

英国・米国におけるカメラ画像と 顔認識に関する動向

2017年10月5日

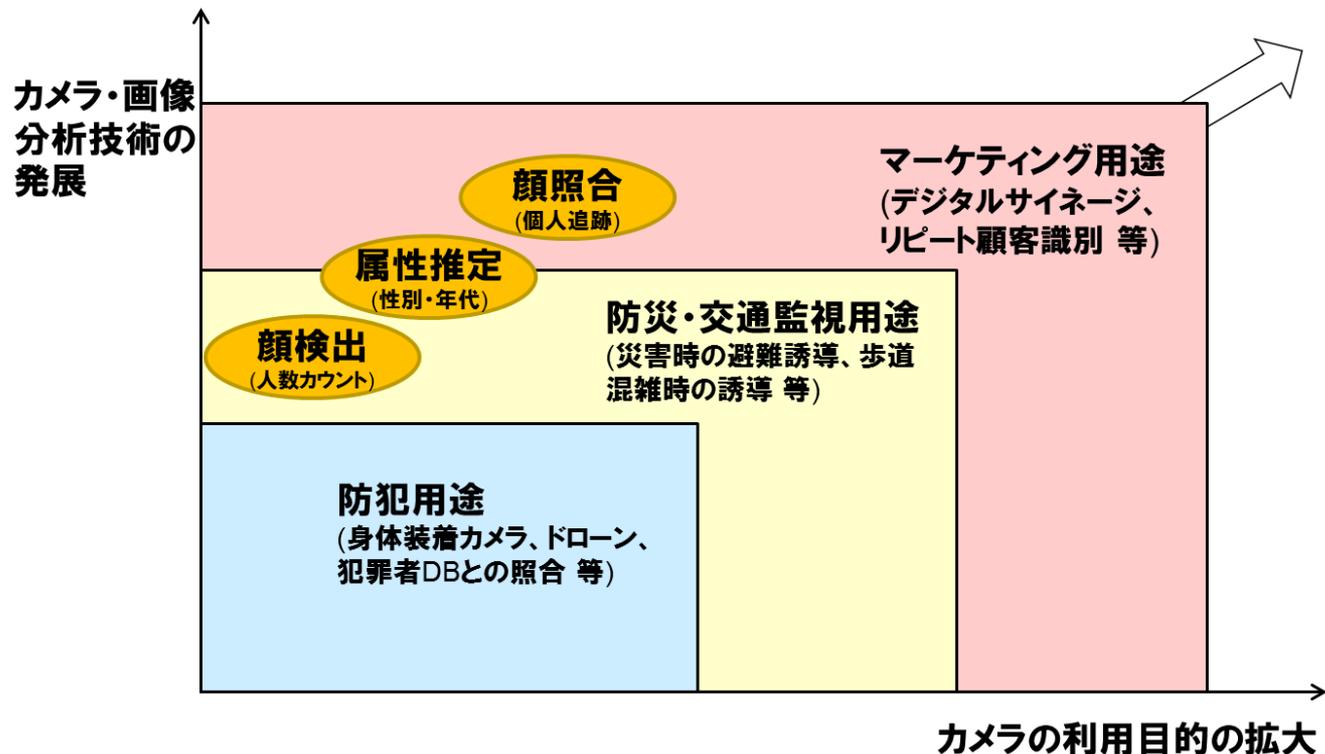
(株)国際社会経済研究所

主幹研究員 小泉 雄介

y-koizumi@pd.jp.nec.com

日本におけるカメラ画像利活用の課題

- カメラ映像/顔画像・センサーデータなどIoT機器で大量に取得されるパーソナルデータの利活用に当たっては、以下のような課題がある。
 - ① 個人情報として取扱う必要があるか否か。個人情報に該当する場合、どのように本人に利用目的等を公表・通知し、「本人の同意」を得ればよいか 【法令遵守の課題】
 - ② 利用者の漠然とした不安感に対処し、反発を受けない(炎上しない)ためにはどうしたらよいか 【社会的コンセンサス獲得の課題】
- そのため事業者等がこのようなIoTデータを活用した新規サービスに二の足を踏む事態も生じている。



