犯罪予防や安全確保のためのカメラ画像利用に関する有識者検討会（第２回）
議事概要

１　日時　令和４年３月９日 10 時 00 分～12 時 00 分

２　場所　Ｗｅｂ会議による開催

３．出席者
（１）構成員（敬称略　五十音順）
生貝構成員、石井構成員、遠藤構成員、菊池構成員、宍戸構成員、新保構成員、巽構成員、星構成員、森構成員、山本構成員（以上１０名）
（２）個人情報保護委員会
丹野委員長、福浦事務局長、佐脇審議官、三原次長、赤阪参事官、矢田企画官 他

４．議事
（１）事務局説明
・事務局より、資料１及び資料２に基づき説明があった。
（２）カメラ画像の利用に関する不法行為法上の評価について（森構成員、遠藤構成員）
・森構成員より資料３について、遠藤構成員より資料４について、それぞれ説明があった。
（３）意見交換
各構成員からの主な意見は以下のとおり。

個人情報保護法と不法行為法の関係

○　資料４・７頁における「個人情報保護法違反の行為が不法行為を成立させるかというよりも、問題となっている具体的な権利利益侵害行為を防止することを目的としているかどうかが重要な視点だと思われる」との説明について、特定の個人情報保護法の条文ないしは規律が、例えば肖像権とかプライバシーといった民事法上も保護されている利益を保護することを目的としているのかどうか、個人情報保護法の具体的な規律が何を目的としているのかが重要であるということであり、抽象的に個人情報保護法への違反行為と不法行為との関係を議論するというよりは、個人情報保護法の個別の規定の目的を、不法行為法において判断することとなるとの趣旨であれば、その通りだと思う。
○　市長が前科情報を第三者に提供した事件や、大学が講演参加者の名簿を警察に提供した事件などは、個人情報保護法上では適法だが、プライバシー侵害を惹起しているため、民事法上又は国家賠償法上は違法になるという説明がされることがある。この場

合、個人情報保護法がプライバシー的なものからは切り離されて解釈されているようにも見えるが、そのような事例であっても、個人情報保護法上違法であると言えないか。

本件検討会のスコープに引き付けていうと、第１回の事務局説明において、防犯カメラにより撮影をすることは、適正取得義務（法第20条第1項）に違反する可能性があるとされていたが、Q&Aにおいては、当該条文には触れずに、防犯カメラにより撮影されていることを被撮影者が分かるような措置を取ることが「望ましい」という書き方がされている。

適正取得義務という条文が、プライバシーや肖像権等の保護を取り込んだ条文として解釈されるべきなのか、それともプライバシーや肖像権等の保護とは切り離して考えた上で、個人情報保護法の外でプライバシー侵害を捕捉すべきものなのかという点が、今回の検討会では問題になると考えている。

○　制定当初の個人情報保護法は、個人情報についての取締法規であり、個人情報の中に機微性における区別はなかった。

平成27年改正法により、要配慮個人情報の規律が課され、一定の機微性について配慮することになった。また、セキュリティーや安全管理措置との関係で、機微性に応じた管理が義務付けられるようになり、令和２年改正法で不適正利用の禁止（法第19条）も定められた。しかし、元は個人情報を区別せず、機微性とは関係なく、広く薄く個人情報について規制をかけていくことが趣旨であり、その性質は今でも強く残っている。

第三者提供の際の同意取得義務（法第27条第１項）では、法令上の定めがあるときは例外になり、警察が刑事訴訟法に基づいて捜査関係事項照会で照会を求めたときや、弁護士会が弁護士会照会で照会を求めたときに、当該の照会権限に対応した回答義務があるため、提供しても個人情報保護法違反には当たらないと考えられる。しかし、プライバシー侵害になるかは、情報の性質等に応じた総合判断を要する。そこで、機微性や、追跡、萎縮の問題がある顔認識データは、個人情報保護法違反とプライバシー侵害の判断が最も分かれる問題ではないか。

○　不法行為法上、取締法規違反との関係が問題となる場面では、不法行為法の一般法と特別法の関係で議論されることが多い。例えば知的財産法との関係では、明示的に知的財産法における不法行為と民法上の不法行為が一般法と特別法との関係にあるという形の整理をした上で、相互の関係が議論されている。しかし個人情報保護法が、民法上、特別法として議論されるということは多くはない。現状の議論を見ると、個人情報保護法違反と不法行為の成立を区別するという見解が一般的だと考えられる。その上で、例えば消費者法の議論等でもあるように、エンフォースメント手段として、同じような行為がなされたときに法によって結論が異なることが適切かどうかという点も含め検討する必要があると考える。

