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１回）
議事概要

１　日時　令和４年１月28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）
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９名）
（２）ヒアリング事業者
日本電気株式会社
デジタルプラットフォーム事業部　シニアマネージャー　山田 和弘氏
同事業部　マネージャー　今橋 晃一氏
（３）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）丹野個人情報保護委員会委員長挨拶
（２）開催要綱（案）・座長の選出について
・　事務局より資料１に基づき説明し、開催要綱（案）が承認された。
・　宍戸常寿東京大学大学院教授が座長として選出された。
（３）事務局より資料説明
・　事務局より、資料２及び資料３に基づき、説明があった。
・　各構成員からの主な意見と、事務局との質疑応答は以下のとおり。

用語の使い分けについて

○　顔識別カメラや顔認識カメラと様々な言われ方をしているが、どれが間違いでどれが正しいというものはなく、これらの用語は用途に応じて使い分けられている。例えば、ISO 2382にボキャブラリーについての定義がある。１対１で行うverificationは「検証」、本検討会の検討対象に一番近いと思われる１対Ｎで行う identification は「識別」、身体的及び振舞いなどの性質に基づき行うrecognitionは「認識」と区別されている。

○　国際的な動向との関係では EU の AI 整合規則提案において、remote biometrics identification system という用語が用いられている。biometric identification は識別と訳される。一般的に recognition と authentication の違いは必ずしも明確に分けて用いられていないことも多い。recognition は顔認識のレベルにあり、1 対 1 の認証に至る verification、authentication は認証と訳されるべきであろう。

（事務局）

今回の検討を機に、用語についても必要に応じて見直していきたい。

対象技術について

○　技術的な視点として、高画質、低照度、顔識別の精緻化、小型化による密行性などカメラによる撮影技術の高度化、また、それらの社会における普及という観点からの検討が必要になる。警備ロボット、サイバネティックアバターの利用と AI による分析も想定される。もう一点は新興技術。AI が典型的だが、生体情報の特徴量分析は文字通り検索性、体系性を有するので個人データとしての利用となる。法的視点として、この部分についてとりわけ遠隔生体識別との組合せによる識別性の向上による監視の容易性がある。これらの観点も留意した上で検討したい。

検討会のスコープについて

○　検討会のスコープについて、今回は「顔識別機能付きカメラ」の利用ということだが、カメラで取得した画像を用いて再犯リスクを評価する、それにより差別的な取扱いが生じるといった画像の利用に伴う差別問題のような、必ずしも個人情報保護法でカバーしきれているとは言い難い問題も検討会のスコープに含めてよいのか。

（事務局）

個人情報保護法においても不適正利用に含まれるものもある。それ以外についても議論のスコープを予め限定するつもりはないため、ご指摘の点もスコープに入れながらご検討いただければと考えている。

○　「犯罪予防や安全確保のためのカメラ画像利用」とあるが、「安全確保」の射程について確認したい。また、店舗に設置したカメラについては、公共空間に設置した防犯カメラの射程から外れているのか。

（事務局）

典型的にはテロや重大犯罪、あるいは万引き等の犯罪予防を当面の検討の対象としては考えている。また、公共空間も明確な定義はないと認識しており、店舗であっても、ショッピングモールなど人が自由に出入りできるところはある。店舗の規模がどれぐらいかというところでは、対象を区切りづらい。

○　登録者データを予め持っておらず、特定の公共空間に入った人を識別して追跡していくケースも射程に入るのか。追跡する相手が誰かわからないまま、ある空間の中で動いていることを識別する場合は、用語として識別と言うべきなのか、認識と言うべきなのか。それぞれの場合でリスクが変わってくるが、この人が誰かわからないまま追跡すると、これまでの Q&A においてどういう位置づけがなされているのか。

（事務局）

登録者のデータを持っていない場合に、識別とするか認識とするかは有識者からのコメントをいただいて整理していきたい。不審者やうろつきの人をカメラで捉えて自らデータベース化していくものも検討のスコープに入る。