英国： 監視カメラの設置状況(2017年)



ロンドンの公共空間におけるカメラ
(ビッグベン・国会議事堂前)



民間の建物における
CCTV掲示



食品小売店における
CCTV掲示

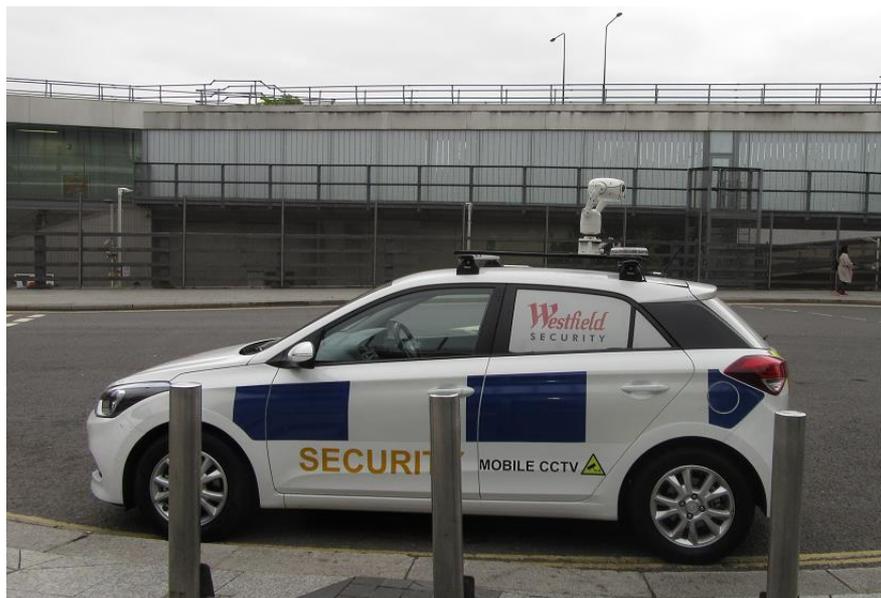
英国： 監視カメラの設置状況(2017年)



地下鉄車内のCCTV
掲示板



タクシー車内のCCTV
掲示板



警備会社のCCTV付き
車両

英国：監視カメラ設置状況と経緯(1/2)

- 監視カメラ設置数
 - **英国全体で600万台** (2015年の推計値)
 - ロンドン全体:60万台(2010年)
 - イングランドおよびウェールズで公的機関が運用するカメラ:10万台
 - ロンドン警視庁がアクセスできるカメラ:6万台(2010年)
 - 全国の自治体:3万台
 - ロンドンの道路上(交通監視用):5000台
 - ヒースロー空港:3000台
 - ロンドン地下鉄駅構内:1万5300台
 - ロンドン地下鉄車内:1万2000台
 - 英国の都市で1日にカメラで撮影される平均回数:300回

英国：監視カメラ設置状況と経緯(2/2)

• 経緯

- 1961年 ロンドン交通公社が初の監視カメラを地下鉄Holborn駅に設置
- 1970～80年代： 店舗や車道、地下鉄等での限定的利用
- 1990～2000年代： 公共空間(公道や学校等)での利用拡大
 - サッチャー首相(～90年)、メージャー首相(1990年～97年)の保守党政権下で監視カメラの積極的推進策が開始。1997年～2010年のブレア政権・ブラウン政権(労働党)下でも継続。
- **1993年 ジェイムス・バルジャー事件(少年二人組による幼児殺害事件)**
 - CCTVが犯人特定に或る程度寄与。この事件を契機に、政府はCCTVの設置をさらに推進。
- 1998年 犯罪・秩序違反法制定。「CCTVイニシアティブ」で内務省は自治体に補助金を拠出
- **2005年 ロンドン市営地下鉄・市営バス同時爆破テロ** →実行犯の特定にカメラ映像が寄与
- **2012年 自由保護法制定。監視カメラシステムを規制**
 - 2010年の総選挙後に成立したキャメロン保守自民連立政権は政策綱領において、従来の治安対策を見直し、市民的自由を回復するための法案を提出、またCCTVについての規制を強化することを政権公約として掲げた。
 - 背景として、(商業施設など私的空間はよいとして)公道などの公共空間においてカメラを設置し、犯罪とは関係ない一般市民を常時撮影していることについて、Big Brother Watch、Liberty、Privacy International等の市民団体から強い反対キャンペーンがあったことが挙げられる。

