「主要国・地域における顔識別機能付カメラの利用に関する法制度」
調査結果報告書

2023年3月

アンダーソン・毛利・友常法律事務所　外国法共同事業

目次

第 1 章　総論

I. 調査体制

本調査を実施するに当たっては、アンダーソン・毛利・友常法律事務所外国法共同事業（各国拠点を含む）及び同事務所からの再委託先となる各国・地域の法律事務所とが連携して、個人情報保護委員会の作成した所定の質問票に現地から回答を得る形で各国・地域における制度調査を行い、各国からの回答を基に本報告書を作成したものである。

Ⅱ. 調査期間

2022 年 6 月より 2023 年 3 月 31 日までの期間、本調査を実施した。

Ⅲ. 基準日

本調査の内容は、2023 年 1 月 31 時点でのものであり、それ以降のアップデートについて網羅しているものではない。

Ⅳ. 調査対象国・地域一覧

本調査の対象となる国・地域は以下のとおりである。

1.中国（中華人民共和国）	2.韓国（大韓民国）	3.欧州連合（EU）
4.英国	5.ドイツ（ドイツ連邦共和国）	6.フランス（フランス共和国）
7.スペイン（スペイン王国）	8.オランダ（オランダ王国）	9.スイス（スイス連邦）
10.オーストラリア（オーストラリア連邦）	11.ニュージーランド	12.カナダ
13.アメリカ合衆国（連邦）	14.アメリカ合衆国（カリフォルニア州）	15.アメリカ合衆国（イリノイ州）

第 2 章　中国（中華人民共和国）

主要国・地域における顔識別機能付カメラシステムの利用に関する法制度に関する調査

第一次調査サマリー（中国）

法域	中国		
1. 調査対象の法令・ガイドラインの名称	民法典	個人情報保護法	情報安全技術 個人情報安全規範
1.1 制定主体	全国人民代表大会		
1.2 規律対象	民間部門及び公的部門（地方自治体を含む）双方		
2. 利用目的			
2.1 顔識別を利用する場合の根拠を要する規定又は利用目的を制限する規定	「個人情報」として保護される（民法典第 1034 条第 2 項）	「個人センシティブ情報」として保護される（個人情報保護法第 28 条、情報安全技術 個人情報安全規範　付録 B 表 B.1）	
2.1A 許容される利用目的	☒　犯罪予防：テロリズム防止法第 38 条第 1 項、公安機関刑事事件取扱手続規定第 263 条、第 264 条。 ☒　要保護者保護：顔認証技術の全面適用による路上生活者・物乞いの救助管理サービス能力の向上に関する民政部弁公庁による通知第 2 条第 1 号 ☒　公衆衛生の維持・向上：伝染病防治法第 12 条 ☒　商業利用：禁止規定なし。		
2.1B 禁止される利用目的	☒　違法行為もしくは、不法行為であるもの、また又はそれらを助長するもの：民法典第 1035 条第 1 項第 4 号、個人情報保護法 5 条 ☒　差別的な取扱いを目的とするもの：個人情報保護法第 24 条第 1 項 ☒　性格特性、内的感情、精神状態の特定：目的自体は適法だが、顔データの取得は、個人情報保護法第 6 条でいう「取扱目的と直接的な関係があり、個人の権益に対する影響が最も小さい方法」とは言い難いため、同条の違反になりやすい ☒　宗教上又はその他の信条の判別：目的自体は適法だが、顔データの取得は、個人情報保護法第 6 条でいう「取扱目的と直接的な関係があり、個人の権益に対する影響が最も小さい方法」とは言い難いため、同条の違反になりやすい。		
3. 撮影場所・撮影態様			

3.1 撮影場所を制限する規定	民法典第 1033 条第 2 号	個人情報保護法第 26 条 顔認証技術による個人情報取扱に係る民事事件の審理における法律適用の若干問題に関する最高人民法院の規定第 2 条第 1 号	－
3.2 許容される撮影場所	－		
3.3 許容される撮影態様	－		
4. 撮影の事前同意を求める規定	民法典第 1035 条第 1 号	個人情報保護法第 13 条第 1 号、第 29 条	－
5. 顔特徴量の取扱いに関する規定	司法解釈 ・顔認証技術による個人情報取扱に係る民事事件の審理における法律適用の若干問題に関する最高人民法院の規定 国家基準（いずれも強制力のないもの）： ・情報安全技術 生体特徴識別情報保護基本要求 ・情報安全技術 遠距離顔認証システム技術要求 ・情報安全技術 生体特徴識別に基づくモバイルスマートデバイス身分識別技術枠組み ・情報安全技術 信頼可能環境に基づく生体特徴識別身分特定規約枠組み ・情報安全技術 顔認証データ安全要求（意見募集稿）		
6. 透明性・説明責任			
6.1 撮影の公表・掲示を求める規定	－	個人情報保護法第 17 条第 1 項、第 30 条	－
6.2A 通知公表や掲示が義務付けられている項目	☒ 利用目的 ☒ 処理方法 ☒ 管理者の身元 ☒ 管理者への連絡先 ☒ その他（該当する場合）：上記のほかに、取り扱う個人情報の種類、保存期間、個人が本法に定める権利を行使する方法及び手続、機微な個人情報の取扱の必要性、個人の権益に対する影響、法律、行政法規が告知すべきと定めるその他の事項も通知公表が必要（個人情報保護法第 17 条第 1 項、第 30 条）。		

6.2B 通知の公表や掲示の方法に関する規律	☒ 通知公表や掲示の場所（個人情報保護法第 17 条第 3 項）		
6.3 本人の同意取得時に示すべき事項	☒ 撮影主体 ☒ 撮影の目的 ☒ 撮影の範囲 ☒ 問合せ先 ☒ 撮影した画像の処理の方法 ☒ その他（自由回答）：保存期間、個人の権利行使の方法及び手続、機微な個人情報の取扱の必要性、個人の権益に対する影響、法律、行政法規が告知すべきと定めるその他の事項		
6.4 保存に関する規定	－	該当する規定あり（詳細は以下参照）。	該当する規定あり（詳細は以下参照）。
6.5 保存に関して規律される項目	－	☒ 登録された個人データの保存期間：個人情報保護法第 19 条、情報安全技術 個人情報安全規範 6.1 ☒ 登録された個人データの削除手続：個人情報保護法第 47 条、情報安全技術 個人情報安全規範 8.3 ☒ その他（該当する場合）：管理制度の構築（個人情報保護法第 51 条）、非識別化（情報安全技術 個人情報安全規範 6.2）、個人センシティブ情報の暗号化等（情報安全技術 個人情報安全規範 6.3）	
7. 救済手段			
7.1 救済手段に関する規定	－	個人情報保護法に規定あり（個人情報保護法第 44 条～第 50 条。詳細は以下参照）。	－
7.1A 適用される救済手段の項目		☒ 開示請求 ☒ 利用停止等請求 ☒ 苦情処理への対応 ☒ その他（該当する場合）：複製、移転、修正、補足、削除、個人情報取扱規則の説明に関する請求権	

8. DPA の免許、届出又は監査を求める規定	－	個人情報取扱数が当局所定の数量に達した場合には個人情報保護責任者の指定・届出が要求される（個人情報保護法第 52 条)。数量に関して､施行中の基準はまだないが､100 万人以上の個人情報を取り扱う場合は届出及び監査が必要との旨の意見募集稿が存在する（ネットワークデータ安全管理条例（意見募集稿）第 26 条、第 58 条第 2 項)。	－
9. 外部監査を求める規定	現状では内部監査で足りるが、外部のデータ安全監査専門機関による定期監査が将来導入される可能性がある（ネットワークデータ安全管理条例（意見募集稿）58 条 1 項)。		
10. その他			
10.1 PIA の実施を求める規定	－	個人センシティブ情報を取り扱うため、PIA の実施は必要（個人情報保護法第 55 条第 1 号)。	－
10.2 AI を使用した個人データの自動処理を規制する規定	－	個人情報保護法第 24 条	－
10.3 特記事項	－		

令和 4 年度調査事業「主要国・地域における顔識別機能付カメラの利用に関する法制度」
第二次調査サマリー（中国）

１．裁判例・執行事例の調査結果

【主要な裁判例】

① (2020)浙 01 民終 10940 号判例

- 事案の概要：動物園の年間パスポートを購入し、指紋を採取された消費者が動物園から、入園時の認証方法の変更を理由に顔データの提供を強要されたとして、動物園を提訴した事案。
- 判旨：中国個人情報保護法施行前の事案で、裁判所は、動物園が入園時の認証方法を指紋認証から顔認証に一方的に変更したことは契約違反と指摘し、消費者に損失を補填し、指紋データと顔データを削除する旨の判決を言い渡した。

② (2022)蘇 0508 民初 5316 号判例

- 事案の概要：住宅展示場を訪れた消費者が、室内に設置された顔識別カメラシステムで顔データを収集されたことについて、不動産会社を提訴した事案。顔データの取得について、不動産会社が入口に設置した看板において公開した利用目的は「防犯用」だが、実際は消費者の識別や仲介業者との料金精算にも利用されていた。また、公開された期間を超えて顔データを保存し、仲介業者に顔写真を送信した事実も裁判で判明した。その後、不動産会社は顔識別カメラを撤去し、消費者の顔データを削除した。
- 判旨：裁判所は、不動産会社による顔データの取扱は消費者の権利侵害にあたるとして、消費者への謝罪を言い渡した。

③ (2022)京 01 民終 7249 号判例

- 事案の概要：集合住宅の住人Ａが、自身が家を出入りする際に、隣の部屋の住人Ｂが設置した防犯システムが自動作動し、自身の様子が撮影されたとして、住人Ｂを提訴した事案。
- 判旨：裁判所は、隣の住人が通らなければならない通路に防犯カメラを設置すること、および防犯システムの自動作動機能を ON にすることはプライバシー権侵害にあたるとして、防犯カメラを撤去し、防犯システムの自動作動機能を OFF にするよう判決を言い渡した。

④ (2022)魯 02 民終 13505 号判例

- 事案の概要：住人 A が、隣の一戸建ての住人 B が室外に設置した防犯カメラで自分と家族の様子が撮影されたとして、住人 B を提訴した事案。

- 判旨：裁判所は、防犯カメラの撮影範囲は両建物の間の一般道路であるため、住人 A の玄関ドア前の様子が撮影されることはなく、防犯カメラを設置することはプライバシー権侵害には該当しないと判断し、請求を棄却した。

【主要な法執行事例】

① 杭江市督局市監罰処〔2021〕32105151 号処罰事例

- 事案の概要：顔識別カメラシステムを設置し、2020 年 11 月 12 日～2021 年 4 月 16 日の間に 10 万枚以上の顔写真を撮影した不動産会社が処罰された事案。
- 決定要旨：同社は住宅展示場の入口に看板を設置し、顔識別カメラの存在を公開したものの、取得する個人情報の範囲と目的について記載が不十分で、かつ消費者の同意を取得しなかった。また、公開された顔写真の使用方法（記録と契約管理用）についても必要性に欠けるものと認定され、「消費者権益保護法」に基づき 25 万人民元（約 500 万円）の過料を課された。

② 清公（南）行罰決字〔2021〕320 号処罰事例

- 事案の概要：住宅団地の入り口に顔識別カメラシステムを設置した不動産管理会社が処罰された事案。
- 決定要旨：顔識別システムで取得した住人の顔写真について、安全保護に必要な管理体制と技術措置を採っていなかったことが「ネットワーク安全法」違反と認定され、行政警告を受けた。

③ 余市監処罰〔2021〕890 号処罰事例

- 事案の概要：顔識別カメラシステムを設置し、2020 年 9 月 6 日～2021 年 4 月 6 日の間に 26 万枚以上の顔写真を撮影した不動産会社が処罰された事案。
- 決定要旨：同社は住宅展示場の入口に顔識別カメラシステムの設置に関する通知を出したが、消費者に同意を求める措置として不十分と認定された。また、消費者への聞込みの結果、消費者への告知と同意取得が行われなかったことが判明したため、「消費者権益保護法」に基づき 25 万人民元（約 500 万円）の過料を課された。

④ 沪市監徐処〔2021〕042021000759 号処罰事例

- 事案の概要：顔識別カメラシステムを設置し、2021 年 1 月～6 月の間に 43 万枚以上の顔写真を撮影した自動車販売店が処罰された事案。
- 決定要旨：顔識別カメラシステムの設置について、販売店は消費者への告知・同意取得を一切行わなかった。その後、販売店はカメラを自主的に撤去し、取得した顔写真も削除した。同社は、「消費者権益保護法」に基づき 10 万人民元（約 200 万円）の過料を課された。

２．調査対象国における犯罪予防や安全確保のための顔識別機能付きカメラシステムの利用動向や主な設置主体の傾向（政府機関や自治体、民間事業者等）
中国において、全体的には、顔識別機能付きカメラシステムを積極的に利用する傾向が見られる。中国電子技術標準化研究院「2020 年顔識別業界研究報告」（http://www.cesi.cn/202012/7156.html）によると、顔識別技術への投資額は 2020 年時点で合計 406 億人民元（約 8120 億円）で、2019～2020 年の間は鈍化傾向が見られたものの、今後 5 年間でも国内市場は平均で 23%の年間成長率で拡大すると予測され、2024 年の市場規模は 100 億元を超えると予想されている。
また、設置主体の傾向について、政府機関が設置する事例が多くみられるが、民間事業者の事例も報じられている。
政府機関が設置する事例：

- 2018 年：内モンゴルフフホト市の監獄が監視用の顔識別機能付きカメラシステムを導入
  https://www.asmag.com.cn/news/201801/93139.html
- 2018 年：河南省平頂山市教育局が子供の溺水防止のために顔識別機能付きカメラシステムを試験運用
  https://www.xincai.gov.cn/a/shipinanquan/20180831/9462.html
- 2020 年：広東省潮州市潮安区が交通違反取締用の顔識別機能付きカメラシステムを導入
  http://www.chaoan.gov.cn/zwgk/zdlygk/gnjg/content/post_3709799.html

民間事業者が設置する事例：

- 2018 年：山東科学技術大学が防犯用の顔識別機能付きカメラシステムを設置
  http://www.sdust.edu.cn/info/1040/3919.htm

３．調査対象国内における顔識別機能付きカメラに係る政策立案の状況（法令整備を含む。）や世論の動向等
下記報告書が近時の代表的なものかと思われる。

- 北京智源人工知能研究院人工知能倫理及び安全研究センター「顔識別及び公共衛生調査研究報告」
  https://attachment.baai.ac.cn/share/aies/cn-facial-recognition-and-public-health-2020-05-17.pdf
- 中国電子技術標準化研究院「2020 年顔識別業界研究報告」
  http://www.cesi.cn/202012/7156.html
- 中国電子技術標準化研究院「顔識別データ安全標準化研究報告（2021 版）」
  http://www.cesi.cn/202112/8185.html

第 3 章　韓国（大韓民国）

主要国・地域における顔識別機能付カメラシステムの利用に関する法制度に関する調査

第一次調査サマリー（韓国）

法域	韓国		
1. 調査対象の法令・ガイドラインの名称	個人情報保護法（Personal Information Protection Act (PIPA)）	生体データ認証ガイドライン（Guidelines on the Biometric Data Protection）	VDPD ガイドライン(Guidelines on Installation and Operation of Visual Data Processing Devices（VDPD))
1.1 制定主体	国会	個人情報保護委員会（Personal Information Protection Commission（PIPC)）	PIPC 及び韓国インターネットセキュリティ庁（Korea Internet and Security Agency (KISA)）
1.2 規律対象	民間部門及び公共部門（地方自治体を含む）双方		
2. 利用目的			
2.1 顔識別を利用する場合の根拠を要する規定又は利用目的を制限する規定	顔認識データは、PIPA の定める「機微（センシティブ）情報」及び「生体認証情報」に分類されるため、PIPA が適用される。また、顔認識に使用するデバイスが CCTV 又はネットワークカメラの場合は、PIPA のビジュアルデータ処理デバイスに関する規定が適用される。	顔認識データは、PIPA の定める「機微（センシティブ）情報」及び「生体認証情報」に分類されるため、生体認証データガイドラインが適用される。	顔認識に使用するデバイスが CCTV 又はネットワークカメラの場合は、VDPD ガイドラインが適用される。
2.1A 許容される利用目的	顔認識デバイスが CCTV 又はネットワークカメラの場合は、以下の目的が許容される。 ☒　犯罪予防 ☒　要保護者保護 ☒　その他 (該当する場合)：詳細は PIPA 第 25 条を参照。	－	顔認識デバイスが CCTV 又はネットワークカメラの場合は、以下の目的が許容される。 ☒　犯罪予防 ☒　要保護者保護 ☒　その他 (該当する場合)：詳細は PIPA 第 25 条を参照。