○　監視カメラの場合に、個人情報保護法上は適法に取得・利用・提供されているため個人情報保護委員会はエンフォースメントの手段を発動しないが、プライバシー侵害が起こった場合は当事者間での解決に任せるということでよいのか気にかかる。
自己情報の開示請求について、特定の個人が識別できない場合でも、なお個人の権利利益を害するおそれがあるものは、不開示情報になる。個人情報保護法制上も、個人識別性に起因するものではない利益がすでに保護されているのではないか。

○　適正取得義務（法第20条第１項）には、「偽りその他不正の手段」による取得を禁じることで、広めに網がかかっている。従来の解説でも、隠し撮りをすることは適正取得義務違反の可能性があると言われている。そこで、適正取得義務の条文の中では、肖像権・プライバシーに関する利益も保護されている利益と解釈して、個人情報保護委員会も何らかの形でエンフォースメントができるという前提の議論を組み立てた方が良いのではないか。

○　個人情報保護法の目的等をどう理解するのかに関係する。当初は行政的な取締法規としてスタートしたとも解されるが、要配慮個人情報等の概念が追加されるなど、目的やアイデンティティが個人の尊厳も含むプライバシー方向に傾いてきている。法解釈のアプローチとして、立法者意思説や原意主義ではなく、法律意思説で考えていくべきではないか。

○　情報取得の方法こそがプライバシー侵害の場面で問題になっているため、適正取得義務（法第20条第１項）の考慮に取り込むべきである。
しかし、顔認識データのような追跡力の高い情報の場合と、それ以外の情報の場合のように、情報の性質が違う場合に、機微性の高い情報であれば適正取得義務違反（法第20条第１項）だが、それ以外の情報の場合は適正取得義務違反ではないと言えるのか。また、広くプライバシー侵害を防止するような形で個人情報保護法の解釈をすると、かなり厳しい規律になっていく。ガイドラインで詳細に適正取得義務違反の例などを書いていくと、事業者等にとっては敷居が高くなりすぎないか。

○　個人情報保護法と不法行為法上の比較について、法律、法目的が違えば、結論も違ってくる。適正な取得の解釈の中で、不法行為法上の解釈を考慮するという場面は十分にあるだろう。ただし、不法行為法はあくまで総合考慮に基づいて個別の事案によって判断するというものであり、抽出できるのは要素でしかないのではないか。

顔識別機能付きカメラを利用することが有効かつ必要であると考えられる場面

○　資料２について、顔識別機能付きカメラシステムを利用することが有効かつ必要であると考えられる場面については、防犯、法執行、安全保障、安全確保、公衆衛生、災害の防止、風景撮影、テロ対策、法令に基づく場合の9つに分け考えることができる。
防犯の具体例としては、万引き防止などの民間事業者による警備目的での利用、商店街や地域コミュニティによる利用、警察や公的機関によるカメラの設置、街灯の緊急

防犯システムでスーパー防犯灯、個人のホームセキュリティなどがある。
法執行は、自動速度取締装置や、自動ナンバー読み取りシステム（Nシステム）。
安全保障については、入国管理や天頂衛星の衛星搭載カメラ。
テロ対策については、これらについて複数が関わってくる。
安全確保については、民間事業者による情報セキュリティーの確保。これは個人情報保護法の安全管理措置義務を達成するため、自主的に個人情報取扱事業者の義務を果たす上での安全確保や、取引の過程におけるバイオメトリクスを用いた認証を行うことによる取引の安全確保のための利用､輸送機関における運行確保･安全確保がある。
また、公共交通機関が運行安全確保目的以外の安全確保のために顔識別機能付きカメラを利用することも最近多々問題になっている。
公衆衛生は、従来は検疫目的でのサーモグラフィカメラが問題になってきていたが、現在は感染拡大防止のための様々な場面でのカメラの利用がある。
災害の防止はダム、河川、道路、海岸などの公物管理。
風景撮影は、お天気カメラ、ウェブカメラ、リアルライブストリーミングなど。
テロ対策は、国の基準としては、カメラと関係するものは大きく５つで、出入国管理の関連情報の収集、ハイジャック防止、NBC、核・生物・化学テロ対策、国内重要施設の重要インフラ警備において従来からカメラが用いられてきている。
法令に基づく場合は、医療系施設が典型例。精神保健福祉法に基づく監視義務の履行や検疫法に基づく隔離措置の実効性確保のための利用などが問題になる可能性がある
この点について興味深い報告書として、２月下旬にイギリスのICOがCCTVガイダンス（Guidance on video surveillance）を公表しており、このガイダンスは資料２の「事業者に対応が求められる事項」を検討するに当たっても非常に興味深い。この中では目的や設置場所、利用する措置について分類しており、自動ナンバープレート識別（AMPR）や身体装着型ビデオ（BWV）、GoProなどのアクションカメラ、スマートドアベルなどを取り上げている。また、車両内監視については、オーストラリアのタクシーではフロントガラスの半分がプライバシーポリシーで埋まっており今後海外の調査が必要であれば面白い例となるのではないか。
一方、ロボットに装着されるカメラは、日本が先んじて今後様々な場面で利用されるのではないか。