英国：カメラ・顔認識に関連した法令・ガイドライン・制度

- 法令
 - 1998年データ保護法：日本の個人情報保護法に相当
 - [2012年自由保護法](#)：地方自治体や警察による[カメラ設置](#)を規制
- 第三者機関
 - 情報コミッショナー・オフィス(ICO)
 - 個人データ保護全般を監督。日本の個人情報保護委員会に相当。
 - [監視カメラコミッショナー\(SCC\)](#)
 - 監視カメラに特化した監督機関。
- ガイドライン
 - CCTV行動規範(2014/2015年)：ICOが策定
 - [監視カメラ行動規範](#)(2013年)：SCCが管轄
- 監視カメラに対する[認証制度](#)(2015年11月開始)
 - 監視カメラ行動規範の12原則を遵守していることを認証。
 - 認証マークはWebサイト等で使用可。
 - 40組織が認定取得(小売企業・病院・大学・警察等)。



英国：監視カメラに対する認証制度

- 認証制度の概要
 - [監視カメラコミッショナー\(SCC\)](#)は2015年11月に[第三者認証制度](#)を立ち上げた。
 - 監視カメラ行動規範(SC Code)の直接的な対象となる[地方自治体や警察のみならず、民間企業も](#)申請できる。
 - [SC Codeの12原則](#)を遵守していることを認証する。
- 認証機関
 - 認証は、SCCではなく、[独立した認証機関](#)(以下の3つ)が実施する。
 - National Security Inspectorate (NSI) • IQ Verify
 - Security Systems and Alarms Inspectorate Board (SSAIB)
 - これらの認証機関は、United Kingdom Accreditation Service (UKAS)によって認定。
 - [認証手続きは2段階](#)
 - ①自己評価ツール(SAT)の結果と他の必要書類を認証機関に提出
 - ②12か月以内に認証機関による現地審査を受ける
 - 認証マークは5年間有効。申請手数料と、年次レビュー手数料が必要。Webサイト等で使用可。
- 認証を取得した組織
 - 2016年11月時点で、[約40の組織](#)が認証を取得。
 - マークス&スペンサー(小売事業者)、Salford University、病院
 - ロンドン警視庁(ボディカメラ)、マンチェスター警察(ボディカメラ) 等
 - SCCは全ての地方自治体に対して、①のステップ(SAT)を推奨。[93%の自治体が①の自己評価を実施済み](#)とのこと。



英国：顔認識技術の利用状況

- 小売業店舗での利用
 - CSCによる2015年の調査では、英国の小売店の27%が顔認識技術を使用。衣料品店は特に積極的であり、59%が何らかの形態の顔認識技術を使用。うち46%が防犯目的(万引き犯顔照合等)で顔認識を使用。
 - 消費者の56%は顔認識技術が何なのか知らないと回答。33%が顔認識技術について知っているが、プライバシー侵害的であると回答。消費者の71%は、自分の性別・年齢層・店内での滞留時間といった情報を記録する技術に対して居心地が良くないと回答。
- ヒースロー空港等
 - 電子パスポートゲート:登録者について、パスポート内の顔写真とゲート通過時の顔画像を自動照合
 - ビザ写真:外国人が居住国の英国領事館で取得したビザの顔写真と、入国時の顔画像を自動照合
 - 犯罪者DBとの顔照合:空港での犯罪者DBとの顔照合は警察が実験を実施
- 警察の拘留者データベース
 - 英国警察は拘留者データベースを持っているが、データベースに取り込む写真が良くない(画質が悪い等)という問題があるという。スコットランド警察は監視カメラやその他のソースから得られた個人の顔写真を識別するために顔認識技術を使用。
- 地下鉄の行動検知システム
 - ロンドン地下鉄では地下鉄乗降客の行動検知を内務省、警察、大学研究者、ベンダーと共に検討。駅プラットフォームでの飛込み者を未然に防ぐシステムや、エスカレーターの運行管理、乗降客の人数カウントなどでの応用を検討中。