2.1B 禁止される利用目的	－		
3. 撮影場所・撮影態様			
3.1 撮影場所を制限する規定	オープンスペースでのビジュアルデータ処理機器（CCTV 及びネットワークカメラ）の設置及び操作については規定がある。	－	VDPD ガイドラインには、許容される撮影場所の例がいくつか示されている。以下の施設はいずれも撮影可能な場所と解される。
3.2 許容される撮影場所	－	－	☒ 歓楽街 ☒ 公共交通施設の構内（例えば、駅、空港、港湾、バス停等） ☒ 公共交通機関の車内（電車、船、バス、タクシー等） ☒ 商業施設（店舗、ショッピングモールなど） ☒ 民間事業者のオフィス（従業員のみが利用する空間） ☒ 公的機関内で市民の往来のある空間（市民対応窓口等） ☒ 公的機関内で市民の往来のない空間（執務室等） ☒ その他（該当する場合）：その他の「オープンスペース」
3.3 許容される撮影態様	－	－	VDPD を使用する場合の撮影態様については、PIPA 第 25 条第 5 項～第 7 項及び VDPD ガイドラインで規定されている。
4. 撮影の事前同意を求める規定	PIPA 第 15 条第 1 項・第 2 項 PIPA 第 58 条第 2 項	－	顔認識に使用するデバイスが CCTV 又はネットワークカメラの

			場合は、VDPD ガイドラインが適用される。
5. 顔特徴量の取扱いに関する規定	PIPA 第 23 条及び施行令第 18 条	生体認証データガイドライン(23 頁)及び生体認証データガイドライン(4 頁及び 17 頁)	－
6. 透明性・説明責任			
6.1 撮影の公表・掲示を求める規定	PIPA 第 25 条 (詳細は VDPD ガイドラインを参照)	－	オープンスペースで、PIPA 第 25 条に定める目的のために VDPD を利用する場合、掲示等を含む、必要な保護措置を講じている限り、個人情報主体の同意は不要である。
6.2A 通知公表や掲示が義務付けられている項目	－	－	☒ 利用目的 ☒ 管理者の身元 ☒ 管理者への連絡先 ☒ その他 (該当する場合) : PIPA 第 25 条第 4 項に規定される。
6.2B 通知の公表や掲示の方法に関する規律	－	－	☒ 通知公表や掲示の場所 ☒ その他 (該当する場合) : VDPD オペレータのホームページ、職場、事業所、事務所、店舗等、特許商標公報、一般日刊紙、週刊紙、オンライン新聞 (一定の場合に限り、PIPA 施行令第 24 条第 1 項を参照)
6.3 本人の同意取得時に示すべき事項	－		
6.4 保存に関する規定	PIPA 第 21 条及び施行令第 16 条第 1 項	生体認証データガイドライン (29 頁及び 30 頁) 及び生体認証データガイ	－

		ドライン（17 頁及び 31 頁）	
6.5 保存に関して規律される項目	－		
7. 救済手段			
7.1 救済手段に関する規定	PIPA 第 35 条～第 39 条の 2	生体認証データガイドライン(25 頁)	－
7.1A 適用される救済手段の項目	☒ 開示請求 ☒ 利用停止等請求 ☒ その他（該当する場合）：訂正請求、損害賠償請求	－	－
8. DPA の免許、届出又は監査を求める規定	－	—	－
9. 外部監査を求める規定	—		
10. その他			
10.1 PIA の実施を求める規定	PIPA 第 33 条第 1 項及び施行令第 35 条 PIPA 第 33 条第 2 項及び施行令第 36 条	生体認証データガイドライン（15 頁）	－
10.2 AI を使用した個人データの自動処理を規制する規定	－		
10.3 特記事項	－		

令和 4 年度調査事業「主要国・地域における顔識別機能付カメラの利用に関する法制度」
第二次調査サマリー（韓国）

1．裁判例、執行事例の調査結果

【主要な裁判例】

① COVID-19 休息結果確認の違憲性に関する憲法裁判所判例 No. 20Heon-Ma468（2021 年 5 月 18 日）。

- 事案の概要：原告は、ソウル市支援センターが施設利用者に COVID-19 検査結果の提出と顔認識サーモカメラによる体温測定を義務付けたことが基本的権利を侵害するとして、憲法上の訴えを提起した。
- 判旨： 憲法裁判所は、前述の要件は公権力の行使ではないとして、請求を棄却した。憲法裁判所は、顔認識サーモグラフィを用いた体温測定によって原告が受けた短時間の不快感は、基本的権利、法的地位、その他の悪影響に大きな影響を与えるとは考えにくいと述べた。したがって、本件の体温測定行為を憲法上の訴えの対象となる公権力の行使とみなすことは困難であるとした。

【主要な法執行事例】

① 城東区映像情報処理関連法解釈に関する個人情報保護委員会事件 No.2020-105-013(2020 年 10 月 28 日)

- 事案の概要：城東区庁は、AI 顔認識サーモカメラによる体温計測を訪問者に義務付けた。進歩ネットワークセンターは、このような要求の法的根拠について問い合わせたところ、城東区役所は韓国個人情報保護法（PIPA）第 58 条第 1 項第 3 号に基づくものであると回答した。進歩ネットワークセンターは、AI 顔認識サーモグラフィによる体温測定が個人情報保護法第 58 条第 1 項第 3 号に該当するかどうかを問うため、韓国個人情報保護委員会（PIPC）に提訴した。
- 決定要旨：PIPC は、城東区役所の AI 顔認証サーモカメラによる体温測定は、PIPA 第 58 条第 1 項第 3 号に該当しないものと判断した。PIPC は、COVID-19 の重大性、COVID-19 の可能性を特定するための体温測定の重要性を認識しながらも、PIPA 第 3 章から第 7 章の適用を除外していることから、PIPA 第 58 条第 1 項第 3 号は狭く解釈されなければならないと判断し、今回のケースでは、単に体温を測定するだけでなく、来場者の写真を撮影する AI 顔認証サーモカメラについて、そのような例外を認める緊急の必要性はないと判断した。また、城東区役所の AI 顔認証サーモグラフィが収集した情報の保存は不要であると判断した。

②（2022)京 01 民終 7249 号決定　個人情報保護委員会事件 No. 2022-007-046（2022 年 4 月 4 日）個人情報保護規定違反に対する是正措置）

- 事案の概要： 報道によると、法務省（MOJ）が入国審査時に収集した顔画像を科学技術省（MSIT）に共有し、科学技術省は AI 識別システムのアルゴリズムを開発するために民間企業に情報を提供した。PIPC は、法務省と MSIT が PIPA に違反しているかどうかを判断するために、この事件を調査した。
- 決定要旨：

  (1) 収集された顔画像が PIPA における「機微情報」に該当するか否かについて

  PIPC は、顔写真が PIPA に基づく機微情報に該当するとの判決を下した。PIPC のバイオメトリクスデータ保護に関するガイドラインによると、一般的な顔写真は個人情報とみなされるが、それ自体が機微情報に分類されることはない。しかし、顔写真から特徴点を抽出するなど、特定の技術的手段によって生成された情報であれば、バイオメトリクス固有の識別子として機微情報とみなされる。したがって、データ管理者は、(i)データ主体からの明示的な同意がある場合、または(ii)機微情報の処理を要求または許可する規定がある場合にのみ、当該情報を処理することが認められる。また、PIPC は、出入国管理法が出国・入国審査目的で機密情報を処理することを明確に認めており、したがって、収集した顔画像の法務省の処理は正当化される可能性があると判断している。

  (2) AI 技術開発のための顔画像利用の適法性

  1) 処理が収集目的の範囲内であったかどうか。

  PIPC は、入国審査の過程で収集された顔画像を顔認識 AI の開発に利用することは、安全な国境管理の確保という入管法の目的に合致するものであり、顔画像の加工は収集目的の範囲内であると判断した。

  2) 個人情報の「処理の委託」または「第三者提供」に該当するかどうか

  PIPC は、入国審査システムの高度化に関する開発契約に基づき顔画像を提供したことから、法務省と MSIT が民間企業に顔画像を提供することは、個人情報の「処理の委託」に該当するとの見解を示した。

  (3) 委託先に関する情報不開示の適法性

  PIPA では、データ管理者は委託先をウェブサイト上で開示し、常に更新しなければならないとされている。しかし、法務省は、顔画像の提供を受けた民間企業をウェブサイト上で開示しなかったため、この要件に違反することとなった。PIPC は、MOJ の関連組織である仁川出入国管理事務所に 100 万ウォンの行政処分を科した。

③ 保育所職員の顔認証による出勤管理システムに関する国家人権委員会事件 No. 22Petition0139800（2022 年 9 月 16 日）

- 事案の概要：高陽市は、管内の国公立保育所の職員に対し、顔認証による出勤管理システムを導入したが、それに代わる出勤管理システムを提供することはなかった。これは、手作業による出勤管理システムは不正確で非効率であり、指紋認証方式は 1 人で複数の指紋を登録できるため、不正の可能性があったためです。顔認証による出勤管理システムについては、従業員が求人票を通じて顔写真画像を保育園に提供し、出勤管理のためにその情報を使用することに同意していた。
- 決定要旨：国家人権委員会（NHRC）は、高陽市が代替手段を提供せずに顔認証による出勤管理システムを導入したことは、従業員の個人情報の自己決定権を過度に侵害するものであると判断した。NHRC は、高陽市に対し、国公立保育所職員のために顔認証カメラ以外の出勤管理手段を準備し、運用するよう勧告した。NHRC の判断の根拠は、顔認識情報は、生きている間に本人と関連づけられた個人性の強い固有の識別子であることであった。顔認識情報は、他の個人情報とは異なり、変更できない生体情報であり、身体そのものから得られる。そのため、蓄積された情報が不当に利用されたり、流出したりすると、データ対象者に深刻な被害を与える可能性があることが問題視された。また、NHRC は、従業員がこのような生体情報の収集に同意しない場合、代替手段が用意されていないため、その準備がなされていないと判断したものである。

２．調査対象国における犯罪予防や安全確保のための顔識別機能付きカメラシステムの利用動向や主な設置主体の傾向（政府機関や自治体、民間事業者等）
該当する情報は見られなかった。

３．調査対象国内における顔識別機能付きカメラに係る政策立案の状況（法令整備を含む。）や世論の動向等
ガイドラインとして“Guidelines on Biometric Data Protection”が公表されている。同ガイドラインでは、生体認証情報として保護される情報の種類、収集・利用・移転・保存等の各場面における特徴的な留意事項、安全管理上の留意事項、生体認証情報を利用するサービスの利用者向けの留意事項を解説している。

また、顔認証技術の導入と使用における人権保護のための勧告と意見と題する国家人権委員会決定（2023 年 1 月 12 日付）が公表されている。
背景事情として、顔認証技術は、大量の個人情報を収集・利用するため、不特定多数の人を監視することが可能であり、表現の自由を制限する可能性があるため、人権侵害の可能性があるとして批判を浴びていることが挙げられる。今回、NHRC は、これらの問題を検討し、顔認識技術の導入に関連する法的枠組みの改善について勧告を行ったものである。以下はその概要である。
(1) 顔認識技術による人権侵害のリスクについて
政府が大量の顔情報を収集・保持・分析し、公共の場で顔認証技術を広く使用する場合、特定の個人を追跡・監視する可能性があり、"プライバシー保護への期待 "を著しく低下させる。また、市民が合法的な集会や結社の自由の行使を躊躇する "チリング効果 "を引き起こし、表現の自由を阻害する危険性がある。

(2) 顔認証技術に関する新たな法制化に関する事項
顔認証技術の導入にあたっては、基本的人権に影響を与えるさまざまな要因や規制措置について検討する必要がある。具体的には、このような技術による基本的権利の侵害に積極的かつ先制的に対応する新たな法的根拠を確立する必要がある。新たな立法は、以下の原則を含むものでなければならない：

1) 人権尊重の原則を反映し、政府による顔認識技術の無差別使用を制限すること。政府は、公共の利益のために必要と判断された場合にのみ、例外的かつ補足的な措置として顔認識技術の使用を許可されるべきである。また、中央政府機関や地方公共団体による顔認識技術の導入や使用は、個別具体的な法的根拠に基づかなければならない。
2) リアルタイム遠隔顔認証技術の使用は原則として禁止し、侵害される私益を著しく上回る明確かつ緊急の公益がある場合にのみ認めるべきである。例えば、欧州連合基本権庁は、行方不明の子供を緊急に捜索する場合に、リアルタイムの遠隔顔認識技術を認めている。

(3) 顔認識技術に関する人権影響評価
顔認証技術を責任を持って開発・活用するためには、人権への影響評価を行う必要があり、その根拠や手順を法律に反映させる必要があります。具体的には、以下のような内容を盛り込むことが必要である。
1) 顔認証技術の開発・活用に先立ち、アセスメントを実施する必要がある。また、既に利用されている場合でも、顔認証システムの目的、適用範囲、内容等に大きな変更があった場合には、再度アセスメントを実施すべきである。2) 評価は、データ量、影響を受けるデータ主体の数、地域、人権侵害の可能性等を総合的に考慮して実施すべきである。3) 顔認証システムにより人権に重大な影響を与えるリスクが明らかになった場合には、当該技術の開発・利用を停止し、人権への悪影響を防止・軽減するための措置を実施し、その内容・結果を開示する必要がある。4) 評価は、人権に関する専門知識を有する独立した機関によって実施されなければならない。

第 4 章　欧州連合（EU）

主要国・地域における顔識別機能付カメラシステムの利用に関する法制度に関する調査

第一次調査サマリー（EU）

法域	EU			
1. 調査対象の法令・ガイドラインの名称	General Data Protection Regulation (GDPR)	ビデオ装置を介した個人データの処理に関する欧州データ保護委員会（EDPB）ガイドライン（3/2019）	Law Enforcement Directive (LED)	Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement
1.1 制定主体	欧州議会及び欧州理事会	欧州データ保護委員会	欧州議会及び欧州理事会	欧州データ保護委員会
1.2 規律対象	民間部門及び公的部門（地方自治体を含む）双方		公的部門（地方自治体を含む）のみ	
2. 利用目的				
2.1 顔識別を利用する場合の根拠を要する規定又は利用目的を制限する規定	GDPR が適用される限り、顔認識の使用を含む個人データのすべての処理について、正当かつ特定の目的を定義する必要がある。データを他の目的に使用することはできない（GDPR 第 5 条）。	－	－	－
2.1A 許容される利用目的	☒　その他（該当する場合）：個別の事例ごとに、目的の正当性、並びに個々の事例におけるその目的のための顔認識の妥当性及び必要性を評価するための要件を検討する必要がある。			
2.1B 禁止される利用目的	☒　違法行為もしくは、不法行為であるもの、また又はそれらを助長するもの ☒　差別的な取扱いを目的とするもの			
3. 撮影場所・撮影態様				
3.1 撮影場所を制限する規定	・GDPR 第 9 条 ・GDPR 第 5 条（1）(b)、(c)	・EDPB ガイドライン 3/2019（margin 27）	－	－
3.2 許容される撮影場所	－			

