意義があるといえますか、社会学的な観点で見ると、こういうことなのかというような話を聞きまして、本日の講演をお願いした次第です。

皆さん、こんにちは。御紹介いただきました木村でございます。

松尾さんとは、私は高校時代からの友人で50年にならんとするような、大変敬愛する友人です。彼から「とにかく出てこい」と頼まれたら、断るわけにはいかないんですね。きょうお見えの皆様の中にも、私が新聞記者時代に、内閣調査室や警察を担当した中でお世話になった方も散見されますし、こうした貴重な機会をいただきまして、大変ありがたく思っております。

最初にお断りしなくてはならないのは、私は監視カメラの分野の専門家でもありません。きょうは、多分にジャーナリスティックな視点から、ジャーナリズムと言うと、すぐに「権力に対するチェック」とか、「権力の暴走をいかに止めるか」といった観点からの問題意識が旺盛なのですが、今日のジャーナリズムが扱うべき問題は、単に権力のチェックだとかに限りません。公益にどのように利するかという問題も視野に複合的な考察を加えることが求められております。先ほどから星先生が議論を展開されていますが、プライバシーという中身も、古典的な「権力とプライバシー保護」という観点を越えて、随分と領域が広がってきている感じがしております。

そういうことで、少し話が雑駁になるかもしれませんが、監視システムが高度化し、かつてないほどの超監視社会とも言われる現代が、どのような新たな課題を私たちにつきつけているのか、お2人の方とはちょっと違う視点から問題提起をできればと思っております。

### 「パノプティコン」近代監視システムの原型

さて、少し歴史を振り返りましょう。監視システムというと「パノプティコン」というモデルがよく引き合いに出されます。私は大学時代に、近代ヨーロッパの思想史を専攻していて多少は知っていましたが、ベンサムという大変有名な英国の功利主義哲学者が、「パノプティコン・



モデル」という考えの始祖とされます。どうやって大勢の犯罪者を効率的に監視していくかという観点から近代的な監獄を構想したとき、一つのロールモデルになっているのが「パノプティコン」というわけです。つまり独居房の受刑者からは逆光に照らされて何も外は見えないけれども、円形に並んだ監獄の真ん中にある看守からは、すべての受刑者の様子が見渡せる。四六時中監視できるシステムですね。そうすると、受刑者は看守がたとえ不在でも、看守を意識せざるを得なくなるということですね。このような、いわゆる「パノプティコン・モデル」というのは、近代と監視ということを考えるときには避けて通れないという理念型になっているのですね。

時代は下って、20世紀のフランスの哲学者ミシェル・フーコーという人は、このベンサム「パノプティコン」システムに着想を得て、現代社会は監獄に限らず、一方的な権力による監視の中に置かれているのではないかというような議論を展開しました。現代の一般的な企業でも、大きな部屋で部長さんや課長さんといった管理職の机が窓を背に置かれていて、一般の職員は部長さん、課長さんに向かい合っているような光景をよく目にします。こういう配置が「パノプティコン」システムの応用、現代版であろうという見方もあるわけです。これを「一望監視システム」と言われることがあります。

そうした中で、監視という問題になってくると、必ずと言うほど引き合いに出されるのは、英国の作家ジョージ・オーエルのディストピア小説、反ユートピア小説の代表格として名高い『1984』という小説であります。

これは、オルダス・ハクスリーの『すばらしい新世界』とともに、いまなおSF小説の最高峰と言われておりますが、去年、アメリカで再ブレイクしました。言うまでもなく、ドナルド・トランプ大統領が誕生して、以来、ホワイトハウス発の「フェイクニュース」がどんどん流されて、危機感が高まった。全米の本屋には、この『1948』の新装版が山積みになっているのですね。さすがに、米国民も考え始めたわけです。たとえウソでもそれを100回言ったら、本当になってしまうという社会への危機感、漠然とした恐怖がアメリカに広がったのでした。

内容をご存じの方は多いことでしょう。モデルはヒトラーなのか、スターリンなのか、その正体はよくわかりませんが、全体主義国家の親分が「ビッグブラザー」と呼ばれて独裁体制を築いている。街のいたるところに「ビッグブラザー・イズ・ウォッチング・ユー」というポスターが貼られている。あなたは四六時中見られている、というわけですね。監視社会、管理社会のこ



とをあまりに戯画的に誇張して描き過ぎているとの批評もあるようですが、この小説の主人公が、「真理省記録局」に勤務するウィンストン・スミスという人です。真理省記録局、これは書きかえ、歴史の改ざんが専門の仕事になっているところですね。あまり大きな声では言いたくないけれども、いま問題になっている財務省理財局みたいなところでしょうか。そういう仕事に追われ、全体主義の国家に不満を抱き、そこでスミスは——お読みになっていない方もいらっしゃると思いますので、あとの筋書きは控えますが、いまなお読み継がれる不朽の社会批評SFだと思います。

しかしながら、こうしたものは日本の中でも、敗戦後、民主主義国家として出直した後もそうですが、とりわけ戦前から戦中にかけての軍国主義のもとでの監視国家という問題は、批判の対象となってきました。吉永小百合さんが主演した映画で、皆さんごらんになったかもしれませんが、「母（かあ）べえ」、お母さんという映画がありました。あるときお父さんが特高警察にしょっ引かれてしまう。いわゆる思想犯として巣鴨の拘置所に入れられる。国体変革を狙う危険極まりない非国民、として白眼視される時代を描いたものですが、これは、年配の皆さんは御存じでしょうし、私たちジャーナリズムにとっても非常に苦々しい思いで振り返るところであります。

その中で、私は直接知っているわけではありませんけれども、御年配の方は「♪とんとんとんからりんの隣組」なんて歌が流れて、どことなく歌の調子は明るい。みんながそれぞれ苦しい中、耐乏しながら助け合おうという隣保組織であります。別の一面は、聖戦遂行に民間レベルで協力していこうという狙いを持つ住民の相互監視組織として機能した。軍事物資を供出する、防火演習をするというのにとどまらず、「あいつはどうも怪しいぞ」「英米の小説を読んでいるらしい。スパイじゃないか」といった根も葉もない噂が容疑に仕立てられていく、軍事体制に奉仕する通報組織にもなっていったような面もあったのです。すべて戦前・戦中は暗かったと申すようなことは避けたいと思いますけれども、このような一面は厳然とした事実としてありました。

### ビッグデータ時代と「マス・サーベイランス」

しかしながら、先ほど星先生もお話になりましたけれども、監視というのはとくに21世紀の世界では、古典的な定義以上に二面性を持っている、たいへん難しい問題であろうと思います。1つは公共全体の利益として、テロリストら凶悪な犯罪者が地域コミュニティに紛れ込まないた



めに監視を強化する、これは至極当然の感情というか、そうした警戒感というのは、私はどの時代にとっても変わらないことであろうと思います。

しかしながら、一方で、これだけ多くの人たちが、自分たちの所属空間というのがいろいろ多様なところにあると、事情はもっと複雑になる。実社会での所属も、暮らしの糧を得るための職業だけでなく、地域、ボランティアなどの社会奉仕などさまざまな空間に横断的に関わるが増える。そればかりか、いわゆる「バーチャルな空間」にも所属してくると、人物の属性をひとことで言い表すことが至難の業になるわけですね。風体、物腰だけで凶悪事件を起こしそうな「怪しい人物」を識別することなど、まずもって時代錯誤だし、難しい。テロリストは往々にしてごく良識的な普通の生活人として世間に紛れているわけです。じゃ、どうするか。つまり、そこにビッグデータの高度活用という観点が出てきます。それでは、いっそのこと全部「マス・サーベイランス」と言いますが、すべての人を、とにかく皆が皆、怪しいというわけではないけれども、すべての人を監視の対象にして、犯行現場近くの複数のカメラの画像にたびたび登場する人物をクロスチェックして、一定の人物を「重要参考人」としてあぶり出すという監視システムに行かざるを得ない。

これについては、議論はいろいろあると思います。それほどひどい全体主義的な国家でいいのかという議論も当然あるでしょうし、一方で、それが一番効率的で、犯罪防止や事件解決という公共益に利するのなら許容されるべきだという議論もあるでしょう。

ビッグデータの経済原理に従いますと、どの特定のデータを選別、集積して保存するかというよりも、とにかく根こそぎデータを持ってきて、そこに保存した膨大なビッグデータから、さっきも顔認証のお話がありましたが、要件が合致するものをコンピュータで絞り込んでいくほうが、よっぽど手っ取り早いし、効率がいいという社会ですね。どちらかという、私は社会全体の大まかなコンセンサスそちらの方に向かっていっているのではないかという気が致します。