英国：Facewatch（1/3）

- 英国のベンチャー企業。小売店向けの[犯罪オンライン通報プラットフォーム](#)を提供。
- [被害届手続きの効率化](#)
 - 顧客となる小売店は、[CCTV画像と被害届](#)をオンラインで警察に提出できる。手続き時間を従来の28日間から20分に短縮。[10,000以上の小売店が登録している](#)（2015年12月時点）。
 - 小売店舗での被害者（窃盗被害者等）は、店からすぐにFacewatchの犯罪参照番号をもらうことができる。その後（店舗がFacewatchを用いて警察に通報後）、警察の犯罪参照番号も受け取れる。
- [警察の業務効率化](#)
 - 警察の業務効率化にも役立っており、West Midlands Policeにおけるケーススタディでは、犯罪報告手続きにおいて推計80万ポンド（約1.1億円）分の警察官の時間の節約につながった。Facewatchによれば、全国の警察から高く評価されている。

英国: Facewatch (2/3)

- インシデント通報フォーム

Report an Incident F464 collapse all

Crime Information ▶

Location ✓ ▶

Date and Time ✓ ▶

Incident Type ✓ ▶

Describe Items - Stolen ✓ ▶

Describe what happened ✓ ▶

CCTV * ▼

No CCTV Reason

Select Reason ▼

If you cannot provide CCTV please select a reason.

Screen capture Upload CCTV ?



Record 120s

出典: Facewatchホームページ

英国：Facewatch（3/3）

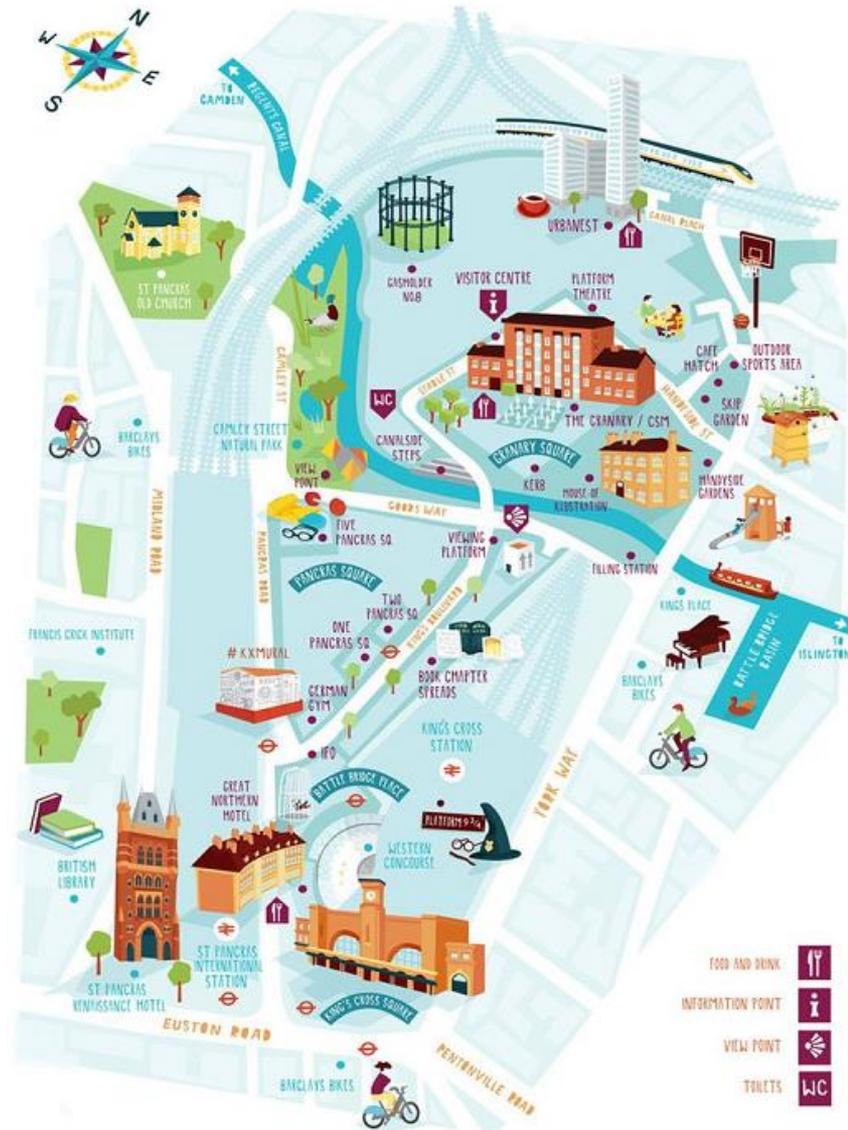
- 小売店における犯罪削減
 - 地域の小売店における犯罪削減にも寄与するという。
 - 例えば、英国で年間に100万件の燃料窃盗が起こっており、ガソリンスタンドの年間損失額は3100万ポンド（約44億円）に上ると内務省は推計している。
- ユーザ企業におけるデータの共有
 - Facewatchには、地域の顧客企業グループ内で、万引き犯その他の潜在的犯罪者のCCTV画像やアラート等を共有する機能がある。既知の万引き犯やバッグ置引き犯の画像等のウォッチリストを地域的に作成したり、共有することが可能である。
 - 「他企業との共有については、プライバシーポリシーで公表しており、data sharing agreementを結んでいけば問題ない。」（SCCより）
- 2017年6月現在、顔認識機能（ウォッチリストと来店客の顔画像を照合）のトライアル中である。
- BBCのTV番組では、Facewatchは「ゲームチェンジャー」として紹介されている。