3.3 許容される撮影態様	・GDPR 第 5 条（1）(b)、(c) ・GDPR 第 5 条（1）(a) ・GDPR 第 25 条（2）	－	－	－
4. 撮影の事前同意を求める規定	・GDPR 第 6 条	－	－	－
5. 顔特徴量の取扱いに関する規定	・GDPR 第 4 条（2）	－	－	－
6. 透明性・説明責任				
6.1 撮影の公表・掲示を求める規定	・GDPR 第 4 条（1)、(2) ・GDPR 第 5 条（1）(a)、第 12 条、第 13 条、第 14 条	EDPB ガイドライン 3/2019、Chapter7	－	－
6.2A 通知公表や掲示が義務付けられている項目	☒ 利用目的 ☒ 管理者の身元 ☒ 管理者への連絡先 ☒ その他（該当する場合)： GDPR 第 12 条、第 13 条、第 14 条、EDPB ガイドライン 3/2019 pp.26-27			
6.2B 通知の公表や掲示の方法に関する規律	☒ その他（該当する場合)：データ主体には、当該個人データが最初にいつどこで収集されたのかを知らせなければならない。			
6.3 本人の同意取得時に示すべき事項	☒ 撮影主体 ☒ 撮影の目的 ☒ 撮影の範囲 ☒ その他（自由回答)： ・同意をいつでも撤回する権利とその結果に関する情報 ・個人データの種類、特に、個人データの該当する特別なカテゴリ（GDPR 第 9 条（1）（ここでは、生体認証データ)) ・(議論あり）個人データの受信者に関する情報 ・自動化された個人の意思決定に関する情報（GDPR 第 22 条（2）(c)) ・該当する場合、GDPR 第 49 条（1）(a）に説明されているとおり（EU データの第三国への転送）			
6.4 保存に関する規定	・GDPR 第 5 条：データ最小化の原則（第 5 条（1）(c))、デ	データ最小化の原則	－	

	ータ保持の制限（第 5 条（1）(e))、完全性と機密性（第 5 条（1）(f))が適用される。	（LED 第 4 条（1）(e)）でも、処理の目的に関係のないビデオ素材は、導入前に必ず削除するか、匿名化する（例えば、データを回復するための遡及能力のないぼかし）ことが求められる。	
6.5 保存に関して規律される項目	－		
7. 救済手段			
7.1 救済手段に関する規定	アクセス権（GDPR 第 15 条)、訂正権（GDPR 第 16 条)、消去権（GDPR 第 17 条)、処理の制限（GDPR 第 18 条)、データポータビリティ（GDPR 第 20 条)、異議権（GDPR 第 21 条、GDPR 第 6 条 I(f)及びダイレクトマーケティング)、当局への異議申立権（GDPR 第 77 条)、補償（GDPR 第 82 条） さらに、事業者は、管轄権を有する DPA により罰金を科される可能性がある（GDPR 第 58 条（2）(i)、第 83 条)。		
7.1A 適用される救済手段の項目	☒ 開示請求 ☒ 利用停止等請求 ☒ 苦情処理への対応 ☒ その他（該当する場合)：上記参照のこと。		
8. DPA の免許、届出又は監査を求める規定	該当規定なし。なお、DPA は、GDPR 第 58 条に沿って、エンティティのコンプライアンスを調査する権限を有する（とりわけ苦情申立があった場合)。		
9. 外部監査を求める規定	－		
10. その他			
10.1 PIA の実施を求める規定	・GDPR 第 35 条	LED 第 27 条	－
10.2 AI を使用した個人データの自動処理を規制する規定	・GDPR 第 22 条 ・AI Act		
10.3 特記事項	－		

令和 4 年度調査事業「主要国・地域における顔識別機能付カメラの利用に関する法制度」
第二次調査サマリー（EU）

1．裁判例、執行事例の調査結果

【主要な裁判例】

＜欧州司法裁判所（CJEU）＞

加盟国の裁判所は、国内訴訟で決定的な結果を得た場合、EU 法の解釈と有効性に関する質問を CJEU に提出することができる（「予備判決手続き」）。その目的は、EU 法の統一性と有効性を確保するために、加盟国間で EU 法の解釈や適用が異なることを防ぐことにある。予備判決手続きの結果、付託された裁判所とその後のすべての裁判は、CJEU の決定に拘束されることになる。

① - CJEU、2019 年 12 月 1–日 - C-708/18

- 判旨：裁判所は、前身の規定である GDPR Art. 6 (1) (f) (Art. 7 (f) Directive 95/46/EC)、および欧州連合基本権憲章（以下「憲章」）の第 8 条と第 52 条について述べた。裁判所は、解釈の主要な原則をいくつか指摘しているが、最も重要な点は、(i)設置されたビデオカメラの主な目的、すなわち建物の共同所有者の財産、健康、生命の保護は、「正当な利益」として特徴づけられる可能性が高いこと、(ii)そのような利益は、データ処理の日付において存在し有効でなければならず、その日付において仮想的であってはならない（保護対象商品に対する以前の被害は必要ではない）こと、(iii) GDPR Art.6 (1) (f)を法的根拠とする場合、追加の同意は必要ないことを明確にしたことである。

＜欧州人権裁判所（ECHR）＞

ECHR は、欧州人権条約（「条約」）を欧州の 46 の締約国で解釈・執行するために設立された。個人および条約締結国は、条約またはその議定書で保証された権利を条約締結国が侵害しているとの主張を ECHR に訴えることができる。個人は、ECHR に訴える前に、国内のすべての救済手段を利用済みでなければならない。

① - 欧州人権裁判所、2019 年 10 月 17 日、申請番号 1874/13 および 8567/–3 - CASE OF LÓPEZ RIBALDA AND OTHERS v. SPAIN

- 判旨：ECHR は、職場における隠しカメラによる監視について-部分的に-判決を下した。裁判所は主に、条約加盟国は ECHR8 条を維持しなければならないとする。条約の各締約国の当局と裁判所は、私的雇用者による ECHR8 条の制限に関して、乱用に対する相応の保護措置が存在することを保証しなければならない。私的雇用者による ECHR 第 8 条の制限に関しては、乱用に対する相応の保護措置が存在することを、それぞれの条約締約国の当局と裁判所が保証しなければならない。これを保証するためには、相反する利益のバランスをとることが必要である。

  一般にビデオ監視については、裁判所は、従業員がビデオ監視の計画と実施について通知されていたかどうか、ビデオ監視の範囲、従業員のプライバシーがどれほど集中的に影響を受けるか、監視がどのような結果をもたらすか、雇用主がそれを正当化する正当な理由があったかどうかといった点を考慮しなければならない。さらに、雇用主にとって、より穏やかな形の監視が可能で、同じように効果的であったかどうかも考慮されなければならな

い。同様に重要なのは、雇用主が適切な保護措置やセーフガード（例えば、ビデオ監視から身を守る方法について従業員に情報を提供するなど）を講じたかどうかである。比例性の評価においては、ビデオ監視措置が行われる場所もまた決定的な意味を持つ。

【主要な法執行事例】

該当する法執行事例は見当たらなかった。

2．調査対象国における犯罪予防や安全確保のための顔識別機能付きカメラシステムの利用動向や主な設置主体の傾向（政府機関や自治体、民間事業者等）

該当する情報は見られなかった。

3．調査対象国内における顔識別機能付きカメラに係る政策立案の状況（法令整備を含む。）や世論の動向等

【European Data Protection Board (EDPB)】

EDPB より、ガイドラインとして”Guidelines 3/2019 on processing of personal data through video devices (Current document version adopted on 29 Jan 2020)”及び“Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement Guidelines on Biometric Data Protection”が公表されている。前者は、特にビデオ監視の法的根拠、録画の第三者への開示、特殊な個人データの処理、ビデオ監視に関連するデータ主体の権利、透明性の要件/データ主体への通知方法、保存期間、必要なセキュリティ対策、データ保護の影響評価について扱っている。後者は、EU 及び国家レベルの立法者、並びに法執行機関に対し、顔認証技術の導入及び使用に関するガイダンスを提供する。EDPB は、顔認識ツールは、法執行指令（EU）2016/680（「LED」）を厳密に遵守した場合にのみ使用できることを指摘している。

【European Data Protection Supervisor (EDPS)】

EDPS より、ガイドラインとして”The EDPS video surveillance guidelines”が公表されている。「EU の諸機関、団体、事務所および専門機関による個人データの処理に関する自然人の保護並びに当該データの自由な移動に関する規則（EU）2018/1725」が 2018 年 12 月 11 日に発効される前に公表されているが、一般データ保護規則（GDPR）及びデータ保護法施行指令と整合している。本ガイドラインは、EU の機関や団体がビデオ監視システムをどのように設計し、運用するかについての一連の実践的な推奨事項を含むもので、入退室管理など典型的なセキュリティ目的のビデオ監視に焦点を当てている。

第 5 章　英国

主要国・地域における顔識別機能付カメラシステムの利用に関する法制度に関する調査

第一次調査サマリー（英国）

法域	英国		
1. 調査対象の法令・ガイドラインの名称	UK General Data Protection Regulation2016/679（UK GDPR）及び Data Protection Act 2018（2018 年データ保護法）	2012 年自由保護法（Protection of Freedoms Act 2012）（PoFA）及び Surveillance Camera Code（of practice）（監視カメラ規範）	パブリックスペースでのライブ FRT の使用に関する ICO の意見
1.1 制定主体	英国議会	PoFA：英国議会 監視カメラ規範：主務大臣（Secretary of State）の制定及び英国議会の承認	ICO
1.2 規律対象	UK GDPR 及び 2018 年データ保護法（パート 3 を除く）：民間部門及び公的部門（地方自治体を含む）双方 2018 年データ保護法（パート 3 のみ）：公的部門の法執行当局のみに適用（地方自治体を含む）	PoFA は国務大臣（Secretary of State）に監視カメラ規範の制定義務を課す。 監視カメラ規範は、監視カメラ規範を遵守する義務を負う公的機関である「関係当局」（地方自治体の公的機関を含む）に適用される。適用される「関係当局」（法執行機関を含む）は、PoFA の第 33 条（5）に基づいて指定された、警察当局及び地方当局をいう。	民間部門及び公的部門（地方自治体を含む）双方
2. 利用目的			
2.1 顔識別を利用する場合の根拠を要する規定又は利用目的を制限する規定	UK GDPR 及び 2018 年データ保護法（パート 3 を除く）が適用される限り、EU に関する回答は、現時点では英国にも等しく適用される。	－	監視カメラ規範の目的上、 「顔認識又は他の生体特徴認識システムのいかなる使用も、明示された目的を満たす上で明確に正当化され、かつ、釣り合いがとれたものでな

			ければならず、また、適切に立証されなければならない。個人に悪影響を及ぼすような決定(セクション 2.4 の原則 2) を下す前に、常に人間の介入が必要である。」
2.1A 許容される利用目的	常に個別のケースで目的の正当性、その目的に対する顔認証の妥当性・必要性を評価する必要がある。 ☒ 犯罪予防 ☒ その他（該当する場合）		
2.1B 禁止される利用目的	チェックされたものはいかなる場合も正当な目的とはみなされない。その他の項目については、一定の状況下では合法である可能性があること自体を否定することはできない。 ☒ 違法行為もしくは、不法行為であるもの、また又はそれらを助長するもの ☒ 差別的な取扱いを目的とするもの		
3. 撮影場所・撮影態様			
3.1 撮影場所を制限する規定	－	－	パブリックスペースを考慮すべきだが、最終的には、データ保護の一般法に従って個別に決定されなければならない。
3.2 許容される撮影場所	☒ 許容される場所の例示はない。		
3.3 許容される撮影態様	－	－	「特定の技術を推奨したり禁止したりすることは、コミッショナーの役割ではありません。むしろ、既存の法的枠組みが個人データの処理にどのように適用されるかを説明し、リスクとセーフガードの認識を促進し、法律を監視し執行することがコミッショナーの役割である。」

4. 撮影の事前同意を求める規定	顔画像/特徴量の記録又はその他の処理は、データ主体の事前同意（UK GDPR 第 6 条（1）(a)）又はその他の法的根拠（UK GDPR 第 6 条（1）(b) ～ (f)）に基づいて行うことができる。 生体認証データや、人種や宗教に関する情報など、センシティブなデータを処理するには、さらに厳しい要件がある。実際、UK GDPR 第 9 条（1）は、かかるデータの取扱いを禁止しているが、例外は UK GDPR 第 9 条（2）に定められている。	性質上、事前同意を得ることは予定されていない。	公共の場でのそのような処理のために依拠される合法的な根拠は同意ではなく、むしろそのような処理は実質的な公共の利益のために行われる場合にのみ合法的である可能性が高い。
5. 顔特徴量の取扱いに関する規定		－	－
6. 透明性・説明責任			
6.1 撮影の公表・掲示を求める規定	UK GDPR 第 5 条（1）(a)、第 12 条～第 14 条によると、データ主体は、実施されている個人データの取扱いについて十分に知らされなければならない。	監視カメラ規範第 3 原則（透明性）	
6.2A 通知公表や掲示が義務付けられている項目	☒　利用目的 ☒　処理方法 ☒　管理者の身元 ☒　管理者への連絡先 ☒　その他（該当する場合）： UK GDPR 第 5 条（1）(a)、第 12 条～第 14 条	☒　利用目的 ☒　処理方法 ☒　管理者の身元 ☒　管理者への連絡先 ☒　その他（該当する場合）	－
6.2B 通知の公表や掲示の方法に関する規律	☒　その他（該当する場合）：UK GDPR 第 12 条～第 14 条に基づく通知は、対象者が容易にアクセスできるものでなければならない。	－	☒　その他（該当する場合）
6.3 本人の同意取得時に示すべき事項	UK GDPR 第 7 条(3)及び(4)、 Recital 42 ☒　撮影主体	－	－

	☒ 撮影の目的 ☒ 撮影の範囲 ☒ 問合せ先 ☒ 撮影した画像の処理の方法と処理時間 ☒ その他（自由回答）		
6.4 保存に関する規定	データ処理の原則（UK GDPR 第 5 条）が適用される。	監視カメラ規範の第 6 原則は次のように述べている。 「監視カメラシステムの所定の目的に厳密に必要とされる以上の画像及び情報を保存すべきではなく、そのような画像及び情報は、それらの目的が果たされた後に削除されるべきである」。	p.45「データ管理者は、LFR システムを通じて収集されたすべてのデータを可能な限り短い期間保存しなければならない。多くの場合、数秒以内に「一致しない」生体認証テンプレートを削除できる。また、「一致」したテンプレートには、管理者が指定した目的を達成するために可能な限り短い保存期間を設定する必要がある。」
6.5 保存に関して規律される項目	☒ 個人データの登録基準	－	－
7. 救済手段			
7.1 救済手段に関する規定	EU の回答を参照のこと。	－	－
7.1A 適用される救済手段の項目	☒ 開示請求 ☒ 利用停止等請求 ☒ 苦情処理への対応：苦情が上記のデータ主体の権利の行使を含む場合、対応に関する法定の期限が存在する（ただし、他の苦情に関してはそれ以外の期限は存在しない）。 ☒ その他（該当する場合）	－	－

8. DPA の免許、届出又は監査を求める規定	ICO への登録が必要。	「監視カメラシステムがパブリックなスペースをカバーする場合はどこでも、システム運用者は、2001 年民間保安産業法（Private Security Industry Act）の法定免許要件を認識すべきである。これらの要件の下で、セキュリティ産業局（Security Industry Authority (SIA)）は、民間のセキュリティ産業の特定の部門で働く個人のライセンスを担当する。該当防犯カメラ（CCTV）ライセンスは、サービスが関連当局によって提供される場合であっても、サービス契約に基づいて作業員が提供される場合に必要とされる。」(監視カメラ規範　原則 5-5.6)	－
9. 外部監査を求める規定	各管理者には、その処理者（UK GDPR 第 28 条（3）(h)）による個人データの取扱いに関する一般的な監査権がある。かかる監査は、個別契約に応じて、第三者に委託することもできる。		
10. その他			
10.1 PIA の実施を求める規定	現時点では、GDPR に基づく EU の回答に記載したのと同じ規定が、UK GDPR に適用される。	事前の DPIA が必要であることを再確認し、この点に関する ICO ガイダンスを参照のこと。	事前の DPIA が実施されることを期待している。
10.2 AI を使用した個人データの自動処理を規制する規定	－		
10.3 特記事項	－		

令和 4 年度調査事業「主要国・地域における顔識別機能付カメラの利用に関する法制度」
第二次調査サマリー（英国）

1．裁判例、執行事例の調査結果

【主要な裁判例】

① 2020 年 8 月 11 日控訴院決定（Bridges v South Wales Police [2020] EWCA Civ 1058）

- 事案の概要：サウス・ウェールズ警察が公の場でライブ顔認識を実行したことに対し、ブリッジズ氏（公民権運動団体リバティが支援）が異議を申し立てた事例（プライバシー権、データ保護法、平等法に違反すると主張）。
- 判旨：2019 年、先の高等裁判所の審理では、顔認識はプライバシーの権利に干渉するものの、その法的枠組みは十分なセーフガードを提供していると判断されていたところ、控訴審である控訴院において、ブリッジズ氏は、こうした処理が私生活の権利（ECHR 第 8 条）の侵害、データ保護法および平等法の違反に相当し得ることを含む 5 つの根拠のうち 3 つで勝訴した。 しかし、サウスウェールズ警察による特定の利用が、ECHR 第 8 条の権利に対する不釣り合いな干渉であることや、リスク評価プロセスが正しく実施されていないことを証明することはできなかった。