先ほどプライバシーの定義につきましては、星先生から大変精緻な議論がありました。プライバシーというのは、単に政治の恣意的な権力監視から私生活をというのではなくて、まさにアメリカのボストンの2人の弁護士が、1890年代に「プライバシーの権利」という論文を公表したことに始まります。要するに、当時の扇情的なイエロージャーナリズム、これにさらされて私生活が覗き見されるのはかなわないと。そこからプライバシーという権利を守ろうという動機が最初だったのです。プライバシーをめぐる議論は、もちろん、先ほどの「静穏を守る」ということにとどまらず、例えば最近ではウェブ空間でいつまでも自分の肖像や情報が残っていることに対する異議申し立て。つまり「消す権利」、「消えてしまいたい権利」も新たな論点として議論されてきました。プライバシー保護という古い問題も、先ほど星先生からお話がありましたように、かなり対象領域が広がってきていると思います。

プライバシーが「一人にしてほしい」権利だとすれば、逆に、セキュリティの原則は「決して1人にしない」ということですね。決して社会から孤立させない、1人にしないという、この権利と原則との間に、当然のことながら相克が生じます。

## 2005年の同時テロが潮目 英国の民意の変化

さて、きょうの主題でもありますけれども、監視カメラをめぐる具体的な議論に進めましょう。これは、私が10年ほど前に新聞社の特派員としてロンドンにいましたときの直前でしたが、2005年7月7日にロンドンの地下鉄と市営バスが同時テロに遭って、多くの犠牲者が出たことがあります。それから私は何度かイギリスへ行き、おととしもイギリスで暮らしましたが、かなりイギリスの国民の感情は変わってきているなと思いました。7・7と呼ばれる同時テロの前には、もちろん2001年の9・11同時テロがアメリカでありましたけれども、7・7の時は監視カメラに映った画像を追ってテロリストたちが一網打尽にされた。これ以降、個人のプライバシーの問題は残るが、やはり公共益のためには街角や公共施設、交通機関などいろいろなところにCCTV（クローズド・サーキット・テレビジョン）を置くのは致し方ない、という世論が増えていきました。



10年ほど前に、私がロンドンで暮らしておりましたときにも、イギリス国内に300万台から400万台のCCTVがある、と言われていました。それで今は、先ほどの御紹介だと590万台とか600万台ということですか、まさに飽和状態にあると思います。ロンドンの街中を、1日朝から晩まで行動すれば300回は記録されるだろう、ということです。ロンドンの警視庁・スコットランドヤードの知人の話だと、いまもそれは大きく変わっていないそうです。例えばロンドンの地下鉄の中にも、大体1万2000台ぐらいのCCTVが備えられていると言われていています。ヒースロー国際空港でも300台あると言われていています。また、例えばスコットランドヤード、ロンドンの警視庁の中にも、監視カメラの画像処理のための専門チームがあり、100人ぐらいの要員で、始終それを分析している。それから、ビクトリア駅という大きなターミナルがロンドンにありますけれども、その近くにはイギリスの鉄道警察ですね。BTP（ブリティッシュ・トランスポート・ポリス）。鉄道のCCTVを網羅的に、専門的に監視しているセクションもあります。特派員のときにそこにお邪魔して、お話をいろいろ聞いたことがありました。テロ防止とプライバシー保護の関係をめぐる議論はなお続いていますし、2012年でしたか、デーヴィッド・キャメロン首

相のもとで、プライバシー保護にもう少し重きを置いてはどうかという議論も浮上したようですが、概して、イギリス人の中では監視カメラは、テロ防止という公共益を守るための装置として、許容されているというような方向ではないかと思います。

ただ一方で、ヨーロッパの大陸、特にフランスとかスペイン、それからドイツの一部等には、まだまだこういうCCTVのようなテレビへの不信感が強い。「ビッグブラザー」の監視社会への潜在的な恐怖ですね。それはそれで理解できます。ヨーロッパと一口に言っても、大陸系とイギリスとでは、かなり温度差がある、というような感じを持たざるを得ないということでもあります。

### スノーデン告白の衝撃

少々、本日のテーマとはずれるかもしれませんが、情報収集、インテリジェンスをめぐる議論となると、数年前になりますけれども、世界を驚かせたアメリカのCIAの元職員、スノーデンによる衝撃の告白に触れざるを得ません。彼によると、アメリカのNSA(国家安全保障局)によって、ハイテクを駆使したインテリジェンス活動というのが地球の隅々で展開されていた。その対象はロシアや中国は言うに及ばず、ドイツの首相、イギリスの首相から日本の安倍首相——第1期目の安倍さんのところですが——の周りから、いろいろなところに盗聴装置が仕掛けられて情報が集積されてということでありました。それで、このスノーデンという人は、NSAの基地内での大量のトップシークレットを全部USBメモリーに入れて持ち出して、それを懇意なジャーナリストを通して世界に拡散させたということでした。こうしたことは、皆さんも記憶になお新しいところでもあろうと思いますけれども、少なくとも第1次安倍内閣のころから、しかも同盟国日本に対してもやられていたという事実は衝撃でした。

かつての非常に古典的な「007」が暗躍したようなスパイの時代とはまた違って、極めてハイテクな情報処理システムを駆使しながらのインテリジェンス活動というのが、地球上で24時間展開されているということですね。

さて、そうした中で、アメリカのインテリジェンス史に名を残すであろうマイケル・ヘイデンという人物がいます。NSAやCIA(中央情報局)の長官もつとめたインテリジェンスのプロの軍人です。2001年9月11日に世界を揺るがす同時多発テロがニューヨークやワシントンで起きたわけでありますが、そのときのジョージ・W・ブッシュ——これはジュニアのほうですが——にテロ撲滅に向けた対応策を問われたマイケル・ヘイデンが、「この際、大規模な盗聴をやりましょう」とささやいた。まさに悪魔のささやきですね。それが、ブッシュ政権後にもどんどん肥大化して、次のオバマ大統領のときもこれが受け継がれたということです。この点、イギリスは実は、もっとアメリカよりも盗聴規制が緩くて、裁判所の令状もなくして行政府の長の判断で通信傍受というのできるということです。

### あなたが知らないうちに、個人情報集積される

これまでお話したのは割と古典的で、政府というのは、やはりどの国にかかわらず非合法的なこ

とも含めて、いろいろなことをやるものだねと改めて思わせる権力乱用の問題ですね。しかしながら、時代は超高速で変化しております。政府が、あるいはだれかが、意図をもって個人情報収集するという図式とはまた違い、私たちが気づかないうちに、いろいろな情報がすべて漏えいし、抜き取られ、集積されているという社会が私たちの前にたち現れている現実を目を向けなければなりません。ビッグデータの時代ならではの新たな問題です。いま、地球上でインターネットに接続している機器の数は10億台と想定されています。それで、既に世界の総人口というのは90億ぐらいありますけれども、これはもっともっと、これからも幾何級数的に情報量は伸びていこう。1970年でしたか、アルビン・トフラーという人が『第三の波』というベストセラーを書き、情報化社会が出てきて脱産業化社会に行くに違いないと予言しました。トフラーさんの本をいま読み返すと、まことに牧歌的な未来社会の景色だと言わざるを得ませんね。

最近のアメリカの新聞に載っていましたが、「F A G A」、これは何かというと、フェイスブック、アップル、グーグル、アマゾンですね。これにマイクロソフトを合わせると、そうした巨大IT関連企業の株式時価総額は計3.6兆ドルという途方もない規模になっている。彼らが扱う情報量、まさにどれだけのギガバイトになるのか。考えられないような量の情報が、四六時中飛び回っているという時代でもあるわけであります。専門家によると、今でも1人当たり150個のセンサーが虚空に向けて発信を続けている、スマホやグーグル検索や、GPSを当たり前のように使っている中で、自分が好むか好まざるにかかわらず、その個人情報が自動的に収集され、蓄積されているという世界に生きている。

わが国では第四次産業革命が喧伝されております。「IoT」ということも最近をよく聞きますね。ドローンも次々と小さなもの、本当に小さな蚊かハエみたいなドローンが暮らしの中に定着して、生活は豊かで便利になるかわりに、その家庭の個人情報がクラウドなどに集積されていくというようなことさえ、現実になりつつある。かつて、SFと言うと「サイエンス・フィクション」でしたが、いまや「サイエンス・ファクト」。もうフィクションではないのですね。