英国：警察におけるリアルタイム顔照合(監視)実証実験

時期	実施主体	実施イベント	顔照合データベースの内容
2015年6月	レスターシャー警察	屋外音楽イベント (ロックフェスティバル)	レスターシャー警察の拘留者DB、 およびユーロポールから得た国際 犯の顔写真DB
2016年8月	ロンドン警視庁	ノッティングヒル・カー ニバル	カーニバルへの参加を禁じられた 人や、犯罪を行うためにカーニバ ルに参加する可能性があるとして 警察が指定した人(組織犯罪者 等)
2017年6月	南ウェールズ 警察	欧州サッカー連盟チャ ンピオンズリーグの決 勝戦 (南ウェールズのカー ディフ)	組織犯罪者・違法チケット販売者・ フリーガンなど50万人のDB (スタジアムのみならずカーディフ 市内全域で顔照合)

英国：市内での常時リアルタイム顔照合(監視)

- キングスクロス再開発地
 - ロンドンのキングスクロス駅前の東京ドーム6個分の広さ(27万平方メートル)の再開発地。
 - 既にセントマーティンズ大学が入っており、Googleの英国本社も入居予定。その他、高級マンションや中学校などが入る予定。
 - 敷地内に240台のカメラがあり、不動産会社が保有。CCTV室で集中管理。
- リアルタイム顔照合
 - リアルタイム顔照合のトライアルを実施(サービスインも予定)。
 - 警察から犯罪者や行方不明者の顔写真を含む人物データを受領。
 - 欧州の公共空間で初めての「常時」リアルタイム顔認識とのこと。



地図の出典: www.kingscross.co.uk

英国：リアルタイム顔照合(監視)に対する懸念

○ 市民への通知(透明性):

- 「レスターシャーの事例では、自動顔照合を行うことに関する通知は、チケットの裏面に小さな文字でなされたのみであり、それに気づいた参加ミュージシャンが反対声明を出すなど、かなり大きな問題になった。」(SCCより)
- 「自動顔照合の問題は、アルゴリズムの正確性以外にも、市民は撮影されていることには気づいているが、データベースと照合されていることについては知らないことだ。」(SCCより)