② 2012 年 7 月 5 日調査権限審判所（Investigatory Powers Tribunal）決定（BA and others v Cleveland Police IPT/11/133/CH and IPT12/72/CH）

- 事案の概要：弱者である成人の家に、本人の同意のもと、事前の監視許可なく CCTV を設置し、その結果、彼女の介護者の一人が逮捕されたという警察の行為について検討したものである。
- 判旨：裁判所は、この行為が保護された監視の許可の対象ではなく、Art 8 の権利を侵害する違法行為はなかったと判断した。

③ 2013 年 2 月 19 日第一審判決(FTT)（サウサンプトン・シティ・カウンシル対情報コミッショナー EA/2012/0171）

- 事案の概要:認可を受けたタクシー車両に乗客を乗せ､継続的にオーディオビジュアルを記録することに関する事件｡英国個人情報保護監督機関(ICO)が先に出した録音中止の強制通知に対し、特にその処理が不当かつ違法であるとして、Southampton City Council が FTT に控訴した。Southampton City Council は、1）録音方針が機密性の高い個人情報に関わるものであること、2）音声データの録音と保存が乗客のプライバシー権に不釣り合いな干渉であることを争点にした。
- 判旨：FTT は、上記の争点 2 点について ICO を支持し、Southampton City Council の訴えを棄却した。

④ 2017 年 1 月 エディンバラ・シェリフ・コート（Edinburgh Sherriff Court）決定（Anthony Woolley and Deborah Woolley v Nahid Akbar or Akram）

- 事案の概要：監視カメラや音声記録装置を設置する不動産所有者や居住者は、その装置が敷地外の公共空間を監視する場合、データ保護法を遵守しなければならないとする隣人紛争の事件。
- 判旨：原告は、隣人による非常に侵入的な監視によって受けた「極度のストレス」が認められるとして、被告から原告に対して£17,268 の支払いが命じられた。

⑤　2021 年 10 月 12 日 オックスフォード郡裁判所決定（Dr Mary Fairhurst v Mr Jon Woodard）

- 判旨：家庭用ビデオ・オーディオ監視カメラの視野が所有者の敷地の家庭内境界を越えて広がることは、訴えられる迷惑行為ではなく、また責任者による他の行為がなければそれ自体が嫌がらせになる可能性もないが、データ保護法 2018 の違反となる可能性がある。

【主要な法執行事例】

① 2023 年 1 月 31 日英国個人情報保護監督機関（ICO）決定（ノース・エアシャー・カウンシル）

- 決定要旨：ICO は、North Ayrshire Council (NAC)が顔認識技術を使用して、学校の食堂で生徒の「キャッシュレス」ケータリングを管理していることを受けて、正式な書簡を発行した。これに対し、NAC は処理を停止した。

②　2022 年 5 月 23 日英国個人情報保護監督機関（ICO）決定（Clearview AI）

- 決定要旨：ウェブから収集した英国及びその他の地域の人々の画像をグローバルな顔認識データベースに使用したとして、ICO が Clearview AI に課した罰金額は 7,7552,800 ポンドにのぼる。

③ 2013 年 7 月 24 日英国個人情報保護監督機関（ICO）決定（ハートフォードシャー州警察）

- 決定要旨：ICO は、ハートフォードシャー州警察に対し、ロイストンの町を囲む車両用自動ナンバープレート認識カメラの使用を見直すよう、強制的な通達を出した。カメラの使用は非常に広範囲に及んでいたため、ロイストンを車で出入りする際に、その走行記録が記録されることは事実上不可能であった。ハートフォードシャー州警察は、ICO の介入を受け、カメラを削減した。

２．調査対象国における犯罪予防や安全確保のための顔識別機能付きカメラシステムの利用動向や主な設置主体の傾向（政府機関や自治体、民間事業者等）

該当する情報は見られなかった。

３．調査対象国内における顔識別機能付きカメラに係る政策立案の状況（法令整備を含む。）や世論の動向等

報告書多数あるが、その内容としては以下の事項を含む。

① 顔認識カメラ及び監視カメラの所有者及び管理者についての一般的な情報

② 顔認識カメラ及び監視カメラの利用方法に関する一般的な情報

③ 顔認識カメラや監視カメラに関する世論

第 6 章　ドイツ（ドイツ連邦共和国）

主要国・地域における顔識別機能付カメラシステムの利用に関する法制度に関する調査

第一次調査サマリー（ドイツ）

法域	ドイツ					
1. 調査対象の法令・ガイドラインの名称	ドイツ連邦データ保護法（German Federal Data Protection Act）（Bundesdatenschutzgesetz）（BDSG）	ドイツ連邦著作権法（写真及び視覚美術）（German Copyright Act for Photographic and Visual Art）（Kunsturhebergesetz）（KUG）	ドイツ刑法（German Criminal Code）（Strafgesetzbuch）（StGB）	連邦警察法(Federal Police Act)（Bundespolizeigesetz）（BPolG） Hamburg Law on the Protection of Public は Safety and Order (SOG) Law on data processing of the Hamburg police (HmbPolDVG) etc.)	民間企業によるビデオ監視に関するガイドライン（“Orientierungshilfe Videoüberwachung durch nicht-öffentliche Stellen” vom 17. Juli 2020, only available in German）（ＤＳＫガイドライン）	生体認証解析に関する DSK のポジションペーパー（a positioning paper of the DSK on biometric analysis）（“Positionspapier zur biometrischen Analyse” vom 3. April 2019, only available in German）（ポジションペーパー）
1.1 制定主体	ドイツ連邦議会			BPolG:ドイツ連邦議会 SOG 及び HmbPolDVG：ハンブルグ州議会	Conference of German Data Protection Authorities（Datenschutzkonferenz）（DSK）	DSK
1.2 規律対象	民間部門及び公的部門（地方自治体を含	GDPR と抵触する可能性が指摘		BPolG：連邦警察 SOG 及び	民間部門及び公的部門（地方自治体	民間部門及び公的部門（地方自体を

	む）双方（ただし、民間部門についてはGDPRが優先し、適用されない可能性が指摘されている）	されている。		HmbPolDVG：ハンブルグ州警察	を含む）双方	含む）双方
2. 利用目的　※「－」と記載の項目についてEUの回答も参照のこと（以降、同じ）						
2.1 顔識別を利用する場合の根拠を要する規定又は利用目的を制限する規定	－					
2.1A 許容される利用目的	－					
2.1B 禁止される利用目的	－					
3. 撮影場所・撮影態様						
3.1 撮影場所を制限する規定	EU の回答を参照のこと。 BDSG第4条が適用される限りにおいては（すなわち公的部門である場合）、ビデオ監視は、同条に定める要件を充足する場合のみ、許容される。	－	StGB 第 201 条、第 201a 条	HmbDSG が適用される限り、ビデオ監視は、①公的機関がその業務を遂行すること、②公的機関が、アクセスの可否を決定する権限を行使することのいずれかに必要で、かつ、データ主体の利益を上回る正当性が認められるときにのみ、許容される。	－	－
3.2 許容される撮影場所	－					
3.3 許容される撮影態様	－	－	－	ドイツ警察法は（顔認識の使用にかかわらず）ビデオ記録の保存/	－	－

				削除の義務を定めている。		
4. 撮影の事前同意を求める規定	－	KUG 第 22 条及び第 23 条が適用される場合、人物の映像の公開・共有には、撮影された本人の同意が必要である。 ただし、現代美術や高度な芸術性が認められる場合など、一定の例外が認められている。	－	－	－	－
5. 顔特徴量の取扱いに関する規定	－	－	－	－	－	ポジションペーパーでは、様々な生体認証のセンサー及びシステムを説明している。
6. 透明性・説明責任						
6.1 撮影の公表・掲示を求める規定	LED を国内法化するため、ドイツ国内法である BDSG は、独自の透明性義務を導入した（BDSG 第 4 条（2））。	－	－	LED を国内法化するため、ドイツ国内法である警察法は、独自の透明性義務を導入した（BPolG 第 27 条、HmbDSG 第 9 条(3)）。	－	－

6.2A 通知公表や掲示が義務付けられている項目	－					
6.2B 通知の公表や掲示の方法に関する規律	－					
6.3 本人の同意取得時に示すべき事項	－					
6.4 保存に関する規定	－	－	－	ドイツ警察法は（顔認識の使用にかかわらず）ビデオ記録の保存/削除の義務を定めている。	－	－
6.5 保存に関して規律される項目	－					
7. 救済手段						
7.1 救済手段に関する規定	GDPR が適用されるので、EU の回答を参照のこと。差し止め及び損害賠償請求に関しては、ドイツの民事法及び行政法が適用される。				－	－
7.1A 適用される救済手段の項目	☒ 開示請求 ☒ 利用停止等請求 ☒ 苦情処理への対応 ☒ その他（該当する場合）：上記参照のこと。				－	－
8. DPA の免許、届出又は監査を求める規定	－					
9. 外部監査を求める規定	－					
10. その他						
10.1 PIA の実施を求める規定	－				さらに、DSK は、GDPR 第 35 条（4）を踏まえたいわゆるブラックリスト を	

		公表している。民間部門のブラックリスト No.1 によれば、生体認証データを取り扱い、かつ、以下のいずれかを行う場合、DPIA が必要である。 ・弱者のデータを取り扱う場合 ・システマティックなモニタリング ・新規の技術的又は組織的なソリューションのイノベーティブな利用又は適用 ・アセスメント又は分類(スコアリング) ・データセットのマッチング又は統合 ・法的効果又は類似の重大な効果を伴う自動的な決定 ・データ主体が権利行使、サービスの利用、契約の遂行を妨げられる場合 公的部門については、このようなブラックリストは、地域ごとに、書く DPA が公表している。たとえば、ハンブルグ州の公的部門向けのブラックリスト は、民間部門向けブラックリスト No.1 と同一である。
10.2 AI を使用した個人データの自動処理を規制する規定	−	
10.3 特記事項	−	

1．裁判例、執行事例の調査結果

【主要な裁判例】

＜Bundesverfassungsgericht (BVerfG) – Federal Constitutional Court＞

① **BVerfG, Urt. v. 18.12.2018 - 1 BVR 142/15**

- 判旨：裁判所は、バイエルン州警察タスク法（以下、BayPAG）に基づく自動車のナンバープレートの自動監視を、情報的自己決定権の侵害として一部違憲であると判断した。バイエルン州では、警察は自動化されたナンバープレートチェックを実施する権限を与えられている。このプロセスでは、通過する車両のナンバープレートがナンバープレート読み取りシステムによって覆面下で自動的に記録され、場所、日付、時間、進行方向に関する情報とともに保存され、指名手配中のナンバープレート番号のデータベースと比較される。身元確認は、重要な法的利益に対する危険または差し迫った危険がある場合にのみ許される（第 13 条 I BayPAG)。

  まず、このようなチェックは、チェックの結果がヒットするかどうかにかかわらず、ナンバープレートを記録し比較されるすべての人の基本的権利を妨害するものであるとの判決が下された。技術的な理由だけで対象を絞らないデータ収集を不干渉とする判例は適用されず、不干渉はその人に対する調査結果がないことを条件としてなされるからである。したがって、ナンバープレートの自動チェックは、その侵入的な性質に鑑み、少なくとも相当な重みを持つ法的資産の保護、または同等の重みを持つ公益に役立ち、その目的に関して合理的であることが必要である。

  第二に、人または財産の的を絞った捜索のための警察のチェックは、理由なく許されるものではなく、客観的に判断され、限定された重大な理由が必要であることである。ドラグネット規制の手段として、比例原則により、免許証のチェックは、国境との十分な具体的関連性を必要とする。

  第三に、透明性、個人の法的救済、監督管理に関する要件を満たす必要があり、データの使用と削除に関する規定が必要である。

＜Bundesverwaltungsgericht (BVerwG) – Federal Administrative Court＞

① **BVerwG, 27.03.2019 – 6 C 2/18**

- 判旨：歯科医院内の公共エリアでの撮影について、標識を掲示するだけでは同意があったとはいえないとし、さらに、「犯罪の行為の予防と捜査」は正当な利益になり得るものの、一般生活よりも以上にリスクが高い場合に限定されるとして、撮影を行う法的根拠に欠けるという判断を下した。

＜Bundesgerichtshof (BGH) – Federal Court of Justice＞

① **BGH, 15.5.2018 – VI ZR 233/17**

- 判旨：ダッシュカムを使用して、公道を走行中に周囲を監視する際に、周囲のプライバシーを侵害するものであると結論づけた。

② **BGH, 24.5.2013 - V ZR 220/12**

- 判旨：民家にカメラを物理的に設置した場合の撮影が許容されるかを検討している。

＜Oberlandesgerichte (OLG) (high courts and courts of appeal of a federal state)＞

① **OLG Stuttgart, judgment of 18 May 2021 – 12 U 296/20** (not published in court's database)

- 判旨：スーパーマーケットの敷地内に設置された監視カメラによる撮影の違法性を検討している。

＜Bundesarbeitsgericht (BAG) – German Federal Labor Court＞

① **BAG, judgment of 28 March 2019 – 8 AZR 421/17** (see in particular marginal no. 38- 39)

- 判旨：過剰かつ永続的な従業員のビデオカメラによる監視は、重大な義務違反の合理的な疑いがある場合のみ許容される。

【主要な法執行事例】

ドイツ連邦各州ごとの個人情報保護監督機関による執行が多数、行われている。

２．調査対象国における犯罪予防や安全確保のための顔識別機能付きカメラシステムの利用動向や主な設置主体の傾向（政府機関や自治体、民間事業者等）

該当する情報は見られなかった。

３．調査対象国内における顔識別機能付きカメラに係る政策立案の状況（法令整備を含む。）や世論の動向等

Data Protection Conference ("DSK")より、多数のガイダンス・レポートが公表されているほか、Federal Data Protection Officer (BfDI)からも"Statement of the Federal Data Protection Officer on video surveillance"が公表されている。

第 7 章　フランス（フランス共和国）

主要国・地域における顔識別機能付カメラシステムの利用に関する法制度に関する調査

第一次調査サマリー（フランス）

法域	フランス			
1. 調査対象の法令・ガイドラインの名称	Law N° n° 78-17 of January 6, 1978 relating to information technology, data files and freedoms as amended (i.e. the “French Data Protection Act”)（フランスデータ保護法）	2019 年 1 月 10 日付の職場の敷地、設備、コンピューターアプリケーションへのアクセス・コントロールのための生体認証機器の使用についてのモデル規則（Règlement type）	2012 年 5 月 4 日付政令番号 2012-652 及び 2013 年 12 月 4 日付政令番号 2013-1113	CNIL ガイダンス（2019 年 11 月 15 日付の顔認識についての文書、2020 年 10 月 9 日付の空港におけるか認識についての CNIL の文書及び 2017 年 3 月 8 日付と 2018 年 7 月 24 日付の顔認識を含む生体認証の使用についての CNIL の文書）
1.1 制定主体	フランス議会	CNIL	フランス共和国大統領または首相	CNIL
1.2 規律対象	民間部門及び公的部門（地方自治体を含む）双方		管轄の国務大臣	民間部門及び公的部門(地方自治体を含む）双方
2. 利用目的				
2.1 顔識別を利用する場合の根拠を要する規定又は利用目的を制限する規定	－			
2.1A 許容される利用目的	フランスデータ保護法第 6 条に基づき、GDPR 第 9.2 条に規定される特定の状況を除き、（顔認識を含む）生体認証データの処理は禁止されている。 顔認識を含む特定の処理活動は、フランスの規制によって特定の目的のために許可され、規制される。 その他の処理活動については、当局は GDPR 第 9 条第 2 項の条件のいずれかを満たすかどうかを個別に評価する。 ☒　犯罪予防（被疑者の犯行防止、不法入国防止等）			