盗聴という英語はふつう、ワイヤタッピングあるいはバグとか言いますが、これは意図的に盗聴することを意味します。これに対して、イーブズドロップという言葉もあります。イーブズドロップというのは「立ち聞き」ですね。思いもよらず、聞いてしまった、というやつです。でも、現代では、その境目は果てしなくぼやけている。ビッグデータというのは基本的にイーブズドロップです。何気なく莫大なデータを解析すると、「えっ、こんなのが入っちゃった」というのがあるわけですね。それは意図的ではないけれども、現代流のイーブズドロップではないかという議論も出ています。そこに意図があるなしにかかわらず、いろいろな雑音(ノイズ)も含めて集積されていく。

ブルース・シャナイアーというジャーナリストに『超監視社会』という本があります。この中で彼が提起している問題はかなり深刻です。クレジットカードとポイントカードのデータがあれば、この人は、いつもどのような食料品を買って、どんなアルコールを飲んでいて、どういう店で外食したというのが全部わかってしまう。ウェブサイトのアクセスを見れば、どのような医学用語を検索したかということで、どんな持病なのかも推定できる。どんな怪我をしているなとい

うのもわかってしまう。アマゾンの例、さきほど星先生からも御紹介がありましたけれども、まさに、勝手に情報はわりして集めなくとも、次々と入ってきてしまう。やろうと思えば、ある人の思想傾向から、食べ物の性向から、いろいろな個人データが全部わかってしまうということです。例えばレストランで注文したメニュー、あるいは夕方のジョギングのときの脈拍、ラブレターにどんなことを書いたのかということまで知られてしまう。これはたまりませんね。フェイスブックで「いいね」とボタンを押せば、その新たな情報がまた追加される。

グーグルのCEOでありましたエリック・シュミットという人が2013年、今から5年ほど前にこんなことを言っています。「私たちは、あなたが今何を考えているかも大体知っている。これまでどこへ行ったかも知っている」。つまり、グーグルを検索したら最後、すべての情報が自動的に抜き取られてしまうということなんですね。



### 国民の利便か公安目的か 「顔認証」 先進国・中国

情報集積という問題で、とくに注意を払わなくてはならないのは、ロシアや中国、なかんずく中国であろうと私は思います。中国はAI技術の急進展で、先ほどもお話がありましたが、顔認証が大変進んでおります。そして、例えばことしの2月からは、中国の警察は眼鏡に装着した超小型の、いわゆる携帯型顔認証システムというものを導入しております。そして、今の中国共産党の一党支配、習近平氏による強権支配のもとで個人データを公安目的で活用していく。反体制活動家のあぶり出しはもちろんでしょうが、交通事故の監視等にも使ったりする。それだけではない。中国ではマネーレス社会が急速に進んでいますから、顔認証によって、アリババによるアリペイが行き渡り、まったく新たな消費社会を形成しつつある。すべてが顔認証だけで支払いができて、スーパーのレジで財布からお金を払うようなことは消えつつある。驚くべき近未来社会が中国の都市部ではすでに実現しているということですね。このことが、国民の利便にかなうのか、実は巨大な独裁型情報管理国家への過程なのか、そのところの見分けはなかなか難しいのですが。

最近、例えば都内でも「ららぽーと豊洲店」という大型ショッピングセンターが顔認証のシステムを導入した。これは一部のメディアでも騒取り上げられましたが、消費者がどういう購買行動をするのか、お客を顔認証で解析して情報を集積し、それをマーケティングに役立てようということなのでしょう。いわゆる顔認証の画像の分析ソフトを使ってのことですが、こうした例

に限らないことですが、その情報が別の目的で使われることはないのか、という議論は国内ではあまり進んでいませんね。ただ、これもいろいろな形で法整備ができていけば、必ずしも危険な面ばかりではないでしょう。そこはかなりニュートラルに見ていく必要があると思います。

もはや、どこにも諜報員はいない。密告者もない。自分から進んでプライバシー情報を、ウェブ空間を通してせっせと発信している。国家による権力乱用を厳しく監視していくのは、ジャーナリズムの大きな使命であると思いますが、科学技術の飛躍的な発展に伴って、プライバシーと公益保護をめぐるはこれまでは違う構図がどんどん立ち上がってきている。そのことから目をそらさず、私たちはきちんと認識する必要があると思います。とりあえず、私の報告はそこまでとさせていただきます。ご清聴ありがとうございました。(拍手)

## 質疑応答

### 超監視社会における公的機関の情報収集に関するガバナンスについて

質問に答える前にひとこと。私も長い新聞記者生活を振り返ってみると、正確な情報伝達がメディアの役割だとすると、まさにメディアが「中間項」として機能することを期待されてきたという思いが強いわけです。ある情報をプロフェッショナルな視点から記者、編集者が味付けしたり解釈したりしながら、新聞であれば次の日の紙面の一番手に何を持ってくるか、そういう価値のヒエラルヒーを判断していくというのはメディアの側が主導権を握ってきたわけですね。

しかし、今の世の中では、ウェブ空間を中心に縦横に情報が飛び交う。新聞などの伝統的なメディアを媒介せずとも、直接、情報は自分たちで得るというスタイルが増えてくる。いわゆる「ミイ・メディア」の登場ですね。そうすると、もうメディアのような「中間項」はいらない、という雰囲気が多分出てきていると思うのです。ウェブ空間で飛び交っている情報も雑多で、我々もそれを活用することはありますけれども、なかには相当にいいかげんな噂話が、全く精査もされないまま、フィルターにかけられないまま飛び交い、いつのまにか「事実」とみなされるといいう危険がつきまとう。こうした情報をどこか政府や権威が統制していくというのは、お隣の中国なんかはできるかもしれませんが、日本ではあり得ないと思います。

どこかで話した内容が、たちどころに誰かによってフェイスブックなどのウェブ上にアップされ、世界中に拡散する。これは、民主主義国家である以上、上からの規制をかけてとどめようがない。いわゆる「ランナウェイ・グローバリゼーション」もそうですが、実体経済の裏付けのないマネーが世界中を瞬時に駆け回っているのと同じように、そうした「行き過ぎ」に歯止めをかけるのは難しい。私たちはそういう脅威にさらされているという覚悟を持つしかありませんね。スマホは危ないから、GPS機能もすべてやめて、世界と断絶することは、中にはそういう仙人みたいな人はいるかもしれませんが、現実的な解決にはならない。無理ですよ。情報もそうだと思います。

そこで大事ななのは、情報過多社会の中で何が本物かどうかということを見極める力でしょう。言い換えるなら、デジタル社会の中におけるアナログ的な知判断力だと思います。つまりは、1かゼロかでは割り切れない社会の尊重ですね。お尋ねの公共機関の情報収集についてのガバナ

スも、だれもがうなずく決定的な指針を定めるというのは難しい。「公序良俗に照らし、人権、プライバシーに配慮して」というお題目を定めたところで、単なる倫理目標では意味がありませんね。失礼ながら、お役所の自主的なガバナンス規定はたいてい「まゆつば」ものです。そこは、まさにアナログ的な手法で、明確なひとつの答えを探し当てるのは難しいという相互理解に立って、社会（世論）とキャッチボールしながら、徐々に落ち着きどころを見出していくというプロセスを経るしかないのではないのでしょうか。

### 補足発言

きょうのお話を聞かせていただくと、何だ当たり前のことじゃないのと言われるかもしれませんが、大切なのは社会の大まかなコンセンサス、合意に基づく「バランス感覚」だと思いますね。ハイテクなツールを犯罪捜査や未然のテロの防止というものに、どうやって高度利用するかという模索は当然のことだと思うし、私はそこに共通の公益を見出す国民は結構多いと思います。もちろん、先に触れた「ビッグブラザー」のように四六時中だれかに監視されていることに不快感、危険性を覚える人も少なからずいるわけです。そのなかで妥協点、中点を見出すのは至難の業ですが、なによりも情報公開を徹底して、例えば監視カメラがなぜ、その場所に必要なのか、可能な限り公共機関が説明責任を果たすことで、社会の理解を得ていく、そうしたプロセスがきわめて大事です。

マイナンバー制度が導入されましたが、これに対しても国民総背番号制による監視強化、というネガティブな反応がある一方で、タックスイベージョン（脱税）を防ぐという観点から、公共益に資する面もあるわけですね。私もアメリカに住んでいるときはセキュリティカードというのが必需のアイテム。どこへ行っても、ホワイトハウスを担当しても、それがないとどこにもアクセスできない。最初は、大変煩わしいなと思いましたがけれども、やはり自分たちのきちっとした身元証明ができるということを考えると、これはなかなか便利でもある。たいへんアンビバレントですね、そのあたりの価値評価は。「ビッグブラザー」が支配する陰鬱な監視社会は願い下げですが、その危険性を声高に言い立てるだけでは、ジャーナリズムは公共の安全を求める社会の負託に十分にこたえているとは言えない。多様な視点で議論を深めていく必要があると思います。