○　民間事業者が設置する場合を検討のスコープとするのか。

（事務局）

議論はいろいろ広がり得るが、基本的なスコープは民間事業者が施設管理をしてカメラを設置している場合を念頭に置いている。

現行の Q&A について

○　資料２・８頁。法第 22 条に関する Q5-4 は、必要最小限性を取り込んで権利利益の侵害が起こらないようになっている。法第 22 条は努力義務になっているので、「必要」とまでいえるのか。

（事務局）

Q&A の中で法律上努力義務になっているところが「必要」となっている。ここはわれわれも意識して「必要がある」と書いている。顔識別データを使うからにはこういったことを求めていく必要があると考えているため Q&A のなかでこうした表現を使っている。

○　資料２・６頁目の要配慮個人情報の取得、Q1-31 で「防犯カメラの映像等で、犯罪行為が疑われる映像が映ったのみでは、要配慮個人情報には該当しない」と整理されているが、撮影している中で現行犯逮捕等の刑事手続きが行われた場合はその段階から要配慮個人情報になるのか。

（事務局）

現行犯逮捕の現場が写っているものは要配慮個人情報にあたると基本的には考えているが確認したい。

従来型の防犯カメラについて

○　技術が発展してきたときに、従来型防犯カメラの性格が変わって、顔識別をすることが当然となったら、「取得の態様から利用目的が明らか」との解釈が変わるのか。

○　顔識別をしないつもりで設置した防犯カメラであっても、カメラの外観上は顔識別が

されるか否かは認識できず、それにより自分が識別されているかもしれないと思う市民はいるのではないか。そうすると、資料２・５頁にあるような、「取得の状況から見て利用目的が明らか」（法第 21 条第４項第４号）といえる防犯カメラはもはや無いのではないか。

○　顔画像をデジタルで撮影したが顔識別を行わないときに、その後、画像から特徴量を抽出することはできるのではないか。そのような場合に利用目的の通知公表についてどう考えればいいのか。後で抽出するのであるからもちろん顔識別機能付きカメラと同様に利用目的の通知公表が必要ということか。

（事務局）

まだ顔識別機能を有している防犯カメラが一般的に普及しているとまで言えないと認識している中で、こういった解釈を示している。従来型防犯カメラに係る Q&A についても、本検討会での検討を踏まえ、必要に応じて見直していきたい。

プライバシー侵害について

○　利用目的の設定について個人情報保護法はニュートラルであり、他方、一度設定された利用目的のために必要最低限の範囲内において個人情報を取り扱うことを定めていると認識。そこで、利用目的自体は不適正利用になるようなものでなければよく、その範囲で自由に設定されているが、プライバシー侵害の裁判例では、個人情報の利用の必要性が重要視されている。プライバシー権侵害に関する裁判例においては、利用目的がどんな利用目的なのかということが考慮されている。

○　大阪地裁平成６年４月 27 日の裁判例があり現在もよく参照されるが、約 30 年経過して考え方の違いがあるのか、その枠組みに則ったやり方があるのか、考える必要がある。

○　肖像権侵害では撮影の場所等も検討の対象となっている。公共空間や店舗等の場所でも、裁判の中身が変わってくる。そのあたりも検討したい。

適正取得について

○　個人情報保護法は様々な個人情報を規律の対象にしているが、それらを均一に取り扱うことを定めるのではなく、権利利益の侵害のおそれが高い個人情報は強く保護するようにグラデーションをつけて保護している。適正取得においてもその考え方を取り入れて、顔識別機能付き防犯カメラによる場合は特別にある対応をとらなければならないとするやり方はある。

○　従来型の防犯カメラについて、本人が個人情報を取得されていることがわかる措置が望ましいと書かれているが、本人が「自分が撮られている」ということを認識することが重要というのは、識別されるのかされないのか、利用目的が分かるようにせよというのではなく、適正取得の話だと思う。そうすると、個人情報を取得されていることがわかる措置が望ましいというにとどまらず、そうした措置を講ずる必要があるといわな