	☒　その他（該当する場合）：個別の事例ごとに、目的の正当性、並びに個々の事例におけるその目的のための顔認識の妥当性及び必要性を評価するための要件を検討する必要がある。			
2.1B 禁止される利用目的	フランスのデータ保護法第 6 条では、GDPR 第 9.2 条に言及されている特定の状況を除き、生体情報（顔認証を含む）の処理は禁止されている。 違法・不法行為、違法・不法行為を助長する行為、差別的取り扱いを意図した行為に顔認識付きカメラシステムを使用することは、いかなる場合も許可されたものとはみなされない。フランスでは、肌、色、人種の識別や宗教、その他の信条の識別のために顔認識装置を使用することも、GDPR 及びフランスデータ保護法に定められた要件をほとんど満たさないことになる。 ☒　原則として顔識別の利用が禁止されており、例外的に許容される利用目的がある。			
3. 撮影場所・撮影態様				
3.1 撮影場所を制限する規定	顔認識を実行する場所を制限する特定の法律、規制、ガイドラインはない。	－	－	CNIL は、カメラを用いて、以下の行為は決して行ってはならないと定めている。 ・特別な事情によりカメラの設置が必要な場合（例えば、従業員が金銭を扱う際のセキュリティ上の理由）を除き、従業員の作業風景を撮影すること。 ・休憩時間専用の場所（職員室、クローク、浴室、トイレ、学校の校庭、カフェテリアなど）や店舗の更衣室を撮影すること。 ・従業員代表、特に組合の事務所または施設専用のエリア（これらの事務所または施設にのみ通じる廊下を含む）を撮影すること。 ・個人宅の玄関または窓、個人用バルコニー、個人用テラスを撮影

				すること。
3.2 許容される撮影場所	特定の正当な目的のためには、特定の処理活動が必要でなければならない。そのため、いずれの場所でも撮影が許可される場合がある。 ☒その他（該当する場合）：上記のとおり。	－	－	－
3.3 許容される撮影態様	EU の回答を参照のこと。 ・GDPR 第 5 条（1）(b)、(c) ・GDPR 第 5 条（1）(a) ・GDPR 第 25 条（2）	－	－	－
4. 撮影の事前同意を求める規定	GDPR と EU のセクションの回答に従い、同意は、データ管理者が顔認証の文脈で処理されるような生体認証データを含む個人データの処理について、依拠できる法的根拠のひとつにすぎない。	モデル規則（Règlement type）に関する FAQ において、これらの特定の状況においては従業員の同意は必要ないことを明確にした。雇用者と従業員の間の力の不均衡により、従業員の同意はほとんどの場合自由ではなく、したがって GDPR に基づいて有効ではない。このため、CNIL は、別の法的根拠に依拠することを推奨している（同 FAQ の質問 15 を参照）。	空港での顔認証の使用は、利用者の同意がある場合のみ実施しなければならない。	CNIL は、特定の規則が顔認識の使用を許可している場合を除き、同意が最も適切な法的根拠となるべきであると考える傾向にあることがうかがわれる。
5. 顔特徴量の取扱いに関する規定	同上。なお、フランス議会が公表した、公共空間における生体認証認識に関する 2022 年 5 月 10 日に公表された報告書がある。			
6. 透明性・説明責任				
6.1 撮影の公表・掲示を求める規定	GDPR に基づき、フランスデータ保護法の第 48 条は、「情報に対する権利は、GDPR 第 12 条か	CNIL は、使用者は、GDPR 第 12 条以下でデータ主体に提供しなければならないと規定されている必	国境管理における顔認識の利用に関しては、個人情報主体の	(i) カメラの横には、最低限の情報（データ管理者の身元、法的根拠、画像の保存期間...など）とと

	ら第 14 条までに規定される条件の範囲内で適用される」と定めている。したがって、この点に関して EU の回答を参照のこと。	須の個人情報を、データ主体に提供しなければならないと述べている。	情報に対する権利は、GDPR 第 13 条に基づき、関係する空港、港湾及び鉄道駅の国境警察の長又は税関の責任者に対して行使することができる。	もに、カメラを表す記号を含む特定の標識が表示されるべきである。(ii) 他の関連情報を含むより包括的な情報の通知がデータ主体に提供されるべきである(例えば、インターネットのウェブサイト)。
6.2A 通知公表や掲示が義務付けられている項目	☒ 利用目的 ☒ 管理者の身元 ☒ 管理者への連絡先			
6.2B 通知の公表や掲示の方法に関する規律	☒ 通知公表や掲示の場所 ☒ その他（該当する場合）：上記参照のこと。			
6.3 本人の同意取得時に示すべき事項	☒ 撮影主体：データコントローラの情報詳細 ☒ 撮影の目的 ☒ 撮影の範囲（個人情報主体がそのデータを使って何が行われているかを完全に理解できるように詳細に説明する必要がある） ☒ 問合せ先 ☒ 撮影した画像の処理の方法 ☒ その他（自由回答）： ・加工目的 ・収集した個人データの分類 ・任意の時点で同意を撤回する権利の存在と GDPR の下で付与される法的権利（特に画像にアクセスする権利）の行使方法 ・データが EU 域外に転送されるかどうか ・その取扱いが、プロファイリングを含む、実施される自動化された取扱いに基づくものであるかどうか、及びその判断が、自然人に関して法的効果を生じさせるか、又は当該自然人に同様に重大な影響を及ぼすかどうか			

6.4 保存に関する規定	フランスデータ保護法第 4 条は、個人データは、「データ主体を特定できる形式で、そのデータ主体が処理される目的に必要な期間を超えない期間保存される」ものとし、「不正又は違法な処理に対する保護、偶発的な損失、破壊、損傷、又は権限のない者によるアクセスに対する保護を含む、適切なセキュリティが確保されるような方法で処理される」ものとする。	(i) データへのアクセスを許可された者（第 6 条）、(ii) 生体認証テンプレートが保存されなければならない条件（第 7 条）、(iii) 生体認証システムの一部として収集されたすべてのデータの保存期間（第 8 条）及び (iv) データ管理者が実施しなければならないセキュリティ対策のリスト（第 10 条）に関し、かかる種類の処理活動に対する特定の要件を規定している。	政令番号 2013-113 号：データの保持期間、及びデータへのアクセス方法とアクセス権者に関する要件 政令番号 2012-652：データの保存方法及びアクセスに関する制限（保持期間、データへのアクセス権者...など）	スマートフォンでの生体認証データの使用に関する CNIL のガイドラインには、生体認証データの保存方法に関する推奨事項も含まれている。
6.5 保存に関して規律される項目	☒ 個人データの登録基準 ☒ 登録された個人データの保存期間			
7. 救済手段				
7.1 救済手段に関する規定	・アクセス権（GDPR 第 15 条、フランスデータ保護法第 49 条） ・訂正権（GDPR 第 16 条、フランスデータ保護法第 50 条） ・消去権（GDPR 第 17 条、フランスデータ保護法第 51 条） ・処理の制限（GDPR 第 18 条、フランスデータ保護法第 53 条） ・データポータビリティ（GDPR 第 20 条、フランスデータ保護法第 55 条） ・異議申し立て（GDPR 第 21 条、フランスデータ保護法第 56 条） ・監督官庁に苦情を申し立てる権利（GDPR 第 77 条） ・補償（GDPR 第 82 条） さらに、義務に違反した者は、CNIL によって制裁を受ける可能性がある（フランスデータ保護法第 20 条～第 23 条）。			
7.1A 適用される救済手段の項目	☒ 開示請求 ☒ 利用停止等請求 ☒ 苦情処理への対応			

	☒ その他（該当する場合）：上記参照のこと。			
8. DPA の免許、届出又は監査を求める規定	フランスデータ保護法の第 32 条に基づき、フランス国家に代わって実施される、個人の身元の認証又は管理に必要な遺伝子データ又は生体認証データの処理は、CNIL の意見を受けた政令によって許可することができる			
9. 外部監査を求める規定	顔認証に関連する外部監査については、特定の法律やその他のルールはない。			
10. その他				
10.1 PIA の実施を求める規定	フランスデータ保護法第 90 条の下で、DPIA も必要とされるのは、公共の安全への脅威からの保護と脅威の防止を含む、犯罪の防止、捜査、探知、若しくは訴追、又は刑事罰の執行を目的とする個人データの処理が、関連する公的機関、又は公的機関から公的権限の行使を委託されたその他の団体若しくは事業体によって行われる場合であって、当該処理が個人の権利及び自由に対する高いリスクをもたらす可能性がある場合である。	CNIL はモデル規則において、そのような処理活動は DPIA の対象でなければならないと指摘している。	－	・空港での顔認識の使用に関するガイドライン ・スマートフォンにおける生体認証データの利用に関するガイドライン
10.2 AI を使用した個人データの自動処理を規制する規定	－			
10.3 特記事項	－			

令和 4 年度調査事業「主要国・地域における顔識別機能付カメラの利用に関する法制度」
第二次調査サマリー（フランス）

1．裁判例、執行事例の調査結果

【顔認識に関する主要な裁判例】

＜French Council of State＞

① 2022 年 4 月 26 日 French Council of State 決定

- 判旨：顔認識が可能な画像データを含む刑事裁判の記録の処理の違法性が争われた事案で、裁判所は違法性を否定した。

② 2020 年 11 月 4 日 French Council of State 決定

- 判旨：顔認識技術を用いるシステム（ALICEM）の処理の違法性が争われた事案で、裁判所は違法性を否定した。

＜Administrative Court of Marseilles＞

① 2020 年 2 月 7 日 Administrative Court of Marseilles 決定

- 地方政府が、学校に入校する際の本人確認に顔認識のシステムを導入する決定を下したことの違法性が争われた時点で、裁判所は違法性を認め、当該決定を取り消す判断を下した。

【顔認識に関する主要な執行事例】

① 2020 年 10 月 17 日 CNIL 決定

- 事案の概要：CLEARVIEW AI は、アカウントにログインすることなく閲覧できるすべての写真をオンラインで収集している。この収集により、同社は、写真を使って個人を検索することができる検索エンジンの形で、人物の画像データベースへのアクセスを販売していた。 そのために、同社は「バイオメトリックテンプレート」、つまり、人物の身体的特徴をデジタルで表現したものを作成する。画像がキャプチャされ、検索エンジンに含まれるほとんどの人は、自分がこの機能の影響を受けていることに気づいていなかった。
- 決定概要：CNIL は、GDPR の要件に対する以下の違反に関して、CLEARVIEW AI に 2,000 万ユーロの罰金を課した。CNIL が認定した主な違反事由は以下の通りである。

  1）法的根拠の欠如 法的根拠の欠如：CLEARVIEW AI は、自社のソフトウェアを提供するために写真を収集し使用することについて、データ対象者の同意を得ておらず、特にこのプロセスの特に侵入的で大規模な性質に鑑みて、このデータを収集し使用することに正当な利益を有していない。

2）データ主体の権利を遵守していないこと： CLEARVIEW AI は、データ主体のアクセス権の行使を促進せず、アクセスおよび消去の要求に対して効果的に対応しない。

3) CNIL との協力の欠如：CLEARVIEW AI は、同社に送られた管理質問書に部分的にしか回答せず、CNIL の会長によって出された正式な通知にも応じなかった。

２．調査対象国における犯罪予防や安全確保のための顔識別機能付きカメラシステムの利用動向や主な設置主体の傾向（政府機関や自治体、民間事業者等）

該当する情報は見られなかった。

３．調査対象国内における顔識別機能付きカメラに係る政策立案の状況（法令整備を含む。）や世論の動向等

顔認識、監視カメラのいずれについても、CNIL より、多数のガイダンス・レポートが公表されているほか Human Rights Defender、French Senate、French National Assembly 等の機関からも文書が公表されている。

第 8 章　スペイン（スペイン王国）

主要国・地域における顔識別機能付カメラシステムの利用に関する法制度に関する調査

第一次調査サマリー（スペイン）

法域	スペイン	
1. 調査対象の法令・ガイドラインの名称	・個人データの保護及びデジタル権の保証に関する 12 月 5 日の基本法 3/2018（スペイン語での頭文字をとった略称は LOPDGDD。以下「LOPDGDD」という。） ・さらに、顔認識機能を搭載したカメラを通じて実行された処理について、スペインのデータ保護機関（スペイン語の頭文字をとった略称は AEPD。以下「AEPD」という。）が発行した 3 つのレポートと決議がある。	2021 年 5 月 26 日付の基本法 7/2021（犯罪の予防、探知、捜査、訴追及び刑事罰の執行の目的で処理される個人データの保護に関する）（基本法 7/2021）
1.1 制定主体	LOPDGDD については代議員会。レポート及び決議については AEPD。	代議員会
1.2 規律対象	民間部門及び公的部門（地方自治体を含む）双方	公的部門（地方自治体を含む）のみ
2. 利用目的		
2.1 顔識別を利用する場合の根拠を要する規定又は利用目的を制限する規定	EU の回答を参照のこと。 決議及び報告は、欧州の規定（GDPR、ガイドラインなど）に基づいており、目的の制限に関する欧州の条項に定められている以上の規則を定めていない。	－
2.1A 許容される利用目的	☒　その他（該当する場合）：上記の通り。	－
2.1B 禁止される利用目的	EU の回答を参照のこと（チェック項目も同じ）。 ☒　違法行為もしくは、不法行為であるもの、また又はそれらを助長するもの ☒　差別的な取扱いを目的とするもの ☒　その他（該当する場合）：上記の通り	－
3. 撮影場所・撮影態様		
3.1 撮影場所を制限する規定	EU の回答を参照のこと。 さらに、LOPDGDD は第 89.2 条で「いかなる場合においても、労働者の休息または娯楽を目的とした場所への録音またはビデオ監視システムの設置は許可されない。ビデオ監視システムは、更衣室、トイレ、食堂、その他同様の場所など、労働者、公務員、公衆の休息や娯楽を目的とする場所には設置してはならない」と定め	－

	ている。	
3.2 許容される撮影場所	－	－
3.3 許容される撮影態様	EU の回答を参照のこと。	－
4. 撮影の事前同意を求める規定	EU の回答を参照のこと。 しかし、LOPDGDD は、第 9 条（2）で「スペインの規定に基づく GDPR 第 9 条（2）(g)、(h) 及び (i) に定める処理活動について、データの機密性及び安全性に関する追加要件を定めることができる法的地位を伴う規則の対象となるべきである」と定めている。現在、GDPR 第 9 条（2）(g) に基づく生体認証データの処理を規制する法律は存在しない。	－
5. 顔特徴量の取扱いに関する規定	EU の回答を参照のこと。	－
6. 透明性・説明責任		
6.1 撮影の公表・掲示を求める規定	LOPDGDD では、EU と同じ規定を適用し、すべての種類のデータ処理に同じ透明性要件が適用されることに留意すること。 さらに、LOPDGDD の第 11 条では、撮影画像について個人に通知するためにレイヤーシステムを使用する可能性があることを定めている。 この意味で、最初の層には、カメラが撮影しているという事実、データ管理者の身元、権利行使の可能性、個人が GDPR 第 13 条に規定された残りの情報にアクセスする方法に関する情報のみを含める必要がある。 第 2 層には、GDPR 第 13 条が要求するすべての情報を含めなければならない。	－
6.2A 通知公表や掲示が義務付けられている項目	☒　利用目的 ☒　管理者の身元 ☒　管理者への連絡先 ☒　その他（該当する場合）： EU の回答（GDPR 第 12 条、第 13 条、第 14 条、EDPB ガイドライン 3/2019 pp.26-27）及び上記のレイヤーシステムに関する情報を参照のこと。	－
6.2B 通知の公表や掲示の	☒　通知公表や掲示の場所	－