## 付録 当日配付のハンドアウト

### 超監視社会をどう生きる——公益とプライバシーのはざまで

2018・3・19 警察政策学会フォーラム

木村伊量

21世紀の「1984年」。あなたのすべては監視され、記録される。ビッグデータ時代がもたらす「マス・サーベイランス社会」の功罪

★ 近代の監視社会の原型 いつでも、誰かから見られている「パノプティコン・モデル」

英国の功利主義哲学者ジェレミー・ベンサム（1748～1832）による「パノプティコン」（panopticon=pan すべて+ opticon 見る）という監獄モデルこそ監視の原型。

円形に配置された収容者のひとつひとつの牢が「多層式看守塔」に面するよう設計。囚人たちにはお互いの姿や看守が見えないが、中心にいる看守はその位置からすべての囚人を監視できる。囚人はいつも、天頂からの逆光に遮られて自分からは見えない看守を意識することになる。功利主義哲学を説いたベンサムは犯罪者らを恒常的な監視下におくことで、生産的な労働習慣を身につけさせられると考えた。鉄格子も、からだをつなぐ鎖も、重い錠前もはや不要。その方が、むしろ権力による訓育に「服従する」ことに慣れていく（魂の刑罰装置とも）。

ポストモダンの構造主義の旗手、フランスの哲学者ミシェル・フーコー（1926～1984）は、ベンサムの「パノプティコン」に着想を得て、現代社会を批判的に分析。刑罰は、残虐な刑などの身体的抑圧から、監獄などの精神的抑圧をはかるものへと変化し、人間の人格的尊厳と主体性を奪うという現代の権力構造をかたちづくる（『監獄の誕生—監視と処罰』などより）。

近代の学校、病院、監獄、工場が「一望監視システム」という同じ原理から作りあげられているというフーコーの考察。

★ 戦慄の未来社会小説「1984」 無差別監視社会のなかで、プライバシーとセキュリティの間に、どう「線引き」ができるのか

ディストピア（反ユートピア）小説の最高峰とも、反ファシズム、反全体主義のバイブルとも目される英国の作家ジョージ・オーウェル（1903～1950）の近未来小説『1984年』（1948年）。

架空の国オセアニアでは、ソ連の独裁者ヨシフ・スターリンをモデルにしたと言われる「ビッグ・



ブラザー」によって、思想、言語、家族、恋愛など市民生活のあらゆる場面が四六時中監視される。至るところに「ビッグ・ブラザーがあなたを見守っている」(BIG BROTHER IS WATCHING YOU)という言葉とともに、彼の写真が張られている。ビッグ・ブラザーが「 $2 + 2 = 5$ 」といえば、それはオセアニアでは真実となる。疑いを持つ者は「joycamp (歓喜収容所)」と呼ばれる強制収容所に入れられる。国民は「テレスクリーン」によって、敵対国の首領に対する「2分間憎悪」を強要される。小説の中の主人公で真理省記録局に勤務ウィンストン・スミスは、歴史の改ざんが仕事だが、屈従を強いる全体主義国家の横暴に不満を抱き、ついに……。

日本では、2008年に公開された吉永小百合主演の映画「母(かあ)べえ」。1937年のある日の早朝、「父(とう)べえ」は、特高警察によって検挙され、巣鴨拘置所に収監される。思想犯が国体変革を狙う危険極まりない者として白眼視される時代を描いた。

♪とんとんとんからりんと隣組……。隣組(となりぐみ)は戦時体制の銃後を守るための官主導の隣保組織で、1940年に内務省が布告した「部落會町内會等調整整備要綱」(隣組強化法)によって制度化された。戦争遂行に民間レベルで協力するための物資供出、空襲での防火・避難活動などにもあたったが、思想的な危険人物やスパイ摘発などのための地域住民の「相互監視」も目的の一つと目されてきた。

監視という行動の二面性。一つは「(ごく一部の)凶悪な人物が罪を犯さないように監視すること」であり、もう一つは「善良な市民が被害にあわないように見守ること」。これら二つの側面がうまく使い分けられれば、公共的な利益は担保されるはずだが、そもそもこうしたことは可能なのか。凶悪な人物と善良な市民とは区別できるのか。こうして、「市民の安全を守る」システムは、「すべての市民を潜在的な犯罪者(だれもが罪を犯すかもしれない可能性を持つ)」ことを前提とした「マス・サーベイランス(無差別監視)」社会として機能することになる。

つまり、ビッグデータの経済原理に従うと、どのデータが収集し、保存するかを判断するより、すべてのデータを根こそぎ収集し、保存するほうが効率的で、誰を監視すべきかより、全員を監視する方が手っ取り早い。

プライバシーの古典的な定義は「一人にしてもらう権利」(プライバシーという法的概念を確立したとされるのは米ボストンの二人の弁護士が1890年に「プライバシーへの権利」という論文を公表。当時の扇情的・イエロージャーナリズムに業を煮やして「今や生命への権利は人生を享受する権利、すなわち一人にしておいてもらう権利を意味する」と表明)。

一方、セキュリティの基本は、「けっして一人にはしないこと」。

英国では世界の CCTV (Closed-circuit television = 有線テレビ) 4000 万台のうちの 10 分の 1 が街角や地下鉄、バス車内などに配置されている (一説には 600 万台とも)。「ロンドン市内を一日歩けば、300 回は撮影されている」とも。テロの未然防止や犯罪捜査などの公共の安全確保と、個人のプライバシーをめぐる論争が続くが、2005 年に起きたロンドン同時爆破事件から「テロ対策」としてものすごいスピードで設置が進む。テロの頻発を受けて CCTV のテロ防止、犯罪捜査活用を容認する声が高まる傾向。

★ 凍りつくような超監視社会。元 CIA 職員スノーデンによる衝撃の暴露

合法、あるいは非合法的な監視はアメリカでは日常茶飯事。米政府が監視活動に費やしている金額は、判明しているだけで年間 720 億ドルにのぼる。

2013 年 6 月、米監視社会の凄まじいまでのハイテク・インテリジェンス活動、過剰な通信秘密の侵害を暴露して世界に大きな衝撃を与えたのが、元 CIA 職員で、NSA の下請け企業、ハワイ・オアフ島の「ブーズ・アレン・ハミルトン」の職員だった エドワード・スノーデン。

スノーデンは NSA の基地内で大量のトップシークレット文書をダウンロードし、USB メモリーに入れて持ち出し、それをジャーナリストたちに渡した。NSA が米国の大手通信会社バライゾンから大量の顧客データを収集していたことや、NSA や米国政府によるサイバースパイ活動は中国などにとどまらず、ドイツやフランス、日本にもおよんでいたことが明るみに。犯罪者同然のハッキング。([『スノーデン 日本への警告』、グレン・グリーンウォルド『暴露: スノーデンが私に託したファイル』などより)

2013 年 12 月、連邦裁判所判事リチャード・レオンは NSA のデータ招集が合衆国憲法を違反している可能性を提示した上で、「NSA のメタデータ大量集積による分析が実際にテロ攻撃を阻止したと言う成功例を、政府は一件も提示できていない」と結論づけた。

ウィキリークスが 2015 年 7 月に発表した資料では、NSA は少なくとも 2006 年に始まった第 1 次安倍内閣の頃から盗聴をしていたと説明、その対象だとされている 35 電話番号のリストを一部を隠した状態で公開。これらの番号は、内閣府、官房長官秘書官、日銀総裁、日銀幹部の自宅番号、財務省、経済産業省、三菱商事の天然ガス部門、三井物産の石油部門のものが含まれるという。ほかにも、盗聴の結果をもとに NSA が作成したとする日米の通商交渉や日本の地球温暖化対策に関する報告書が掲載されている。

この「スノーデン・リーク」の衝撃波は各国に及び、中国の習近平国家主席は自らをトップとする「中央ネットワーク安全・情報化指導ワーキンググループ」を直ちに創設。

そもそも、こうした監視活動が日常化したのは、2001年の9・11同時多発テロが発端。ジョージ・W・ブッシュ大統領に対応策を問われたマイケル・ヘイデン NSA 長官（空軍大将）は「令状なしの大規模な通信傍受（盗聴）」を提案。それがさらに肥大化し、オバマ政権にも引き継がれた。英国では、裁判所の令状もなしに行政府の長の判断で通信傍受が可能という、米国よりも「ゆるい」状況。