ければならないのではないか。

開示請求について

○　万引犯として登録されている相手から開示請求があった場合には、施行令第５条の保有個人データに該当しない場合として扱っているのか。

（事務局）

開示請求に応じているかはケースバイケース。我々が承知している中では、渋谷プロジェクトは開示請求の手続きも定めている。

GDPR について

○　GDPR 第９条２項ｇ号の「重要な公共の利益」を理由とする取扱いについて、EU 加盟国については EU 法又は加盟国の国内法、イギリスは国内法あっての適用となる。このあたりの条文が具体的に適用されて顔識別カメラを用いた防犯目的の取扱いがなされているケースがあるか。

○　GDPR 第９条第２項第ｇ号は「求められる目的と比例的であり、データ保護の権利の本質的部分を尊重し、また、データ主体の基本的な権利及び利益の安全性を確保するための適切かつ個別の措置を定める EU 法又は加盟国の国内法に基づき、重要な公共の利益を理由とする取扱いが必要となる場合」と定めているため、EU 法又は加盟国の国内法による法律の根拠は求められていると読める。同号は、法律の根拠がありかつ「重要な公共の利益を理由とする取扱いが必要」であるときに、特別な種類の個人データの取扱いができるという趣旨なのか。

（事務局）

ご認識のとおり。EU 各国の国内法がどうなっているかは調査をしたい。

（４）事業者ヒアリング

・　日本電気株式会社より、資料４に基づき、説明があった。

・　各構成員との主な意見と、日本電気株式会社との質疑応答は以下のとおり。

○　資料４で紹介された感染症対策は、３年前は説得力なかったものの今は説得力をもった目的になった。これを踏まえて柔軟性をもった方向性を示さないといけない。顔識別技術と映像解析技術の使い方の相違があるということも勉強になった。個人情報の利活用と保護のどちらかに傾きすぎても国民の利益にならない。バランス感覚が重要。国際協調の流れもある一方、国や地域ごとの背景、時代的な背景の違いをできるかぎり反映させられる方向がいい。

○　個人の特定を行いたいときに顔の情報が一番特定しやすいのか。画像に含まれる顔以

外の情報でも個人を特定することができるのか。肖像権侵害で問題となる裁判例では、必ずしも顔が前向きに映っている画像が問題になっているわけではないためお伺いしたい。

（日本電気株式会社）

個人を特定する用途では顔識別が必要だと思う。資料４・22 頁で紹介した人物照合の技術もあるが、精度面では顔識別の精度が最も高い。物や服装の情報から識別しようとすると精度向上が難しい。現時点において個人を識別したいという用途においては、まずは顔識別。顔の向きについても、エンジンの精度の向上に伴い横向きでも個人を特定できる。しかし正面の方が精度はよいため、運用面で、できるだけ正面からの画像を利用できるようカメラの設置場所等に留意している。

○　資料４・22 頁で紹介された映像分析技術の中の人物照合技術は、HD のカメラを用いた事例だと思う。これを高画質なカメラにより行った場合は人物照合技術の精度はあがるのか。仮に人物照合技術の精度が向上し、特定個人の識別に至り得るのであれば、法的な議論にも影響する。

（日本電気株式会社）

カメラの精度向上に伴い人物照合の精度は上がる認識。ただ、どの技術を用いるか決めるには、求める精度と利用目的が鍵となる。顔認識による９９．９%の識別精度が必要なのか、それとも８０%程度の識別精度があればいいのか。ざっくり検知対象者をすくい上げることができればいいという目的であれば人物照合でも足りるが、誤認識しないように十分な配慮が必要ということであれば顔認識を用いて高精度に運用しなければならない。

（５）その他

・　事務局より、今後の予定について説明があった。

以上