方法に関する規律	☒　その他（該当する場合）：データ主体には、個人データが最初に取得された時期及び場所を通知しなければならない。	
6.3 本人の同意取得時に示すべき事項	☒ 撮影主体 ☒ 撮影の目的 ☒ 問合せ先 ☒ 撮影した画像の処理の方法 ☒ その他：上記参照のこと。	－
6.4 保存に関する規定	EU の回答で示した規定及びコメントが適用されるので参照のこと。 さらに、LOPDGDD は、CCTV を通じて収集された画像に適用される第 22 条 (3) において、「データは、人、財産又は施設の完全性に反する行為が行われたことを証明するために保管しなければならない場合を除き、取得されてから最大 1 月以内に削除されなければならない。これらの場合には、画像は、記録の存在を知った時から最長 72 時間以内に、権限のある機関が利用できるようにしなければならない。」	－
6.5 保存に関して規律される項目	☒ 登録された個人データの保存期間 ☒ その他（該当する場合）：アクセス及び訂正義務、正確性義務、保護義務	－
7. 救済手段		
7.1 救済手段に関する規定	EU の回答で示した規定及びコメントが適用されるので参照のこと。	－
7.1A 適用される救済手段の項目	☒ 開示請求 ☒ 利用停止等請求 ☒ その他（該当する場合）：EU の回答を参照のこと。	－
8. DPA の免許、届出又は監査を求める規定	免許、届出の要件はない。 AEPD は、LOPDGDD 第 51 条から第 54 条に準拠した調査権限及び予防的監査スキームを有している。LOPDGDD 第 51 条から第 54 条の内容については、EU の回答を参照のこと。	－
9. 外部監査を求める規定	EU の回答で示した規定及びコメントが適用されるので参照のこと。	－
10. その他		

10.1 PIA の実施を求める規定	EU の回答で示した規定及びコメントが適用されるので参照のこと。 さらに、LOPDGDD の第 28 条は、処理活動の開始前に DPIA を実施しなければならないかどうかを判断するために、処理活動の枠内で考慮すべき主なリスクを定めている。具体的には、第 28 条 2 項(c)に以下のように記載されている。 「GDPR 第 9 条及び第 10 条並びに LOPDGDD 第 9 条及び第 10 条に言及される特別なカテゴリのデータ又は行政犯罪の遂行に関連するデータに単に付随又は付属しない処理が存在する場合」 さらに、AEPD は、DPIA を必要とするデータ処理の種類のリストを公表している。特に、このリストでは、次のような場合に DPIA を実施すべきとされている。 「自然人を一意に識別するための生体認証データの使用を伴う処理作業」	－
10.2 AI を使用した個人データの自動処理を規制する規定	EU の回答で示した規定及びコメントが適用されるので参照のこと。	－
10.3 特記事項	－	

令和 4 年度調査事業「主要国・地域における顔識別機能付カメラの利用に関する法制度」
第二次調査サマリー（スペイン）

1．裁判例、執行事例の調査結果

【主要な裁判例】

① 2021 年 2 月 15 日 JUDGMENT 72/2021 OF THE BARCELONA PROVINCIAL COURT

- 事案の概要：スペイン最大のスーパーマーケットチェーンである Mercadona（「メルカドーナ社」）の一部店舗において、2 人の人物が接近禁止命令を言い渡された。現実問題として、メルカドーナ社側では店舗へのアクセスをコントロールできないため、前述の接近禁止命令を執行することが不可能であることから、同社は裁判所に対し、2 名を特定するための電子的手段を導入するよう要請した。
  メルカドーナ社は、顔認識技術を用いたビデオ監視システムにより、有罪判決を受けた者の店舗への入店を検知する自動システムの設置を認めるよう裁判所に要請していた。メルカドーナ社側は、このシステムから得られる個人データの処理は、公共の利益と、メルカドーナが被害者または被告となった裁判の判決を確実に遵守するという正当な利益によって正当化されると主張していた。

- 判旨：メルカドーナの主張にもかかわらず、バルセロナ州裁判所は、このシステムは私生活への侵入を伴うとして、メルカドーナ社の主張を認めなかった。同裁判所は、スーパーマーケットチェーンが提案したシステムは、十分な法的根拠がないままバイオメトリックデータを処理することになり、顔認識技術を用いたビデオ監視システムの使用は、バイオメトリックデータが自然人を明確に識別するために使用されるため、特殊な個人データの取り扱いを意味すると述べた。特別なカテゴリの個人データの処理は、GDPR 第 9 条 2 項に含まれる例外が適用されない限り、原則として GDPR によって禁止されている。
  判決では、GDPR 第 9 条 2 項(g)の例外を適用するためには、法律の地位を有する規則に明示的に規定された本質的な公共の利益が存在することが必要であると述べている。バルセロナ州裁判所は、現在、スペインの法制度において、顔認識技術の使用を許可する規則は存在しないことを強調している。同判決はさらに、顔認識技術から派生する処理は、このシステムが基本的権利に非常に悪い影響を与える可能性があるため、細心の評価を必要とすると述べている。この評価は、データの性質や起源、処理の手段、そして何よりも処理の目的など、さまざまな側面を考慮する必要があります。これらの側面は、データ保護原則とともに分析され、実施された措置がデータ主体の私的領域への侵入に適切であるかどうかを判断しなければならない。
  以上のことから、バルセロナ州裁判所は、顔認識技術を用いたビデオ監視システムから派生する処理は、スペインの法制度には識別目的のバイオメトリックデータ処理を認める規定がないため、公共の利益を根拠として実施することはできないと結論付けた。

【主要な執行事例】

① AEPD RESOLUTION IN THE SANCTIONING PROCEDURE 120/2021

- 事案の概要：スペイン最大のスーパーマーケットチェーンである Mercadona（「メルカドーナ社」）は、メルカドーナまたはその従業員に対して最終判決や接近禁止命令を受けた人を特定する目的で、2020 年に一部の店舗で顔認証システムを導入した。

- 決定概要：AEPD は、メルカドーナ社が行う上記処理の法的根拠を検討した。AEPD は、メルカドーナが行う処理の法的根拠としての公共の利益（GDPR 第 6 条(1)(e)）は、規則で規定される必要があるため、本件では適用されないとした。
  上記に加え、AEPD は、以下の要件 （i）当該処理が、法律の地位を有する欧州法または国内法の規則によって規定されていること。（ii）当該欧州規則または国内法が、個人データの保護に対する権利の制限を正当化する必須の公共の利益を特定していること；（iii）欧州の規則または国内法は、個人データ保護の権利を制限することができる状況を決定し、その制限とその結果をデータ主体が予見できるようにしなければならない（iv）欧州の規則または国内法は、採用されるべき適切な保護措置を決定しなければならない、を満たす必要があるため、GDPR 第 9 条 2 項（f）の例外も適用できないとした。
  さらに、AEPD は、リスクの高い処理を開始する前に、データ保護の影響評価を実施し、処理を妨げるような問題を適切に検出することが必要であると定めている。
  また、AEPD は、（i）メルカドーナが設置した看板には、このシステムが顧客保護を目的としていることが示されていたが、このシステムの最終目的はメルカドーナの施設とその従業員を守ることであり、（ii）メルカドーナはデータ対象者にどのメルカドーナの店舗が顔認識システムを導入したかを明確に知らせず、（iii）メルカドーナは適用した顔認識処理で適用したロジックについて意味のある情報を提供せず、データ対象者に処理の即時性に対する権利行使をも認めず、透明性の義務を怠ったものと認定した。

２．調査対象国における犯罪予防や安全確保のための顔識別機能付きカメラシステムの利用動向や主な設置主体の傾向（政府機関や自治体、民間事業者等）
該当する情報は見られなかった。

３．調査対象国内における顔識別機能付きカメラに係る政策立案の状況（法令整備を含む。）や世論の動向等
AEPD より、複数のレポートが公表されている。

第９章　オランダ

主要国・地域における顔識別機能付カメラシステムの利用に関する法制度に関する調査

第一次調査サマリー（オランダ）

法域	オランダ		
1. 調査対象の法令・ガイドラインの名称	カメラ監視に関する一般的なガイドライン （カメラ監視ガイドライン）	顔認識機能を備えたカメラシステムに特化したガイダンス （顔認識ガイダンス）	オランダ GDPR 施行法（the Dutch GDPR Implementation Act ）（GDPR 施行法）
1.1 制定主体	オランダデータ保護機関（the Dutch Data Protection Authority）（DPA）	オランダデータ保護機関（the Dutch Data Protection Authority）（DPA）	オランダ議会
1.2 規律対象	民間部門及び公的部門双方	民間部門及び公的部門（地方自治体を含む）双方	民間部門及び公的部門（地方自治体を含む）双方
2. 利用目的			
2.1 顔識別を利用する場合の根拠を要する規定又は利用目的を制限する規定	－	－	GDPR 施行法第 29 条 「GDPR 第 9 条(2)(g)について、人間の識別を目的とする生体認証データ処理の禁止は、当該処理が認証（authentication）又はセキュリティのために必要な限り、適用されない。」 なお、同条は改正の予定あり。
2.1A 許容される利用目的	☒　犯罪予防		
2.1B 禁止される利用目的	☒　違法行為もしくは、不法行為であるもの、また又はそれらを助長するもの ☒　差別的な取扱いを目的とするもの。 ☒　性格特性、内的感情、精神状態の特定		

	☒　人の肌の色、人種の判別 ☒　宗教上又はその他の信条の判別 ☒　商業利用 ☒　その他（該当する場合）		
3. 撮影場所・撮影態様			
3.1 撮影場所を制限する規定	カメラ監視ガイドラインは、カメラ監視一般について、以下のように述べている（40 頁目）。 「公共の場所における公共の秩序を目的とするカメラ監視は市町村法（the Municipalities Act）第 151c 条のもとで、地方自治体のみに認められている。しかしながら、これは、民間組織が公共の場所の一部を時々使用している事実から導かれるものではない。民間組織は、公共スペースで民間組織が使用する場所の撮影が、ケアを託された人間及び財産の保護のために避けられない場合のみ、カメラ監視を許容される。」	－	－
3.2 許容される撮影場所	－		
3.3 許容される撮影態様	－		
4. 撮影の事前同意を求める規定	－	顔認識ガイダンスでは、顔認識カメラの利用について有効な同意であるために遵守しなければ	－

5. 顔特徴量の取扱いに関する規定	－	ならない要件についての情報を示している。もっとも、その内容は、ＥＵ法と比較して異なるところはない。	－
6. 透明性・説明責任			
6.1 撮影の公表・掲示を求める規定	オランダ刑法（the Dutch Criminal Code）第 441b 条は、公共のスペースにおける隠しカメラによる人物の違法な録画を罰則対象と定めている。さらに、GDPR と同様の透明性要件が適用される。		
6.2A 通知公表や掲示が義務付けられている項目	☒ 利用目的 ☒ 管理者の身元 ☒ 管理者への連絡先 ☒ その他（該当する場合）： EU の回答を参照のこと（＝GDPR 第 12 条、第 13 条、第 14 条、EDPB ガイドライン 3/2019 pp.26-27 を参照のこと）		
6.2B 通知の公表や掲示の方法に関する規律	☒ その他（該当する場合）：EU の回答を参照のこと（＝データ主体には、当該個人データが最初にいつどこで収集されたのかを知らせなければならない（例：現地における告知（EU の回答セクション VI 参照のこと。））。		
6.3 本人の同意取得時に示すべき事項	EU の回答を参照のこと。		
6.4 保存に関する規定	－	DPA は、カメラ画像は、詐欺事件などの正当化する理由がない限りは、4 週間以上保存すべきでない、との意見を、監視カメラガイダンスにて示している。	EU の回答を参照のこと
6.5 保存に関して規律される項目	－		
7. 救済手段			
7.1 救済手段に関する規定	－	－	EU の回答を参照のこと。 加えて、データ管理者が GDPR 第 15 条から第 22 条に定められている権利行使について書面上の決定を下す場合は、データ主体は、裁判所

			に、データ管理者の決定について、当該決定について提訴することができる（GDPR 施行法第 35 条)。
7.1A 適用される救済手段の項目	－	－	☒ 開示請求 ☒ 利用停止等請求 ☒ 苦情処理への対応 ☒ その他（該当する場合)：上記参照のこと。
8. DPA の免許、届出又は監査を求める規定	－	－	EU の回答を参照のこと。
9. 外部監査を求める規定	－	－	EU の回答を参照のこと。
10. その他			
10.1 PIA の実施を求める規定	－	－	EU の回答を参照のこと。
10.2 AI を使用した個人データの自動処理を規制する規定	－	－	顔認識に関連して、AI を使用した個人データの自動処理を規則する法令、規則又はガイドラインはない。
10.3 特記事項	・GDPR 施行法第 29 条は、改訂される可能性がある。新しいドラフトでは「セキュリティ目的であり、かつ、特定の場所、建物、サービス、製品、情報システム又は業務プロセスのシステムに合法的にアクセスすることに一般的な超越する利益が認められ、当該利益に必要な限度で」とされている。このドラフトはかなり高い確率で変更になるので、留意すべきである。 ・2020 年 12 月 15 日、DPA はスーパーマーケット内の顔認識の利用に関して、スーパーマーケットに対して警告するプレスリリース を公開した。(同プレスリリース内で) DPA は、顔認識は、スーパーマーケットのセキュリティのためには必要とはいえない、と述べた。DPA の言葉を借りれば「スーパーマーケットは原子力発電所ではない」という言い回しをしている。		

令和 4 年度調査事業「主要国・地域における顔識別機能付カメラの利用に関する法制度」
第二次調査サマリー（オランダ）

1．裁判例、執行事例の調査結果

【主要な裁判例】

① 2022 年 9 月 28 日 District court of Zeeland-West-Brabant 判決

- 事案の概要：従業員と雇用主との間の紛争事案である。従業員は、勤務時間中、コンピュータのカメラをつけたままにするよう雇用主から指示されたが、これに従わなかったところ、「勤務拒否」と「不服従」を理由に解雇されていた。
- 判旨：裁判所によると、雇用主が解雇の理由を十分に明確にしていなかったため、解雇は法的に無効であった。さらに、就業拒否を証明することができず、雇用主による合理的な指示もなかった。カメラをつけたままにするような指示は、従業員の私生活尊重の権利に反すると判断された。

② 2022 年 7 月 18 日 District court of Amsterdam 判決

- 事案の概要：アパートの所有者が共同住宅を撮影するカメラを設置したため、アパートの所有者とオーナーズ・アソシエーションの間で争われた事案である。
- 判旨：裁判所は、アパートの所有者が自分の住居の外にある物や人の画像を記録・保存していたことから、GDPR の文脈における個人データの処理に該当すると判断した。このような処理は、データ主体またはその財産が撮影されている人の同意があるか、データ主体の利益を上回る正当な利益がある場合にのみ許可される。アパートの所有者は、住人の誰からも同意を得ていなかった。アパートの所有者は、自分の住居の周囲で強盗が発生したことを証明できず、集合住宅の入り口にはすでにカメラが設置されており、物件はすでに監視されていることになるので、アパートの所有者はカメラを設置する正当な利益を有しない。したがって、共同住宅を撮影しているカメラは撤去されなければならない。

以上のことから、バルセロナ州裁判所は、顔認識技術を用いたビデオ監視システムから派生する処理は、スペインの法制度には識別目的のバイオメトリックデータ処理を認める規定がないため、公共の利益を根拠として実施することはできないと結論付けた。

③ 2021 年 11 月 9 日 District court of Amsterdam 判決

事案の概要：オーナーズ・アソシエーションが集合住宅に新しいカメラを設置したため、オーナーズ・アソシエーションと住民の間で争われた事案である。カメラは、集合住宅のすべての共用部分に設置され、集合住宅への通路やエレベーターを対象としている。オーナーズアソシエーションは、自社と居住者の財産を守るため、また、必要に応じて、セキュリティ事故の報告や、エレベーターなどの不正使用による損害の回復のために、カメラを設置したものである。

判旨：裁判所は、オーナーズ・アソシエーションはカメラを撤去する必要はないと結論付けた。

【主要な執行事例】

① Fine for the lack of risk analysis in using camera cars

- 事案の概要：2022 年 12 月 21 日、オランダの DPA は、ロッテルダムで COVID-19 のパンデミックを治すために配備された 2 台のカメラカーを使用したとして、警察署長に 5 万ユーロの罰金を課した。ロッテルダム市と警察は、5 週間にわたり、360 度カメラを搭載した 2 台の車を配備し、個人が 1.5 メートルの距離を保っているかどうかを監視した。収集された画像はコントロールルームで閲覧、保存され、他の警察拠点に転送することが可能であった。
- 決定概要：DPA は、警察署がデータ保護影響評価（DPIA）を行わなかったとみなしている。しかし、警察がカメラを配備する際に新しい技術を使用していたため、カメラ付き車両を配備することがデータ対象者に高いリスクをもたらす可能性があることを警察は知ることができたため、DPIA は必要であった。