★ 気づかないうちに、あなたのすべての情報が抜き取られる

有史以来、印刷など技術の進展に伴って増え続けてきた情報量は、デジタル化で異次元の「情報爆発」の世界に入りつつある。米 IT 企業 EMC などは 2014 年に発表した調査で、13 年に 4 兆 4 千億ギガバイトだった世界のデジタル情報量が、2020 年には 10 倍の 44 兆ギガバイトにまで増えると予想している（パソコンやスマホで個人が発する写真やメールが増加。監視カメラやセンサーなど、人やモノの動きを把握してデータ化する機械も増えているため）。

現在、地球上でインターネットに接続している機器の数は、10 億台と推定。すでに世界の総人口を上回っているが、この数字は 2020 年までに 300 億台に達するとの試算もある。ひとりあたり 150 個のセンサーが付けられる社会の到来。

「IoT」社会の新たな技術が、プライバシーをおびやかす新たな脅威に。無人の小型飛行機「ドローン」は昆虫サイズのものまで登場。2015 年 9 月、総務省の「『ドローン』による撮影映像等のインターネット上の取扱いに係るガイドライン」が公表。

監視社会に関する研究の第一人者、カナダの社会学者 デイヴィッド・ライアン氏。「情報社会は必然的に監視社会であって、新たなテクノロジーに強く依存する。だが、それに加えて、監視社会とは、統合された情報インフラのおかげで、社会生活の各部門に監視が浸透するという意味でもあるのだ」「人々は、各自の個人としてのアイデンティティーが確立されるにつれて、より明確に固有な存在となったが、裏返せば、より管理し易くもなったのである」（『監視社会』より）

ウクライナ政府は 2014 年、首都キエフのある場所にたまたま居合わせた携帯電話の所有者たちに次のようなメッセージを送った。「親愛なる利用者殿、貴殿は騒乱の参加者として登録されました」。

「クレジットカードとポイントカードのデータを見れば、ある人がどのような食料品とアルコールを購入し、どういう店で外食したかがわかる。ウェブサイトのアクセス履歴を見れば、どのような医学用語を検索したかも、オンライン上で恋人を探している人や、ギャンブルをしている人もわかる」「レストランで注文したメニュー、夕方のジョギングの脈拍数、最後に書いたラブレター

の文面なども記録される……未来の世界では、あなたが店に入った瞬間に、店員に名前と住所と所得水準を知られることになる」(ブルース・シュナイアー『超監視社会 私たちのデータはどこまで見られているのか?』より)

Google は、わたし以上に、わたしの頭の中を知っている。 Google の CEO だったエリック・シュミット氏は 2013 年、「私たちは、あなたたちがいまどこにいるかを知っている。これまでどこにいたかも知っている。いま何を考えているかもだいたい知っている」

中国では、AI 技術の急進展を背景に「顔認証」が浸透。交通信号無視や公共財の盗難防止に、顔認証システムを導入。今年 2 月から中国の警察はめがねに装着して利用できる携帯型顔認証システムを導入。共産党一党支配のもとで、個人データの公安目的での活用（反体制派活動家の洗い出しなど）への歯止め論議は欠如したまま。13 億人の顔認証データにアクセス。

彩や指紋などの生体認証システムや ID カードシステム整備をめざす政府と、そのインフラ導入で利潤に群がる企業。そして、電子マネーの使用記録、携帯電話のデジタル認証、街中にある防犯カメラにいたるまで、あらゆる機関の情報管理者がわたしたちの情報を許可もなく際限なく集め、蓄積している。しかし、その情報を提供しているのはいったい誰だということか。安全や快適さ、利便さを求める、あなた自身ではないのか。

「ここには諜報員はいない。密告者もない。 プライバシーをせっせとサーバーに供給し、かけがえのない『孤独権』を蚕食されるままにしているのは、ほかならない自分自身だということに」(平田剛士『人生が見張られている！-ルポ・「孤独権」侵害の時代』より)

## ソフトターゲットテロ防止におけるカメラ画像の活用と課題

松尾 庄 一（管理運用研究部会幹事・元近畿管区警察局長）

星先生からは、「捜査におけるカメラ画像の活用と課題」という報告がありました。それに対応するものとしては、「犯罪防止におけるカメラ画像の活用と課題」ということになろうかと思いますが、論点が広がりすぎ、時間の関係等もあることから、喫緊の課題である「オリンピック・パラリンピック東京大会でのソフトターゲットテロ防止」ということで議論を進めてまいりたいと思います。

### ソフトターゲットテロ防止の基本

まず、おさらいみたいな話ですけれども、ソフトターゲットテロというのは、ハードターゲットテロに対比される言葉であります。ハードターゲットテロとは、軍事施設であるとか警察施設等の警戒・警備が厳しいターゲットへのテロです。それに対し、ソフトターゲットテロとは、商業施設、ホテル、今回のテーマであります競技場等の、相対的に警戒・警備が弱いターゲットへのテロのことです。

東京大会においては、ソフトターゲットテロが大きな脅威として捉えられているわけですが、オリンピック大会は、オープン性から、狙いやすく守りにくい特性があるといわれており、6年前のロンドン大会でも、2年前のリオデジャネイロ大会でもその防止が最大の課題の一つとなりました。

守りにくいということについては、ハードターゲットテロであれば、軍事施設や警察施設の近くに寄らないなどの自主防衛策があるわけですけれども、オリンピックではそうはいきません。むしろ、日本中、いや世界中から人が参加することを目標にしているわけですから、危険なところに近寄らないという自己防衛策がきかないというのが特徴です。他方、攻める側としては、世界各国の人々が多数参加する場所でありまして、そこでテロを敢行すれば、そういう人たちが多数犠牲になり、マスメディア等を通じて世界中にインパクトや恐怖感を与えるということで、まさにテロリストにとっては格好のターゲットがオリンピック大会だろうと思います。

そういうことで、過去、ロンドン大会やリオデジャネイロ大会では、ソフトターゲットテロを防止するためにいろいろな対策を採ったのですが、極めつけは、競技場の周囲をフェンスで囲み、さらに競技場が幾つか集まっているようなエリア、これをオリンピックパークというようですが、その周囲もフェンスで囲み、出入り口で入場者の所持品を厳重に検査しました。また、本日のテーマに関連しますが、ロンドン大会では、オリンピックパーク周囲約18kmのフェンスに、80mおきにサーチライト付きのカメラを設置したとのこと。こうすることで、競技場内部はもちろん、その周辺もテロの敢行の点では一応クリアにできたわけです。ところが、東京大会では、ロンドン大会やリオデジャネイロ大会と異なり、競技場の周辺を新たなフェンスで囲むことはしませんし、ましてや競技場等が多数集まる湾岸エリアや新国立競技場周辺をフェンスで囲むことはしません。ということは、東京大会は、ソフトターゲットテロ対策ではこれまでとは違って大きなハンディを抱えているということでもあります。

もっとも、高さ数メートルのフェンスで競技場やオリンピックエリアを囲むのは、強烈な威圧感を観客等に与えますから、それなくしてセキュリティが保てるのであればその方がいいともいえます。

### 人の目と機械の目が融合した警備

それでは、大きなハンディを抱えた中でどうすればいいのかということでもあります。

結論を先に申し上げれば、国際テロ全般の対策としては、テロリスト等の入国を水際で阻止する、テロを起こしにくい環境づくり、さらには、テロリストの所在を確認し、彼らの行動を監視することと併せて、これらの網を潜り抜けたテロリストがテロを敢行する前に、これまで我が国におきまして伝統的にとられてきた、警察官を大量動員して警戒監視し、テロの準備行為等をする不審者を発見して、警職法に基づく職務質問等の職務を執行して対応するという点であります。この方針は今回もとるわけですが、警察官を大量動員して警戒監視するという点に関しては大きな問題があります。

その1つは、人の目による警戒監視の限界ということでもあります。雑踏では、不審者というのは見つけにくいわけでありまして。逆に言うと、テロリストは雑踏の中、彼らがよくいう「人民の海」に紛れ込むわけでありまして。他方、警察官の側からすれば、長時間集中して監視することができないということがあること、また、不審者を発見する能力には個人差があるということでもあります。これについては、先ほど野田部会長の挨拶にもありましたように、見当たり捜査、すなわち、指名手配の写真を頭の中へ叩き込んで、それぞれ流儀があるようですが、その特徴点から、目の前を歩く群衆の中から指名手配されている人間を発見するという、大変すぐれた技を持つ人がいます。また、そこまで超人的ではなくても、例えば聞き込みで2人の警察官が行ったときに、同じ場面、同じ状況にあるにもかかわらず、1人はそこから犯罪の端緒を見つけるのに、もう1人は何も気がつかずに帰ってくるというようなこともあるように、発見能力には個人差があるということです。