○ 顔照合データベースの内容:

- 「レスターシャーの事例では、顔照合するデータベースの内容については公表しなかったため、市民が自分も対象となっているのではないかと思ってしまった。」(SCCより)
- 「問題なのはデータベースがどのように作られていて、誰が登録されているのか分からないこと。犯罪者のみならず一般市民も入っているのではないか。」(プライバシー団体より)
- 「自動顔照合が行われるデータベースの正当性(Legitimacy)が課題である。警察では拘留者全員の顔写真(2000万人分)を保持しているが、無実となった人のデータも保持している。判例でも、無実の人の顔写真の保持は止めるべきという判決があった。」(SCCより)

米国：カメラ・顔認識に関連した法令・ガイドライン・制度

• 法令

- （個人情報保護法に相当する民間分野の一般法は無い）
- 連邦取引委員会(FTC)法第5条：企業のプライバシーポリシーに虚偽の記載があれば、FTCは当該企業を訴追できる。
- ビデオ隠し撮り防止法：個人の「私的領域」の写真を、本人の同意なく、意図的に撮影することを犯罪とする。
- 州法：テキサス州とイリノイ州
 - 民間企業・民間団体は生体認証識別子（顔特徴データを含む）の取得に先立ち、本人の同意を得なければならない。

• 第三者機関

- 連邦取引委員会(FTC)：
民間分野における公正な取引（個人データ保護を含む）を監督。

• ガイドライン

- FTCの顔認識に関するスタッフレポート（“Facing Facts”）
- 業界団体による自主規制ルール

米国： 顔認識技術の商用利用の状況(1/3)

- 米国では、商業施設における顔認識技術の利用は(日本に比べて)進んでいる訳ではない。利用が進んでいるのは、SNSにおける写真のタグ付けや、スマートフォン等へのログイン時の本人確認等の用途である。

(1) 比較的利用が進んでいる利用方法

- ①写真の識別/照合と整理
 - SNSにおける写真のタグ付け(Facebook、Google)
 - FacebookのTagSuggest機能(顔照合)
 - 利用者がアップロードした写真に人物が含まれる場合、既に当該利用者と「友人」関係にある人については、その人が誰であるかの「タグ」を「サジェスト」する機能。
 - PC内の写真アルバムの整理(自分の子どもの写真等)
- ②セキュアなアクセス
 - PCやスマートフォンへのアクセス(アンロック機能におけるパスワードの代替)
 - モバイルペイメント
 - マスターカードは「selfie pay」という、スマホサイトでのクレジットカード決済時に顔認識で本人確認するアプリを開発。カナダのモントリオール銀行がコーポレートカード利用者向けに、2016年夏から導入。
 - 建物内のセキュアなエリアへの物理的アクセス

米国： 顔認識技術の商用利用の状況(2/3)

(2)パイロット(試験運用)中／一部実用化された利用方法

③セーフティとセキュリティ

- **小売店**： 窃盗防止目的で、顔認識ソフトウェアを備えた防犯カメラシステムを試験運用(書店や衣料品店等)。来店客の画像を、[既知の万引き犯](#)や犯罪組織メンバー等の画像DBと比較する。マッチングした場合、警備員や管理者にアラートが送られ、当該人物に関する既知の情報が送られる。
- **カジノ**： 既知のギャンブル詐欺犯や犯罪組織メンバー等を識別するために利用している。カジノは顔認識のメジャーユーザーである。カジノ内で歩ける場所が決まっているので、顔画像を撮りやすい。
- **金融機関**： 幾つかの金融機関の防犯システムにも、強盗容疑者等を識別するために顔認識ソフトウェアが組み込まれている。
- **アパートメント**： 顔認識システムにより住民と非住民を識別。

米国： 顔認識技術の商用利用の状況(3/3)