○　最判平成17年における考慮要素から、利用できる要素を挙げてみてはどうか。
例えば撮影場所については、トイレなどカメラを設置するとあまりにもプライバシー的に問題がある場所も考えられる。EDPBのガイドラインの中で、データ主体の合理的な期待を裏切るような使い方は望ましくないという記載があり、その例のひとつとしてトイレが挙げられている。場所自体に非常に機微性がある点も考慮する必要がある。

○　撮影態様、設置場所については、過去の裁判例を参考にできるだろう。設置場所に関するポイントとして、公共空間か否かという点がある。設備の管理者が、設備の保護、

保安の目的のためにカメラを設置することができる空間と、そうではない公共の誰もが通る空間については、大きな区別がある。

○　行動追跡によってプライバシー侵害性が飛躍的に高まるというのは御指摘のとおり。しかし行動追跡は無益なプライバシー侵害だけというものでもない。例えば昨年の白金高輪での硫酸事件のような事件など、さらなる被害防止のためにはある程度の追跡も必要になると考える。窃盗の事案などでも、場合によっては店舗ごとにある程度の追跡ができないと、さらなる犯罪被害の防止にもつながらない。どのようにバランスを取るかが課題。

事業者に対応が求められる事項

○　事業者に対応が求められる事項ではなく、事業者に対応を求めるために必要な事項を決める、すなわち運用基準の明確化がまずは必要。事業者側がどういうふうに対応してよいかということがなかなか分かりづらい。撮影した画像の取扱いに応じて運用基準を明確にしてもいいのではないか。識別性、照合性、検索性、自動処理の4つの観点から、運用基準は明確にできると考えている。

識別性については､個人の肖像にとどまらず生体情報の特徴量も含めることが必要で、これは個人識別符号として規定されている。

照合性については、他のデータベースとの照合性についてである。例えば医療記録、納税記録、犯罪記録、投票とか政治団体への加入とか記録といったデータとの照合によってどのような問題が生ずるのかという点。

検索性については、特徴量を抽出して個人データとしての顔情報の取得、それにより検索性が容易になっている。とりわけAIを用いて検索性は飛躍的に高まっている。

自動処理については、日本における課題としては、GDPR第22条に基づく自動化された決定との関係における問題、いわゆるプロファイリングとの関係における問題がなかなか解決できない部分だろう。自動処理について、提供も含めてGDPR第22条に基づくような自動化された意思決定との関係におけるこのような監視、カメラの利用というものについては運用の基準をどういう形で明確化していくのか。法的には個人情報保護法に根拠がないため、どのようにこれを求めていくのかということは今後の課題である。

○　比例性が非常に厳密に問われることになるため、設置の目的が厳格に問われることになる。例えばテロや重大犯罪については権利侵害性が高かったとしても許容し得るのだろう。

これに加えて、設置場所の固有のリスクをきちんと具体化して、洗い出していく。重大犯罪、テロ等に加えて、場所の固有のリスクをどのように捉えていくかが考えられる論点。

店舗型カメラにおける透明性は消費者に対して選択権を与えるために必要となるが、

公共空間の場合には選択が事実上できないため、透明性の目的が異なる。顔識別カメラの設置は伝える必要があるが、設置場所等をどこまで詳細に書くべきか、カメラを設置する目的との関係で議論しなければいけない。

○　他機関との連携が非常に重要になってくるのではないか。例えば、登録の必要性がなくなった場合のデータの消去をどう担保していくのか。最判平成6年2月8日（ノンフィクション「逆転」事件）は「更生を妨げられない利益」を認めている。名古屋地判令和3年1月18日では、DNA型記録の抹消請求が認められている。

必要性がなくなった場合のデータの消去を担保するには、例えば警察あるいは法務省との情報連携、不起訴や無罪になった場合の情報が的確に伝わる必要がある。情報連携をどのように担保していくかが重要。

○　顔認識の技術に加えて、例えばAIを使った不審者予測や不審な行動に対するフラグ付与などを同時に行う場合には、AI倫理に関わる問題がプラスアルファとして出てくる。この点は誤登録等の問題も出てくる。例えば障碍者のような、多数者とは少々異なる動きをしていると、何か異常な行動をしていると検知されてしまう可能性もある。このようなリスクをどう防いでいくのかは重要となる。