そこで、人の目にカメラの目を加えて警戒監視に当たるということを提唱したいわけですが。カメラの目は休むことなく監視できますし、またネットワーク化し、先ほど来話題になっております顔認証等の画像解析ソフトを組み込むことによって、雑踏でも不審者を発見できる可能性が高まるという長所があります。ただし、カメラによる警戒監視はいいことばかりではありません。カメラには死角があることと、顔認証を効果的に行うには、カメラの角度、環境の照度などの特定の条件が必要になるという短所があるほかに、何よりも不審者を発見した後の対応は警察官、つまり人間にしかできないことです。

そこで、顔認証等の機能を持ったカメラの目を加えたシステムの導入、標語的に言えば「人の目とカメラの目の融合」ということが必要になるわけです。そのための条件としては、カメラ側には、先ほど簡単に申し上げたことの他に、カメラ設置地点・場所、数が有効であること、正面画像を撮影するために要所に車載型カメラ、可搬型カメラを設置すること、できるだけ死角をなくすため、警戒警察官にウェアラブルカメラを装備することなどの条件があります。

人の目の側でも——このカメラシステムは多数のカメラの画像を1カ所のオペレーションルームに集めるわけですが、そこではモニター画面を見て不審者かどうか的確に見極める能力、あるいはシステムによって不審者のアラートが鳴ったときに、本当にそれがテロに関する不審者なのかどうかを見極めるというような能力が必要になりますし、また、現場警察官に指示をする場合に、不審者の特徴等を音声で指示するだけでは、現場の警察官にはわかりにくいので、不審な状況を撮影した画像を伝送するというような工夫が要ります。

### 顔画像の撮影及び利用の許容性

これらはある意味技術的な課題ですが、法的にも社会的にもクリアすべき大きな課題が2つあります。1つは、先ほど来話題になっている公共の安全と個人のプライバシーとのバランスをとること、もう1つは、「監視社会」批判にどうこたえるかということです。

まず、プライバシーとのバランスのとり方であります。

これについてまず押さえておきたいのは、公道等の公共空間におけるプライバシー保護の程度は、個人の家の中などの私的空間に比べて低いということであります。これを前提にしたバランスのとり方ということであります。その方法として2つあるかと思えます。

1つは、星先生から御指摘のありました、判例法上の基準をクリアするやり方であります。これについて簡単に述べると、路上等の公共空間や不特定又は多数人の出入りがある店舗等、他人から容ぼうを観察されること自体は受忍せざるを得ない場所に滞在している間の撮影については、①正当な目的及び②客観的・具体的必要があるか、③設置・使用により効果があるか、④設置状況が妥当か、⑤使用方法（撮影態様）が相当か、の5要件（大阪地裁判平6.4.27より）を満たすことにより、犯罪予防活動として許容されると考えられます。

次に、これも星先生から御指摘のありました実定法上の基準、個人情報保護法の要請をクリアするやり方があろうかと思えます。

これについて詳しく述べたいと思えます。まず、オリンピックでのテロ防止のために顔撮影が許されるのかどうかということではありますが、これも星先生の報告の繰り返しになりますけれども、利用目的をできる限り特定して、特定された利用目的の達成に必要な範囲でのみ設置・利用することであれば許容されると思えます。

特定された利用目的の達成に必要な範囲内での顔画像の利用について、ひとこと述べたいと思えます（筆者注；以下は質疑応答で述べたものを本文に組み入れたものである）。

先般、ある国会議員がタクシー内で暴言を吐いた状況を車内のドライブレコーダーが記録した画像をマスコミに公表したという事案がありました。最初は、私は運転手が小遣い稼ぎにやったのだらうなと思っていたら、どうもタクシー会社がマスコミに向けて公表したということであります。これも、車内のドライブレコーダーの設置目的が車内におけるドライバーへの犯罪防止等であることを考えれば、得られた画像を第三者であるマスコミに提供するという事は、許容されるものではないし、顔画像という個人情報を扱う「事業者」としてプライバシー保護の意識が薄いといわざるをえないのではないかと思います。

## 顔認証機能の許容性

次に、顔認証機能をもたせることが、果たして許されるのかどうかということでもあります。顔認証技術とは、登録画像と撮影された顔画像とをコンピュータ処理により自動照合し、人の識別を行うものということでもあります。結論からいえば、特定された目的の達成の範囲の中でとどまるかどうかということによって判断すればよいと思います。

配布資料に私見を掲げておりますが、テロの予防の目的でカメラを設置し、顔画像を撮影することが許されるのであれば、顔認証機能があっても許容されるということです。なぜならば、顔認証の対象者をテロリスト等に厳格に限定すれば、大多数の国民にとって顔認証機能がないカメラシステムでのプライバシーへの影響と本質的には相違しないからということでもあります。

法的には、以上によりカメラ画像の活用の適法性等はクリアされると考えるのですが、これについても国民の理解を確かなものにする、あるいは無用の不安感を抱かせないようにすることから、やり過ぎの批判を招かないようにすることが、運用上は大きな留意点だろうと思います。

そのためにはどうすればいいかということでもあります。設置目的や運用の判断基準を定めた防犯カメラ設置ガイドラインを公開し、カメラの設置やその理由等を看板等で告知したり、ホームページで発信したりする。それから、顔画像については一定期間保存した後、期間経過後は確実に廃棄する旨をオープンにして実行する。顔認証を導入する場合には、宮城県の「防犯カメラの設置及び運用に関するガイドライン」の中に書いてあるように、設置目的以外で画像の加工等を行わない旨を設置運用要領に記すというような配慮が必要になるかと思えます。

## 顔画像の第三者提供の制約

オリンピックでのテロ防止のための顔画像の活用について、もう1つ考えなければいけない問題があります。先ほど、オリンピックのエリア内の警戒監視ということを申しましたが、オリンピックの競技場周辺のエリアの中の公共空間には、警察が設置するカメラのほかに組織委員会、競技施設の管理者、鉄道事業者等が自己の事業目的を達成するために設置した、自己が管理する敷地の中ではあるが、事実上、不特定多数の者が通行できる場所を撮影するカメラが多数あります。それらの画像が一堂に集約され、警察がモニターするというのがテロ防止の観点からは理想的であります。ロンドン大会では、ロンドン警視庁に、期間中、管理者の異なる1万2000台のカメラの画像が集まったといわれております。ただ、画像を一堂に集める点では、先ほど木村先生の報告にもあったように、イギリスの場合はCCTVという、それ専用のシステムでカメラを設置しておりますから問題ないのですけれども、東京大会に適用するとなると、それぞれメーカーが違えば出力方式が異なるカメラの画像を一堂に集めるためには、仕組みというかシステムの工夫が必要になってきます。それをビデオマネジメントシステム（VMS）というわけですが、それを導入することが必要になってくるのがロンドン大会との違いであろうと思います。

顔画像の第三者提供の問題にもどります。いわゆる民間側からすれば、民間側が撮影したカメ



ラ画像を警察に提供するということが、これは第三者提供に当たるわけであり、これは法的課題は、星先生から理論的に説明がありましたが、第三者提供の制限に関する規定が個人情報保護法 23 条にあって、第三者提供は、原則として本人の事前同意を得ることが必要だと書かれています。ただし、個人データの有用性の観点から、本人の同意がなくても第三者提供できる旨の幾つかの例外が設けられております。本件のようなテロ防止のためのシステムに即して言えば、テロ防止のための顔画像の警察、すなわち、第三者への提供は、23 条にある「個人の生命・身体・財産の保護のために必要がある場合」という要件に該当すると思われま。

設置者が固有の目的のために撮影している公共空間の撮影画像を警察に提供する法的根拠を法解釈的に述べてきましたが、設置者がカメラ画像をテロ防止の必要上、警察に提供する実質的な根拠について検討したいと思います。結論からいえば、東京大会でのテロの未然防止の社会的責任が組織委員会等にはあることが根拠であります。