(2)パイロット(試験運用)中／一部実用化された利用方法

・ ④マーケティングと顧客サービス

- 電子看板： 既に顔認識技術が一部で利用されている。閲覧者の性別、年代といった属性を推定し、それに応じたターゲット広告を提示する。小売店や広告者はリアルタイムで、消費者に関連する製品やセールを表示することができる。将来的には電子看板を用いて顧客の氏名を識別したり、過去の購買履歴やその他の個人情報に基づいてターゲット広告を行なったりすることも想定されるという。
- 小売店における電子看板以外の用途としては、顧客の店内での動線を追跡して商品レイアウトの変更等の顧客サービス改善のために利用することや、既存顧客が来店した際に店員にアラートを送ることも想定できるという。これらは現時点での利用というよりは、将来的なポテンシャルのある用途である。
- NRF(全米消費者協会)によると、米国ではこれらの用途はまだ模索中であり、進み方がゆっくりしている。

- ・ 米国で商業施設での利用が十分に進まない理由は、ユーザ企業がレピュテーションリスクを恐れているため。消費者の顔認識技術に関する認知度・理解度も高くなく、マスコミ報道等に煽られた漠然とした不安感がある。社会的に受容されるための下地がまだ整っていない。これらの点は、日本と類似している。

米国： 警察における顔認識技術の利用

- FBIやニューヨーク市警などで、捜査支援のために顔認識技術を利用
 - 2017年3月、米国下院の監視・政府改革委員会で、顔認識技術のメリット・課題・法制化の必要性について検討し、FBIにおける顔認識の利用について吟味するために公聴会が開かれた。
- FBIがアクセスできる顔画像データ
 - FBI自前の顔認識システム： 約3000万人分
 - 国務省 (パスポート申請者(米国人)、ビザ申請者(外国人))
 - 国防総省
 - 18州 (運転免許証写真等)

合計1億2500万人のデータ
(米国成人の51%)
- FBI等の顔認識システムに対する懸念： (米国のプライバシー団体が表明)
 - 「パスポートや運転免許といった犯罪と無関係のソースから収集した顔画像が80%を占め、それが犯罪捜査に使われている。照会にあたって令状も必要ない。」
 - これは、本人同意のない目的外利用に当たる。
 - 「シカゴ、ダラス、ロサンゼルス、ニューヨーク、ウェストバージニアの警察がリアルタイム顔照合技術を既に購入しているか、あるいは検討している。」
 - 「さらに、米国の18000の警察機関のうち6000がボディカメラを使っていると推定されるが、ボディカメラがリアルタイム顔照合システムにつながるまで時間の問題だ。」

カメラと顔認識に関する米・英・仏・西比較

	米国(アメリカ) (2016年調査)	英国(イギリス) (2017年、2015年調査)	フランス (2015年調査)	スペイン (2017年調査)
セキュリティとプライバシーの兼ね合い	セキュリティ(防犯、国家安全保障)重視		プライバシー重視 (2015年テロ以降はセキュリティ寄りに)	プライバシー重視
監視カメラ設置の事前認可	不要		必要 (公共空間への設置)	
顔画像、顔特徴データの扱い	FTCの言う「保護対象データ」に該当	データ保護法上の個人データに該当		
利用目的等の公表／通知方法	(明確なルールなし)	現地での掲示が必要		
本人による開示・消去請求への対応	(明確なルールなし)	開示・消去請求への対応が必要		
顔画像データの保存期間	(規定なし)		1ヶ月以内(公的機関)	30日間以内
商業施設や公共空間における顔認識技術の利用状況	・店舗等において防犯・商用目的で利用 ・いくつかの警察がリアルタイム顔照合システムを購入	・店舗等において防犯・商用目的で利用 ・公共空間でのリアルタイム顔照合を一部実施	・スタジアムでの顔照合実証実験のみ許可(CNIL、2015年時点)	・店舗や公道等では使われていない