○　EDPBのガイドラインの中で、バイオメトリックデータを取り扱うときのリスクを最小化するための対策案がまとめられており、その中で、取扱いに適法な根拠がなくなったような場合には生データを削除することが望ましい等が記載されている。国外の資料も参考にしていただきつつ、対応が求められる事項を整理する必要があるだろう。

顔識別機能付きカメラによる権利侵害性

○　コンビニの防犯カメラも違法になったケースは存在する。撮影行為自体の適法性を問題にするのであるが、撮影方法、撮影した後の画像の管理方法次第では撮影行為自体が肖像権侵害になり得る。万引き防止というのは、目的においては正当だが、それでだけではなく総合判断で決まる。

○　顔認識機能付きカメラによる撮影は、権利侵害性が従来よりも強いと考えるべきではないか。裁判例でも、容貌にピントを合わせることが尊厳との関係で重く捉えられてきている。顔認識も顔にピントを当てる必要があるため、これまでの裁判例が参考になる。

プロファイリングの可能性については個人と紐付けた形で、様々な属性分析が技術的に可能になっていることから、萎縮効果があるのではないか。

○　プロファイリングについては人種差別や性別といったさまざまな情報を引き出すことができる。目的を達成するために必要なデータ処理、解析はどこまでかを情報の機微性も考慮しながら考えていく必要がある。

○　情報の高精度化、画像の高精細化によって侵害の程度は高くなる。他方で、個人データであればデータ内容の正確性の確保の義務（法第22条）があり、また不鮮明な画像

を使用し誤認識が増えれば迷惑をばらまく装置にもなる。誰の何の利益を保護するのか、どのような影響を及ぼすのか、場面ごとに即した判断をしなければいけない。
認証の自動化自体はプレーンな利用形態の１つでしかなく、自動化されると様々な目的に容易に使える点が問題なのであって、識別、認証機能自体が直ちに問題になるのではない。

○　カメラの被写体となる生活者の利益をどのように守っていくのか。何段階かあると思うが、個人データの保護に関する具体的な権利や請求権のレベル、抽象的にプライバシーと言ってきた話、さらに差別されないことや実体的な不利益、尊厳を守るためのやり方という話があり得る。これらについても整理をし、それとの関係で個人情報保護委員会がどのような権限や監視監督、あるいはモニタリングなどが求められるのかということを今後整理していく必要がある。

生活者とのコミュニケーション

○　生活者とのコミュニケーションについて、まだ議論が進んでいないように感じる。事業者としては、単なる画像の取得だけではなくて、それが個人データになっているか、なっていないかを生活者に分かるように説明する必要がある。
個人データになっている場合は、今度は本人関与義務がかかり、開示等請求に対する対応をどうやって担保していくかも必要になる。

検討すべき事項

○　欧州のAI規則案について、許容できないリスクのAIとハイリスクAIの分類をしている。許容できないリスクのAIとして公共空間におけるリアルタイムのリモート生体識別システムの使用があげられている。顔認識データを取って誰かを探すということは原則として禁止されているが、重要な目的の場合には例外の規定がある。この点は本検討会で俎上に載せるべきである。

○　顔認識やプロファイリングに基づく様々な推測が可能になるときに、バイアスの問題などの、AI特有の問題が様々な形で議論されている。AI規則案で議論されているようなデータガバナンスの論点をこの枠組みの中でどのように捕まえていくのか興味深い。

○　本日の検討で紹介された裁判例は昭和44年から平成22年まで長い期間にわたっている。その間に街頭で撮影されることの意味合いが昔と比べて相当違ってきていると考える必要があるのではないか、ここの変化をどうフォローアップしていくかが問題。

○　カメラ画像利活用ガイドブックは、据付型の店舗のカメラについてソリューション思考で策定されてきた。本検討会では、顔識別カメラの有する技術的機能の関係での整理も必要である。

○　比較衡量について、プライバシーに対立する利益の大きさとバランシングの問題と、撮影手法等の相当性の両方の議論が必要。ソリューションと機能を掛け合わせた形で、

どのような目的でどういう機能を使ってカメラ画像を取得し使用したいのかを類型化し、それぞれについてカメラを使う主体、事業者や機関にとって求められること、あるいはガバナンスが整理されればよい。

○　カメラ画像が第三者に提供されたり、あるいは関連機関同士で共有されたりして公共的な目的に役立てる場合に必要なガバナンスや、何について透明性や規律の実現が求められるのか。逆に言えば、それができるのであれば、そのようなカメラ画像の利活用が許されると考えるべきなのかを議論する必要がある。

（５）その他

事務局より今後の予定について説明があった。