冒頭、競技場内部に凶器・武器等を持ち込まないように所持品検査を行うといいましたが、これを実施する警備員等の人的措置、金属探知機の設置等の物的措置及び運用の責任は施設の管理者にあります。これと同じように、それぞれの目的に沿って撮影する際、自己の管理権下にある公共空間において、テロに関する不審な人物の行動や不審物をたまたま発見した場合に警察にできるだけ速やかに録画した画像とともに通報することが、テロの未然防止の具体的な社会的責任の姿といえます。ただし、事業者等はテロ防止のためにカメラを設置しているわけではありま、また不審者等をリアルタイムで発見するというところまで求めるというのは酷であります。そこで、あらかじめ公共空間が映っている画像を警察に提供することでテロの未然防止という目的を果たす仕組みをつくるというのが現実的ですし、それは先ほど申しましたように、個人情報保護法 23 条の要件を満たすことになるのではないかと思います。

ただ、そうはいつでも、これも後々紛議を起こさないためにも、手続的保証としてパートナーシップ協定というものを締結することが、私は必須だろうと思います。民間事業者と警察の間でこの協定を結ぶことで責任の所在を明らかにし、その中で、提供画像は一定期間経過後、確実に廃棄する、目的以外に利用しないことを確約する必要があるだろうと思います。

### 「監視社会」批判への対応

最後に、「監視社会」批判に対してどう反論するのかということでもあります。「監視社会」批判の内容は、ただいま木村先生が簡潔に客観的にまとめてくれましたが、私なりに整理したのがレジュメに書いてあります。「ごく一部の人物が凶悪な罪を犯さないように監視することの問題点」は、まず、「凶悪な罪を犯す人物と善良な市民とは区別できない」ことがあります。そこから、経済原理に従うと、「どのデータを収集し、保存するかを判断するより、すべてのデータを根こそぎ収集し、保存するほうが効率的だ」となります。その結果、「誰を監視すべきか手間暇かけて判断するより、全員を監視するほうが手っ取り早い」。したがって、「すべての市民を潜在的犯罪者と見る」ということで、無差別監視社会になるということでもあります。平たく言えば、カメラシステムによって一般市民を見張るという現象が生じるわけです。

これに対する反論は、合理主義、功利主義の立場ではなかなか難しいといえますか、「そうしないと厳しい情勢の中、東京大会を安全に終わらせることはできないんだ、参加者の身の安全を守る責務が国にはあるのだ」という情緒的なものになってすれ違いになってしまうおそれがあります。そこで、批判回避ないしは反論の糸口として、次のように考えたらどうかについて提案したいと思います。

カメラシステムは、すべての市民を潜在的犯罪者と見て見張るものだという主張の一方で、ソフトターゲットテロは、誰もがテロの被害に遭う可能性がある、つまり、市民すべてが潜在的被害者ということもいえます。となると、このようなカメラシステムは一般の市民の安全を見守るものでもあるといえるのではないか。ここでのプライバシーと安全の相克については、2005年のインターネット上の自由をめぐるディベートでのシカゴ学派の経済学者の発言「自由を最優先の価値と思うかどうかは人それぞれだけど、身の安全を図るのは万人に必要ですよ」ということが取っ掛かりというか、ヒントになるのではないかと考えております。

最後、結論であります、東京大会に参加するすべての市民の身の安全のために「人の目による警戒監視に加えて、限られた時間、限られたエリアの公共空間におけるカメラによる監視、カメラ画像の活用は、適正に運用されれば、ソフトターゲットテロを防止するための有力な武器であり、社会的に許容されるのではないか。」ということであります。

以上、早口になってしまいましたけれども、私の報告を終わることにします。

### **補足発言**

私は、ネットワークカメラシステムによるソフトターゲットテロ防止ということが、果たして社会的に許容されるものであるかどうかということを中心に卑見を述べたわけですが、星先生の報告の中で、ストリートビューが10年たってこんなに——こんなにといいのかわか、受け入れられるようになった理由として、中身が知られるようになるよこんなものなのかという意識ができたことが一つ。こういう便益があるのではないかとということが知られるようになったことが一つ。それから、システムの透明性がある程度理解されたことがあると述べられました。これについては、ネットワークカメラシステムでもいえるのではないか。きょうは、時間の関係があって端折りましたが、このシステムを使えば、いわゆるテロの下見行動とか、あるいは物色のためのうろつき行動も検知することができるというすぐれたものであり、それはテロの防止にも十分つながるのだというような理解を得るための努力を積極的にしていかなければいけないと思います。

ただ、問題はシステムの透明性でありまして、これを余り細かく言えば、例えばこういう性能のカメラをどこそこに設置しているというようなことを言うと、テロリストに手の内をさらすわけですから、そこは言えないでしょう。けれども、可能な限りでシステムの透明性を図っていくことが、社会から許容される重要な条件だということを改めて感じた次第です。

## 付録1 当日配付のレジュメ

### ソフトターゲットテロ防止におけるカメラ画像の活用と課題

管理運用研究部会幹事 松尾庄一

#### ソフトターゲットテロ防止対策の提案

警察官を大量動員して、テロ準備行為等が疑われる不審者を発見し、職務質問等の対応を現場で行うのが基本

(限界)

- ① 雑踏では不審者を見つけにくい
- ② 人は、長時間集中して監視することができない
- ③ 不審者を発見する能力には個人差がある

そこで、

顔認証等の機能を持ったカメラの目を加えたシステムを導入する

- 人の目とカメラの目の融合 -

(限界)

- ① カメラには死角があること、
- ② 顔認証を効果的に行うには、カメラの角度、環境の照度などの特定の条件が必要
- ③ 何より、不審者発見後の職務質問等は人にしかできない。

ここにはクリアしなければならない大きな課題が二つある。

#### 第1 公共の安全の確保と個人のプライバシーの保護とのバランスのとり方

プライバシー概念のポイントは、道路等の公共空間や競技会場等の不特定多数の者が利用する空間での個人の顔画像のプライバシー保護の程度は、個人の家庭内等の私的空間でのそれに比べると相対的に低いとされている（渥美東洋、中野日善則等）ということ

##### 判例法上の基準

① 正当な目的及び②客観的・具体的必要があるか、③設置・使用により効果があるか、④設置状況が妥当か、⑤使用方法（撮影態様）が相当か、の5要件（大阪地裁判平6.4.27より）を満たすこと

##### 実定法上の基準（個人情報保護法の要請をクリアすること）

###### 1 顔撮影の許容性

顔を撮影するカメラを設置、運用するには、その利用目的をできる限り特定し（法15条1項）、原則としてその特定された利用目的の達成に必要な範囲でのみ許容される（16条1項）。

###### 2 顔認証の許容性

顔画像を登録したものと、カメラで撮影された顔画像とをコンピュータ処理により自動照合し、人の識別を行う顔認証のテクノロジーについては、テロ予防の目的でカメラを設置することが許

容されるのであれば、顔認証機能があっても許容される。

また、顔認証のテクノロジーについては、薄気味悪さや漠然とした不安感を抱く向きがあるが、対象者をテロリストやテロの準備行為等をする者に厳格に限定すれば、大多数の国民に及ぼされるプライバシーへの影響は、顔認証機能のないカメラシステムと本質的には相違しないと思われる。

### 3 顔画像の第三者提供の制約のクリア

個人情報保護法は、利用目的による制限を定めた16条の特則として、第三者提供の制限に関する規定を23条として設けた。ここでは、第三者提供は、原則として本人の事前同意を得て行うことが定められている。

ただし、個人データの有用性の観点から、本人の同意がなくても第三者提供できる旨のいくつかの例外が設けられている。

顔画像データの第三者である警察への提供は、個人情報保護法23条における「個人の生命、身体、財産の保護のために必要がある場合」という要件に該当すると思われる。

○民間が公共空間で撮影したカメラ画像をテロ防止の必要上警察に提供する場合の私見（別添「ネットワークカメラシステムに関する法的諸問題」参照）

### 4 運用上の留意点

「やりすぎ」との批判を招かないように、

○防犯カメラ条例や防犯カメラ設置ガイドライン等の運用規定等を定めて公開する。

○カメラを設置している事実やその理由等を看板による告知、ホームページによる発信等によりオープンに説明する。

○顔画像については、一定期間保存したのち、期間経過後は確実に廃棄する旨、オープンにする。

○顔認識等のシステムを導入する場合には、その設置目的以外で画像の加工等を行わない旨を運用規程等に記載する。参照) 宮城県「防犯カメラの設置及び運用に関するガイドライン」(平成28年10月制定)。

○各事業者が警察に画像を提供する際には、パートナーシップ協定を結ぶなど根拠を明確にする。また、その中で目的外利用をしないことを警察が提供者に確約することで、目的外利用の禁止の要請を果たすことになるとと思われる。