２．調査対象国における犯罪予防や安全確保のための顔識別機能付きカメラシステムの利用動向や主な設置主体の傾向（政府機関や自治体、民間事業者等）

該当する情報は見られなかった。

３．調査対象国内における顔識別機能付きカメラに係る政策立案の状況（法令整備を含む。）や世論の動向等

研究報告やガイダンス等、複数のレポートが公表されている。

第 10 章　スイス（スイス連邦）

主要国・地域における顔識別機能付カメラシステムの利用に関する法制度に関する調査

第一次調査サマリー（スイス連邦・チューリッヒ州）

法域	スイス連邦					チューリッヒ州
1. 調査対象の法令・ガイドラインの名称	2005 年 12 月 16 日の外国人及び外国人の統合に関する連邦法（FNIA）	2018 年 8 月 15 日の査証の入国及び発給に関する規則（OEIV）	・1992 年 6 月 19 日のデータ保護に関する連邦法（Federal Act on Data Protection of 19 June 1992）（FADP） ・2020 年 9 月 25 日の（新）連邦データ保護法（(new) Federal Act on Data Protection of 25 September 2020）（新 FADP）	2018 年 9 月 28 日の刑事問題におけるシェンゲン協定適用内のデータ保護に関する連邦法（SFADP）	連邦データ保護・情報コミッショナー（Federal Data Protection and Information Commissioner）（FDPIC）による、ビデオ監視に関するファクトシートと詳細情報	チューリッヒ州 2007 年 2 月 12 日情報及びデータ保護に関する法律（AIDP/ZH）
1.1 制定主体	スイス連邦議会				FDPIC	チューリッヒ州議会
1.2 規律対象	民間部門及び公的部門（地方自治体を含む）双方		民間部門及び公的部門（地方自治体**を含まない**）双方	公的部門（地方自治体**を含まない**）のみ	民間部門及び公的部門（地方自治体**を含まない**）双方	チューリッヒ州の公的部門のみ
2. 利用目的						
2.1 顔識別を利用する場合の根拠を要する規定又は利用目的を制限する規定	空港における顔認証システムの具体的なユースケース	空港における顔認証システムの具体的なユースケースについ	FADP 第 4 条(3) 新 FADP 第 6 条(3)	SFADP 第 4 条(3)	－	ADIP/ZH 第 9 条(1)

	について、FNIA 第 103 条	て、OEIV 第 54 条～第 62 条				
2.1A 許容される利用目的	特定の目的のための一般的な許可はない。顔認識システムを使用するたびに、それぞれの目的の妥当性と必要性を個別に評価する必要がある。 ☒ その他（該当する場合）：上記の通り。					
2.1B 禁止される利用目的	チェックされた項目は、いかなる状況においても許容されるとはみなされないので要注意。その他の項目は、特定の状況下では許されるかもしれないということ自体を否定することはできない。 ☒ 違法行為もしくは、不法行為であるもの、また又はそれらを助長するもの ☒ 差別的な取扱いを目的とするもの。					
3. 撮影場所・撮影態様						
3.1 撮影場所を制限する規定	空港における顔認証システムの具体的なユースケースについて、FNIA 第 103 条	空港における顔認証システムの具体的なユースケースについて、OEIV 第 54 条～第 62 条	比例性 ・FADP 第 4 条(2) ・新 FADP 第 6 条(2) 透明性 ・FADP 第 4 条(3) ・新 FADP 第 6 条(4)	比例性 SFADP 第 4 条(2) 透明性 SFADP 第 4 条(3)	FDPIC ウェブサイト https://cutt.ly/xK5C85I	比例性 ADIP/ZH 第 8 条(1)
3.2 許容される撮影場所	合法性／許容性は一般データ保護法のみに準拠し、個々のケースで評価する必要がある。 ☒その他（該当する場合）：	－	－	－	－	－

	上記のとおり。					
3.3 許容される撮影態様	顔認識が行われる方法を制限する特定の法律、規制、又はガイドラインはない。 したがって合法性は一般的なデータ保護法にかかっている。	OEIV 第 58 条	データセキュリティの観点から、 ・FADP 第 7 条（1） ・新 FADP 第 8 条(1)	－	－	－
4. 撮影の事前同意を求める規定	－	－	当局が使用する場合、法的根拠が必要 ・ FADP 第 17 条 新 FADP 第 5 条（c） （4）では、自然人を一意的に識別するバイオメトリックデータを、センシティブな個人データとみなされることになる。FADP 第 4 条（5）及び新 FADP 第 6 条（7）(a) によれば、同意が処理の根拠となる場合（上	当局が使用する場合、法的根拠が必要 ・SFADP 第 6 条	－	当局が使用する場合、法的根拠が必要 ・AIDP/ZH 第 8 条

			記参照)、それは、センシティブデータの場合には明示的でなければならない。			
5. 顔特徴量の取扱いに関する規定	－	－	FADP 第 3 条(e) 新 FADP 第 5 条(d)	SFADP 第 1 条	－	AIDP/ZH 第 3 条(5)
6. 透明性・説明責任						
6.1 撮影の公表・掲示を求める規定		・FADP：機密性の高い個人データまたは個人プロファイルを収集する場合にのみ発生する限定的な情報義務がある（FADP 第 14 条)。 ・新 FADP：データが収集されるたびに情報提供義務が発生する（新 FADP 第 19 条以下)。	－	－	チューリッヒ州のデータ保護委員会のガイドライン：ビデオ監視を使用する州政府当局は、透明性の理由からビデオ監視に関する特定の規則を発行する必要がある（ガイドライン、p.4)。	データ収集の際にはそのたびにデータ主体に情報を提供しなければならない（ADIP/ZH 第 12 条)。
6.2A 通知公表や掲示が義務付けられている項目	FADP ☒ 利用目的 ☒ 管理者の身元 ☒ 管理者への連絡先 ☒その他：情報義務は、データの開示が計画されている場合には、データ受領者のカテゴリも含む。さら					AIDP/ZH ☒ 利用目的 ☒ 管理者の身元 ☒ 管理者への連絡先 ☒その他

	に、第 14 条（2）は、必要な情報を例として挙げている。個々のケースによっては、さらなる情報が必要となる場合がある。 新 FADP ☒ 利用目的 ☒ 管理者の身元 ☒ 管理者への連絡先 ☒その他：情報義務は、データの開示が計画されている場合には、データ受領者のカテゴリも含む。さらに、第 19 条（2）は、必要な情報を例として挙げている。個々のケースに応じて、さらなる情報が必要となる場合がある。					・収集されたデータ又はそのカテゴリ ・法的根拠 ・データの開示が計画されている場合は、データ受領者又はデータ受領者のカテゴリ ・データ主体の権利
6.2B 通知の公表や掲示の方法に関する規律	☒ 通知公表や掲示の場所 ☒ その他（該当する場合）：：一般に、データ主体は、個人データが最初に取得された時期及び場所について通知されなければならない。					－
6.3 本人の同意取得時に示すべき事項	上記、とりわけセクション IV を参照のこと。 ☒ 撮影主体 ☒ 撮影の目的 ☒ 撮影の範囲					
6.4 保存に関する規定	－	空港における顔認証システムの具体的なユースケースについて、OEIV 第 60 条	データ保護法の一般原則、特に比例原則（上記参照）及びデータセキュリティの原則（FADP 第 7 条、新 FADP 第 8 条）が適用される。	－	－	データ保護法の一般原則、特に比例原則（上記参照）及びデータセキュリティの原則（AIDP/ZH 第 7 条）が適用される。
6.5 保存に関して規律される項目	☒ 個人データの登録基準 ☒ 登録された個人データの保存期間				FDPIC のファクトシートによると、財産への損	チューリッヒ州のデータ保護コミッショ

		害又は人々への傷害を防止するためにビデオ監視によって収集されたデータのための 24 時間の保持期間は、この期間内に重要なイベントが発見されなければ、十分であると思われる。	ナーによると、ビデオ監視によって収集されたデータの保持期間は、監視の目的に応じて、24 時間から 100 日までの範囲になる（ガイドライン、p.5）。 ☒　登録された個人データの保存期間
7. 救済手段			
7.1 救済手段に関する規定	・アクセス権（FADP 第 8 条以下、新 FADP 第 25 条以下、SFADP 第 17 条以下） ・訂正権（FADP 第 5 条(2)、第 15 条、第 25 条(3)、新 FADP 第 32 条、及び 41 条(2)(a)、SFADP 第 19 条(2)） ・消去権（FADP 第 15 条及び第 25 条(3)、新 FADP 第 32 条(2)(c)及び第 41 条(2)（a)、SFADP 第 19 条(2)） ・処理の制限（SFADP 第 19 条(3)） ・データポータビリティ（新 FADP 第 28 条以下） ・異議申し立て（FADP 第 12 条(2)(b)、新 FADP 第 30 条(2)(b)、私人の管理者の場合にのみ適用される） ・補償（FADP 第 15 条(1)、新 FADP 第 32 条(2) 。スイス民法第 28a 条(3)及び債務法典第 41 条と連動する。公的機関が顔認識を適用する場合、可能な補償は関連する国家賠償法の対象となる）。 ・データ主体が、当局が自己の権利を侵害したと考える場合、データ主体は裁判所に対して、当局が違法な処理を中止し、違法な処理の結果を排除し、及び/又は処理の違法性を証明することを要求することができる。	－	・アクセス権（AIDP/ZH 第 20 条(2)） ・訂正権（AIDP/ZH 第 21 条(1)） ・消去権（AIDP/ZH 第 21 条）

7.1A 適用される救済手段の項目	☒ 開示請求 ☒ 利用停止等請求 ☒ その他（該当する場合）：上記参照のこと。		－	☒ 開示請求 ☒ その他（該当する場合）：上記参照のこと。
8. DPA の免許、届出又は監査を求める規定	ライセンスや通知の義務はない。 ただし、FDPIC は、連邦当局が FADP を遵守しているかどうかを調査することができる（FADP 第 27 条）。 FDPIC の私人に対する調査権は、現行法では、特にシステムエラーに限定されている（cf. FDPA 第 29 条(1)）。新 FADP ではそのような制限はなくなる（cf. 新 FDPA 第 49 条）。		－	チューリッヒ州では、州のデータ保護当局は、州の政府当局が AIDP/ZH を遵守しているかどうかを調査することができる（AIDP/ZH 第 34 条）。
9. 外部監査を求める規定	顔認識に関する外部監査については、具体的な法令等はない。 また、（一般的な）データ保護法は、顔認識に関して外部の機関による監査を義務付けていない。		－	－
10. その他				
10.1 PIA の実施を求める規定	顔認証に関連してプライバシー影響評価（PIA）を必要とする特定の法律、規制、ガイドラインは存在しない。 FADP はデータ保護影響評価（「DPIA」）を規定していないが、新 FADP には DPIA に関する規定が含まれる予定である。顔認識を伴うほとんどのビデオ監視は、新 FADP 第 22 条のもとで DPIA の対象となる。	法執行の分野では、SFADP 第 13 条は、データ処理がデータ主体の人格または基本的権利に高いリスクを伴う可能性がある場合、連邦当局に DPIA を実施することを義務付けている。	－	チューリッヒ州では、AIDP/ZH 第 10 条が（その文言によれば）、データ処理から生じる潜在的なリスクとは無関係に、データ主体の基本的権利のリスクを評価することを公共機関に義務付けている。

10.2 AI を使用した個人データの自動処理を規制する規定	－
10.3 特記事項	－

令和 4 年度調査事業「主要国・地域における顔識別機能付カメラの利用に関する法制度」
第二次調査サマリー（スイス）

１．裁判例、執行事例の調査結果

【主要な裁判例】

① 2020 年 11 月 13 日スイス連邦最高裁判所判決（Decision 6B_1282/2019） (BGE 147 IV 16)

- 事案の概要：交通トラブルの刑事裁判資料として、GoPro カメラで撮影した映像資料が提出され、証拠能力が争われた事案である。
- 判旨：今回のケースでは、なぜ違法に証拠を取得したのか、正当化する理由がない。本件では、交通トラブルの際の当該犯罪行為に必要な重大性がないため、本件では違法に取得された証拠を使用することはできない。

② 2020 年 9 月 1 日スイス連邦最高裁判所判決（Decision 6B_1468/2019） (BGE147 IV 9)

- 事案の概要：無許可のデモに参加し、財産に深刻な損害を与えたとして訴えられ、「平和の侵害」の罪で有罪判決を受けた人物。その有罪判決は、私有地だけでなく部分的に公共空間も撮影しているホテルの監視カメラで彼が確認されたからこそ可能だった。
- 判旨：裁判所によると、雇用主が解雇の理由を十分に明確にしていなかったため、解雇は法的に無効であった。さらに、就業拒否を証明することができず、雇用主による合理的な指示もなかった。カメラをつけたままにするような指示は、従業員の私生活尊重の権利に反すると判断された。

【主要な執行事例】

該当する事例は見られなかった。

２．調査対象国における犯罪予防や安全確保のための顔識別機能付きカメラシステムの利用動向や主な設置主体の傾向（政府機関や自治体、民間事業者等）

該当する情報は見られなかった。

３．調査対象国内における顔識別機能付きカメラに係る政策立案の状況（法令整備を含む。）や世論の動向等

以下の 5 つの研究報告やガイダンス等、複数のレポートが公表されている。

① Fact sheet on video surveillance by private persons

② Fact sheet on video surveillance of public places by private persons
③ Explanatory note on video surveillance in vehicles (dashcam)
④ Explanatory note on video surveillance at the workplace
⑤ Explanatory note on video surveillance in changing rooms and public bathrooms

第 11 章　オーストラリア（オーストラリア連邦）

主要国・地域における顔識別機能付カメラシステムの利用に関する法制度に関する調査

第一次調査サマリー（オーストラリア連邦・サウスウェールズ州）

法域	オーストラリア連邦	サウスウェールズ州
1. 調査対象の法令・ガイドラインの名称	・連邦プライバシー法 1988（Privacy Act 1988 (Cth*)）及び オーストラリア・プライバシー原則（Australian Privacy Principles (APP)）*Cth は the Commonwealth of Australia の略。	・プライバシー及び個人情報保護法 1998（Privacy and Personal Information Protection Act 1998） (NSW**)（PPIP） **NSW はニューサウスウェールズ州の略。
1.1 制定主体	連邦議会	州議会
1.2 規律対象	民間部門及び公共部門（地方自治体を含む）双方	公共部門（地方自治体を含む）
2. 利用目的		
2.1 顔識別を利用する場合の根拠を要する規定又は利用目的を制限する規定	Australia Privacy Principles, 6.1 – 6.3	PPIP 第 17 条
2.1A 許容される利用目的	－	
2.1B 禁止される利用目的	－	
3. 撮影場所・撮影態様		
3.1 撮影場所を制限する規定	該当する規定なし。なお、撮影場所が私有財産上にある場合、物権法の典型的な原則、当該財産の所有者/管理者の承認又は許可、並びに当該所有者が定めるその他の規則又は内規が適用される可能性がある。	
3.2 許容される撮影場所	－	
3.3 許容される撮影態様	該当する規定なし。なお、撮影場所が私有財産上にある場合、物権法の典型的な原則、当該財産の所有者/管理者の承認又は許可、並びに当該所有者が定めるその他の規則又は内規が適用される可能性がある。	
4. 撮影の事前同意を求める規定	Australia Privacy Principles, 3.3-3.4	PPIP 第 17 条
5. 顔特徴量の取扱いに関する規定	Australia Privacy Principles, 6.1 – 6.3	PPIP 第 17 条
6. 透明性・説明責任		
6.1 撮影の公表・掲示を求める規定	Australia Privacy Principles, 5.1 – 5.2	PPIP 第 10 条

6.2A 通知公表や掲示が義務付けられている項目	☒ 利用目的	
6.2B 通知の公表や掲示の方法に関する規律	－	
6.3 本人の同意取得時に示すべき事項	☒ 撮影主体 ☒ 撮影の目的 ☒ 問合せ先 ☒ 撮影した画像の処理の方法 ☒ その他	
6.4 保存に関する規定	Australia Privacy Principles, 11.1 – 11.2	PPIP 第 12 条
6.5 保存に関して規律される項目	☒ 登録された個人データの保存期間 ☒ その他（該当する場合）：アクセス及び訂正義務、正確性義務、保護義務	
7. 救済手段		
7.1 救済手段に関する規定	Australia Privacy Principles, part 5	PPIP 第 14 条～第 16 条
7.1A 適用される救済手段の項目	☒ 開示請求 ☒ 利用停止等請求 ☒ 苦情処理への対応 ☒ その他（該当する場合）：訂正請求	
8. DPA の免許、届出又は監査を求める規定	－	
9. 外部監査を求める規定	－	
10. その他		
10.1 PIA の実施を求める規定	－	
10.2 AI を使用した個人データの自動処理を規制する規定	－	
10.3 特記事項	－	