まとめ

- 我が国の監視カメラを巡る社会的環境やプライバシーに対する世論、法体系に鑑みるに、カメラ設置や顔認識技術等の導入に比較的寛容な英国の取組みが最も参考になると考えられる。
- しかしそのような英国にあっても、カメラの設置や顔認識技術の利用にあたっては、監視の濫用や誤用を防ぐための様々な対応策(監視カメラ第三者機関の設置、行動規範の策定・促進、認証制度の設立、市民への透明性の確保、市民の権利の保障、広報活動等)が準備されていることに留意すべきである。
- とりわけ、これらの監視技術の利用にあたっては、「透明性の確保(市民への通知・公表、市民による理解)」が重要とされている。また、運用面での困難さを伴う「本人の関与(本人情報の開示・消去請求への対応)」についても対応しなければならないとされている。
- 近年、海外での導入事例が散見される公共空間でのリアルタイム顔照合については、その先駆けとなっている英国においても未だ社会的な議論が十分になされていない。市民がそのような顔照合システムの存在を認知しておらず、「ステルス的」な導入になっている恐れがある。英国レスターシャー州では抗議運動も起こっている。
- 万が一、日本において公共空間でのリアルタイム顔照合を導入することとなった場合には、住民のプライバシーへの影響が甚大であるため、大規模イベント時など期間・場所を限定した利用に留めるべきであろう。また、プライバシー影響評価(PIA)等を通じて、事前に住民への周知徹底や社会的コンセンサスの獲得を十分に行うべきと考える。

【ご参考】 顔認識(facial recognition)サービスの分類

①顔検出(Facial Detection) :

- 映像内の顔の存在を検出し、顔の位置を同定する処理。

②顔映像からの属性推定(Categorisation) :

- 顔映像から年代や性別といった属性を推定する処理。

③顔照合(狭義のFacial Recognition) :

- 顔映像から抽出した顔特徴データを用いて、複数の顔映像が同一人物の顔であることを照合する処理。

– (1) 個人を「特定」しないが、「識別」して追跡する場合

– (2) 個人を「特定」する場合(Facial Identification)

※「特徴情報」とは、顔映像から抽出された個々人にユニークな特徴を示す数値データ。

④顔認証(Facial Authentication) :

- ID/パスワード等に代わる個人認証手段(アクセスコントロール手段)として、顔映像を照合する処理。

※「特定」「識別」は、パーソナルデータ検討会技術検討WG報告書の用語。
「特定」:ある情報が誰の情報であるかが分かること。
「識別」:ある情報が誰か一人の情報であることが分かること。

報告者の略歴

○小泉 雄介

株式会社 国際社会経済研究所 主幹研究員 <http://www-i-ise-com.onenec.net/jp/about/researcher/koizumi.html>

- 専門領域:
 - 個人情報保護/プライバシー、監視社会、電子政府(国民ID/マイナンバー制度)、途上国市場調査
- 略歴:
 - 1998年 (株)NEC総研入社
 - 2008年7月 日本電気(株)パブリックサービス推進本部に出向
 - 2010年7月 (株)国際社会経済研究所(旧NEC総研)に復帰
- 主な著書
 - 『国民ID 導入に向けた取り組み』(共著、NTT出版、2009年)
 - 『ブログ・SNS利用者の実像』(共著、NEC総研、2006年)
 - 『現代人のプライバシー』(共著、NEC総研、2005年)
 - 『経営戦略としての個人情報保護と対策』(共著、工業調査会、2002年)
- 主な論文・解説
 - 「ICT世界の潮流パートV: 諸外国における国民IDカードとeID」(日刊工業新聞2017年6月)
 - 「英国における監視カメラと顔認識の動向」(画像ラボ2017年3月号)
 - 「プライバシー影響評価(PIA)の海外動向と日本への応用」(日本データ通信2017年3月号)
 - 「EUデータ保護規則案の動向と個人データ越境移転」(ITUジャーナル2015年11月号)
 - 「マイナンバー制度とは」(日本経済新聞2013年4月7日「今を読み解く」に掲載)
 - 「EUデータ保護指令の改定と日本企業への影響」(『CIAJ Journal』2012年6月号)
 - 「国民ID制度の概要と海外の最新事情」(共著、『CIAJ Journal』2011年1月号)
 - 「オーストリアの電子IDカードと市民カード」(共著、『情報化研究』情報産業振興議員連盟、2008年) 等