## 第2 「監視社会」への批判

ごく一部の人物が凶悪な罪を犯さないように監視する際の問題点は、凶悪な罪を犯す人物と善良な市民とは区別できないこと

経済原理に従うと、どのデータを収集し、保存するかを判断するより、すべてのデータを根こそぎ収集し、保存するほうが効率的となり、誰を監視すべきか判断するより、全員を監視する方が手っ取り早いということで、無差別監視社会になるおそれがある。

(木村伊量 乃木坂スクール後期第13回での発言)

他方、ソフトターゲットテロにより、誰もがテロの被害にあう可能性がある、つまり、国民す

べてが潜在的被害者である状況の中で、公共空間の安全を確保するにはどうしたらよいかは喫緊の課題

シカゴ学派のある経済学者が、2005年、インターネット上の自由についてのディベートで次のように述べている。(池田純一 「ウェブ文明論」新潮選書より)

「自由を最優先の価値と思うかどうかは人それぞれだけど、身の安全を図るのは万人に必要ですよ。」

限られた時間、限られたエリアの公共空間におけるカメラによる監視は、適正に運用されれば、ソフトターゲットテロを防止するためやむを得ないとの考えは社会的に受け入れられるのではないか。

## 付録2 配付資料

### ネットワークカメラシステムに関する法的諸問題

平成30年3月19日

管理運用研究部会幹事 松尾庄一

以下の論考は、『防犯カメラ・ドライブレコーダー等による撮影の許容性と犯罪捜査・刑事司法における適法性の判断』 星周一郎 警察学論集第70巻（2017年）第11号を参考にした。

#### カメラ顔画像撮影の法的根拠に関する基本的視座

捜査の一環としての撮影とは別に、行政活動（個人の生命・身体・財産の保護及び犯罪の予防・鎮圧）の一環としての撮影がある。

##### 設置主体と法的根拠

警察設置の街頭カメラの設置・運用の根拠～警察法2条規定する責務

民間の防犯カメラの設置・運用の根拠～民法上の所有権ないしは判例（最判昭52.12.13, 最判昭54.10.30等）において認められてきた施設管理権

#### カメラ顔画像取得（撮影）・保存・利用の必要性

1 選手村、競技会場等の施設内部は、管理者が、管理権（業務上の必要性）を根拠にそれぞれの事業目的の遂行のため設置し、目的の範囲内で顔画像取得・保存・利用できる。

2 道路等の公共空間は、警察、オリンピック組織委員会(TOCOG)、地方自治体、鉄道会社等が、それぞれの目的の範囲内で顔画像取得・保存・利用できる。

##### それぞれの目的（例示）

警察～テロの未然防止及び雑踏事故防止等のため

TOCOG～競技の安全かつ円滑な運営を行うため群衆管理や混雑防止のため

地方自治体～地域の安全確保のため

鉄道会社～鉄道の安全運行のため

#### 犯罪予防のための顔画像取得（撮影）・保存・利用の許容性

○根本的課題としては、カメラシステムは、公共の安全確保と国民のプライバシー保護とのバランスをとらなければならないことが挙げられる。ある使用方法が社会的に許容されるとする価値判断を支えるのが公共の安全、許容されないとする価値判断を支えるのがプライバシーの概念

なお、道路等の公共空間や競技会場等の不特定多数の者が利用する空間での個人の顔画像のプライバシー保護の程度は、個人の家庭内等の私的空間でのそれに比べると相対的に低いとされている（渥美東洋、中野目善則等）。

○路上等の公共空間や不特定又は多数人の出入りがある店舗等、他人から容ぼうを観察されること自体は受忍せざるを得ない場所に滞在している間の撮影については、①正当な目的及び②客観的・具体的必要があるか、③設置・使用により効果があるか、④設置状況が妥当か、⑤使用方法（撮影態様）が相当か、の5要件（大阪地裁判平6.4.27より）を満たすことにより、犯罪予防活動として許容されると考える。

## 個人情報保護法の要請をクリアすることでバランスをとる

### 1 顔撮影の許容性

個人情報に当たる映像を撮影するカメラを設置、運用する場合、ごく大雑把に言えば、その利用目的をできる限り特定し（法15条1項）、原則としてその特定された利用目的の達成に必要な範囲でのみ許容される（16条1項）。

### 2 顔認証の許容性

特定人の顔画像やその特徴を記した識別データ（対照データ）を登録したものと、カメラで撮影された顔画像や識別データ（対照データ）とを、コンピュータ処理により自動照合し、当該特定人の識別を行う顔認証のテクノロジーについては、テロの予防の目的でカメラを設置することが許容されるのであれば、顔認証機能があっても、「できる限り特定された利用目的」として許容されるであろう。

また、顔認証のテクノロジーについては、薄気味悪さや漠然とした不安感を抱く向きがあるが、対象者をテロリストやテロの準備行為をする者に厳格に限定すれば、大多数の国民にとってプレーンなカメラシステムにおいて及ぼされるプライバシーへの影響と本質的には相違しないであろう（松尾私見）。

### 3 運用上の留意点

法的には上記のとおりとしても、「やりすぎ」との批判を招かないように、その利用目的を、原則としてあらかじめ公表するか、本人に通知または公表するという基本構図に則った運用を行う必要がある。

具体的には、これらを具体化した判断基準を織り込んだ、防犯カメラ条例や防犯カメラ設置ガイドライン等の運用規定等を定めて公開することなどで許容限界を明らかにし、適正な設置・運用を確保すると同時に、カメラを設置している事実やその理由等を看板による告知、ホームページによる発信等によりオープンに説明することで国民とのコミュニケーションをとり、また、国民一般の理解を含めていくことが求められる。

特に顔画像については、一定期間保存したのち、期間経過後は確実に廃棄する旨、オープンにする必要がある。

なお、宮城県「防犯カメラの設置及び運用に関するガイドライン」（平成28年10月制定）では保存した画像の不必要な複製や加工を行わないことを保障するため、「防犯カメラの設置に際し、顔認識等のシステムを導入する場合には、その設置目的以外で画像の加工等を行わない旨を、設置・運用要領に記載すること」とあるのは参考になる。

#### 4 顔画像の第三者提供の制約

個人情報に関しては、それが第三者に提供された場合、提供後の使用が不明な状態となり、本人に不測の不利益をもたらすおそれが増大する。そのため、個人情報保護法は、当該個人情報が、個人情報データベース等を構成する個人データに該当する場合には、利用目的による制限を定めた16条の特則として、第三者提供の制限に関する規定を23条として設けた。ここでは、第三者提供は、原則として本人の事前同意を得て行うことが定められている。

ただし、個人データの有用性の観点から、本人の同意がなくても第三者提供できる旨のいくつかの例外が設けられている。

##### ○民間が公共空間で撮影したカメラ画像をテロ防止の必要上警察に提供する場合（私見）

オリンピックに関するテロの未然防止については、警察の手だけで行うことは不可能であり、広く国民の協力を求めなければ実現が困難である。特に、TOCOG、各施設設置者等の事業者は、テロの未然防止の社会的責任があるとされている。

具体的には、それぞれの目的に沿って撮影する際、自己の管理権下にある公共空間において、テロに関する不審な人物の行動や不審物を発見した場合に警察にできるだけ速やかに録画した画像とともに通報することなどで協力することが求められる。

しかし、事業者が膨大なカメラ画像の中からいつ現れるかわからない不審者等をリアルタイムで発見することまで求めるのは、事業者のコストや人員のリソースの点で無理がある。そこで、公共空間が映っている画像を予め警察に提供することでテロの未然防止という目的を果たす仕組みを作ることが現実的だと思われる。

また、その際の顔画像データの第三者である警察提供は、個人情報保護法23条における「個人の生命、身体、財産の保護のために必要がある場合」という要件に該当するであろう。

この際、各事業者が警察に画像を提供する根拠としてパートナーシップ協定を結ぶなどの措置をとることが必要であろう。また、その中で目的外利用をしないことを警察が提供者に確約することで、個人情報保護法の要請を果たすことになると思われる。

(参考)

##### ○民間のカメラ画像を捜査の必要上警察に提供する場合（星論文）

防犯カメラの管理者が、事件捜査に協力するため捜査機関に捜査に関する映像を提供することは、「法令に基づく場合」として許容される。

防犯を目的として設置された街頭カメラの場合、その防犯には、犯罪が発生した場合の捜査の手掛かりとなりうる映像の提供が含まれていると考えることができる。そうだとすれば、警察へ犯罪被害等を通報する際に、当該映像を提供することは、「利用目的の達成に必要な範囲」での本来的な利用であるともいえ、それに基づく提供が個人情報保護法上は認められることになる。

以上