令和 4 年度調査事業「主要国・地域における顔識別機能付カメラの利用に関する法制度」
第二次調査サマリー（オーストラリア）

1．裁判例、執行事例の調査結果

【主要な裁判例】

① Chappell v Griffin Coal Mining Company Pty Ltd [2016] FCA 1248

- 事案の概要：西オーストラリア州では、1998 年監視装置法（WA）（Surveillance Devices Act (WA)）に基づき、以下の行為が犯罪となる。
  - 私的な会話を録音するために盗聴器を使用する、または使用させること（第 5 条(1)により）。
  - 私的活動を視覚的に記録するために光学監視装置を使用する、または使用させる（第 6 条 1 項以下）、および/または。
  - 盗聴器または光学監視装置の使用の直接的または間接的結果としてその者の知るところとなった私的な会話、または私的な会話の報告もしくは記録、または私的な活動を故意に公表または伝達すること（第 9 条(1)の規定による）、

  ただし、例外が適用される場合はこの限りではない。

  このような規制がある中で、申立人は第三者との会話中に逆上して雇用主を攻撃する発言を雇用主に隠し撮りされていたため、当該映像の使用停止を求めた事案である。
- 判旨：連邦裁判所は、「私的な会話」の意味を評価し、申立人の隠し撮りされていた会話は私的なものと見なすことができると結論付け、録画の入手とその後の使用が監視装置法（WA）の条項に反することは議論の余地があると判断した。

  (a) その結果、連邦裁判所は、録画の使用を制限する差止命令による救済を認め、雇用主は以下を禁じられた：
  - ビデオ映像の使用
  - ビデオ映像の使用、ビデオ映像に基づく、またはその他の方法で、ビデオ映像が撮影された日の申請者の行為に関する懲戒調査またはプロセスの実施またはさらなるステップを踏むこと
  - 映像に依拠して、申立人の雇用を終了させる、または申立人に対してその他の懲戒処分を行うこと、その他。今回のケースでは、なぜ違法に証拠を取得したのか、正当化する理由がない。

② Farm Transparency International Ltd & Anor v State of New South Wales [2022] HCA 23

- 事案の概要：Surveillance Devices Act (NSW)の Part 2 は、監視装置の設置、使用、保守を規制している。監視装置法（NSW）第 8 条は、視覚的に記録するため、または活動の遂行を観察するために、敷地内または敷地内に光学式監視装置を設置、使用、維持することが、敷地への不法侵入を伴う場合、

知りながら行うことを禁止する。監視装置法（NSW）の第 11 条および第 12 条は、それぞれ、監視装置法（NSW）の第 8 条に反して光学式監視装置を使用した直接または間接の結果として得られた活動の遂行に関する記録または報告の伝達または公表、および記録の所持を禁止している。
録画装置を土地所有者に無断で設置していたことが問題となったため、原告側は、監視装置法（NSW）第 11 条および第 12 条により、動物虐待行為を示すビデオ録画などの情報を公表する能力を不当に損なうものであると主張し、同条による規制の有効性を争った。

- 判旨：高裁は多数決で、監視装置法（NSW）第 11 条および第 12 条は、監視装置法（NSW）第 8 条に違反して独占的に入手された記録や報告に加担した場合、少なくとも合法的活動の遂行に関する記録や報告の人による伝達や公表、記録の人による所持にそれぞれ適用され、憲法が暗示する政治コミュニケーションの自由を不当に圧迫するものではないと判断した。

【主要な執行事例】

① Commissioner initiated investigation into Clearview AI, Inc (Privacy) [2021] AICmr 54 (14 October 2021)

- 事案の概要：Clearview AI, Inc.（Clearview AI）は、顔認識検索ツールを提供し、ソーシャルメディアプラットフォームやその他の一般に利用可能なウェブサイトから取得した 30 億以上の画像（Scraped Images）のデータベースを保持している。このツールは、ユーザーが個人の顔のデジタル画像（プローブ画像）をアップロードし、Clearview AI のデータベースに対して検索を実行することができる。このツールは、一致する可能性の高い画像と、スクレイピング画像が収集されたウェブページのソース URL へのリンクを表示し、ユーザーが追加情報を得ることで、個人の特定を可能にする。
2019 年 10 月から 2020 年 3 月にかけて、Clearview AI はオーストラリアの複数の警察機関に顔認識ツールの無料トライアルを提供し、その構成員はオーストラリアにいる個人の顔画像を使った検索を実施した。
2020 年 3 月 4 日、コミッショナーは Clearview AI に対し、プライバシー法 40 条 2 項に基づく調査を開始し、Clearview AI が APP3.2、3.3、3.5、3.6、5、6、8、10、11.1、11.2、1.2 の要件を満たしているかどうかを検討すると通知した。
- 決定概要：コミッショナーは、プライバシー法第 52 条(1A)に基づき、Clearview AI に以下の宣告を行った。
a)個人のプライバシーを侵害していると判断された行為や慣行を繰り返したり、継続したりしないこと；
b) APP 3.3、3.5 および 5 に違反して、オーストラリアの個人からスクレイピング画像、プローブ画像およびその数学的表現、ならびにオプトアウトベクターを収集することを中止すること；
c）本決定日から 90 日以内に、オーストラリアの個人から収集したすべてのスクレイピング画像、プローブ画像、およびそれらの数学的表現、ならびにオプトアウトベクターを破棄すること；および
d）本決定日から 90 日以内に、以下の事項を確認する書面をコミッショナー事務所に提出すること：
i. 上記 b)で要求された画像およびその数学的表現の収集を終了すること。
ii.上記 c)で要求された画像およびその数学的表現を破棄していること。

２．調査対象国における犯罪予防や安全確保のための顔識別機能付きカメラシステムの利用動向や主な設置主体の傾向（政府機関や自治体、民間事業者等）
該当する情報は見られなかった。

３．調査対象国内における顔識別機能付きカメラに係る政策立案の状況（法令整備を含む。）や世論の動向等
以下の 3 つのレポートが公表されている。

① Official report 1: *Human Rights and Technology Final Report 2021*, published by the Australian Human Rights Commission
② Official report 2: *Privacy Act Review Report 2022*, published by the Attorney-General's Department
③ Official report 3: *Australian Community Attitudes to Privacy Survey 2020*, published by the OAIC (prepared for the OAIC by Lonergan Research)

第 12 章　ニュージーランド

主要国・地域における顔識別機能付カメラシステムの利用に関する法制度に関する調査

第一次調査サマリー（ニュージーランド）

法域	ニュージーランド
1. 調査対象の法令・ガイドラインの名称	・プライバシー法及び情報プライバシー原則（Privacy Act and Information Privacy Principles (IPP)）
1.1 制定主体	国会
1.2 規律対象	民間部門及び公共部門（地方自治体を含む）双方
2. 利用目的	
2.1 顔識別を利用する場合の根拠を要する規定又は利用目的を制限する規定	情報収集の目的が明確に特定されており、情報が収集された目的のためにのみ使用されるか（IPP 10)、情報が収集された目的の 1 つである場合には他の機関に開示される（IPP 11)。
2.1A 許容される利用目的	－
2.1B 禁止される利用目的	－
3. 撮影場所・撮影態様	
3.1 撮影場所を制限する規定	－
3.2 許容される撮影場所	－
3.3 許容される撮影態様	－
4. 撮影の事前同意を求める規定	個人情報を収集する際に明示的な同意要件を設けていない。
5. 顔特徴量の取扱いに関する規定	顔特徴量の処理について具体的に規定する法律、規則、ガイドラインはない。ただし、顔特徴量の処理にはプライバシー法が適用される。これは、顔特徴量の処理は、個人を撮影した写真の「使用」と見なされ、IPP 10 の対象となるためである。
6. 透明性・説明責任	
6.1 撮影の公表・掲示を求める規定	一般に、プライバシー法に基づき、撮影前又は撮影後合理的に可能な限り速やかに、撮影時に個人に通知することが義務付けられている（IPP 3)。
6.2A 通知公表や掲示が義務付け	•撮影していること。

られている項目	•撮影目的。 •撮影対象者。 •情報の収集及び保管を行う機関の名称及び所在地（異なる機関である場合にはその詳細） •撮影が特定の法律に基づいて許可されているかどうか、許可されている場合は、個人が収集への同意を拒否できるかどうか。 •拒否の結果（ある場合）。 •IPP に基づくアクセス及び訂正の権利。
6.2B 通知の公表や掲示の方法に関する規律	－
6.3 本人の同意取得時に示すべき事項	☒ 撮影主体 ☒ 撮影の目的 ☒ 問合せ先 ☒ 撮影した画像の処理の方法 ☒ その他
6.4 保存に関する規定	IPP 5 によれば、情報（顔認識に関連する個人データを含む）を、紛失、不正アクセス、使用、変更、開示、及びその他のあらゆる悪用から保護しなければならない。
6.5 保存に関して規律される項目	☒ 登録された個人データの保存期間 ☒ その他（該当する場合）：アクセス及び訂正義務、正確性義務、保護義務
7. 救済手段	
7.1 救済手段に関する規定	•IPP 6 は、個人が、要求に応じて個人情報を確認し、アクセスすることを可能にし、IPP 7 に基づく訂正権の通知を受けることを可能にする。 •IPP 7 は、機関が保有する情報の訂正を個人が請求することを可能にし、その請求が受け入れられない場合には、保有する情報に訂正書の添付を請求することを可能にする。 •IPP 8 は、状況に応じて合理的な範囲で、情報が正確、最新、完全、関連性があり、誤解を招くものではないことを機関に保証することを要求している。 •IPP 9 は、合法的な使用目的のために必要な期間を超えて保持することを禁じている。 プライバシー法第 70 条～第 96 条：苦情及び調査権限。

	プライバシー法第 97 条～第 111 条：人権審査裁判所での審理。 プライバシー法第 123 条～第 135 条：コンプライアンス通知を発行し、強制する権限。
7.1A 適用される救済手段の項目	☒ 開示請求 ☒ 利用停止等請求 ☒ 苦情処理への対応
8. DPA の免許、届出又は監査を求める規定	該当する規定なし。ただし、プライバシーコミッショナーは、苦情を受けた場合、又はコミッショナー自身の申し立てにより、FRT に関する法律違反を調査することができる（プライバシー法第 79 条～第 96 条)。
9. 外部監査を求める規定	－
10. その他	
10.1 PIA の実施を求める規定	－
10.2 AI を使用した個人データの自動処理を規制する規定	－
10.3 特記事項	－

令和 4 年度調査事業「主要国・地域における顔識別機能付カメラの利用に関する法制度」
第二次調査サマリー（ニュージーランド）

1．裁判例、執行事例の調査結果

【主要な裁判例】

① Armfield v Naughton (2014) 9 HRNZ 808

- 事案の概要：この事件は、2 人の隣人に関するものである。被告は、原告に何ら通知することなく、8 台のカメラを備えた監視システムを設置し、そのうち 3 台は原告宅に面していた。カメラは敷地のフェンスラインの上に設置され、原告の敷地の前面、背面、側面部分全体に遮るもののない視界が確保されていた。
- 判旨：人権審査法廷（以下、「法廷」）は、蓋然性のバランスから、被告がプライバシー法 1993（現在はプライバシー法 2020）の原則 1、3、4、6 に違反して原告のプライバシーを妨害したと判断し、被告が保有するすべての個人情報の破棄を命じた（パラグラフ 99～106 参照）。
  審判所は、プライバシー法 1993 の趣旨を検討し（41.2 項）、監視は同法に基づく個人情報の収集の一形態とみなされるべきであるとした。審判所は、1993 年プライバシー法における「収集」の定義は、監視装置による個人情報の取得を除外することを意図したものではないと述べている。さらに、1993 年プライバシー法の目的及び背景から、監視は収集の一形態とみなされるべきであるとした（44.7 項参照）。
  審判所は、プライバシーを強化するための技術の活用についても議論し、それが価値あるアプローチであり、以下の（非網羅的な）但し書きを条件として奨励されるべきであると指摘した（パラグラフ 54 を参照）：
  - 監視システムの初期設定は、情報プライバシー原則 1～4（プライバシー法第 22 条に規定）を遵守しなければならない；
  - マスキング、ピクシレーションまたはその他の技術は、このような遵守を保証または強化するために適用されなければならない；
  - ソフトウェアは、監視システムがマスクされた領域を見ることと記録することの両方を防ぐ必要がある。マスキングやピクシレーションなどの技術は、そのようなコンプライアンスを確保または強化するために適用されるものでなければならず、ソフトウェアは、監視システムがマスキングされた領域を見ることも記録することもできないようにする必要がある。
  審判所は、監視システムが情報プライバシー原則の文言だけでなく精神も遵守できるような方法で技術やソフトウェアが導入される限り、その使用に原則的に異論はないとコメントしている。

主要な裁判例としては、以下も指摘されている。

② Taylor v Attorney-General (No 3) [2022] NZHC 3170

③ Lorigan v R [2012] NZCA 264
④ Hamed v R [2011] NZSC 101, [2012] 2 NZLR 305

【主要な執行事例】

① Case note 308105 [2020] NZPrivCmr 5: Charity shop failed to notify CCTV cameras recorded audio

- 事案の概要：チャリティショップのボランティアが、CCTV カメラが顧客や他のスタッフの知らないところで音声を録音していることを発見し、プライバシーコミッショナー事務局（OPC）に苦情を申し立てた。
  この苦情は、1993 年プライバシー保護法の原則 1、3、4 に関する問題を提起したものである。
  原則 1 では、機関は、機関の機能または活動に関連する合法的な目的のためであり、その目的のために収集が必要である場合を除き、個人情報を収集してはならない。
  原則 3 では、機関が個人情報を収集する場合、当該個人が収集の事実を認識できるよう合理的な措置を講じる必要がある。
  原則 4 では、機関は、違法または不公正な方法で、あるいは関係する個人の個人的な事柄に不合理な範囲で侵入する方法で情報を収集してはならないことになっている。
- 決定概要：OPC はチャリティーショップに連絡し、申立人の懸念を伝え、音声録音が不当に侵入的であるというコミッショナーの見解を表明した。チャリティショップの経営陣は、音声記録はビデオストリームに追加情報と文脈を提供するものであり、6 台のカメラのうち 4 台で音声機能を永久的に無効にし、特定のエリアが記録されないことを確認したと述べた。また、スタッフへのガイダンスを強化し、"このカメラは音声を記録します "と表示するよう看板を改良することを約束した。

主要な執行事例としては、以下も指摘されている。

② Case note 289943 [2018] NZPriv Cmr 5: NZ Post employee complains about audio recordings made on delivery vehicles
③ Case note 277412 [2016] NZ PrivCmr 13 - Corrections failed to comply with access request from inmate seriously assaulted in prison
④ Case Note 244873 [2013] NZ PrivCmr 5 : Man objects to CCTV camera in the men's public toilets of a pub

２．調査対象国における犯罪予防や安全確保のための顔識別機能付きカメラシステムの利用動向や主な設置主体の傾向（政府機関や自治体、民間事業者等）
該当する情報は見られなかった。

３．調査対象国内における顔識別機能付きカメラに係る政策立案の状況（法令整備を含む。）や世論の動向等
研究報告やガイダンス等、複数のレポートが公表されている。

第 13 章　カナダ

主要国・地域における顔識別機能付カメラシステムの利用に関する法制度に関する調査

第一次調査サマリー（カナダ連邦・ケベック州）

法域	カナダ連邦	ケベック州
1. 調査対象の法令・ガイドラインの名称	・連邦の個人情報保護及び電子文書法（Personal Information Protection and Electronic Documents Act, SC 2000, c 5）（以下「PIPEDA」という。） ・Privacy Act, RSC 1985, c P-21 ・Guidelines for the Use of Video Surveillance of Public Places by Police and Law Enforcement Authorities ・Privacy guidance on facial recognition for police agencies ・Overt Video Surveillance Guidelines and Law Enforcement Surveillance Guidelines; and Biometrics: Principles and Legal Duties of Organizations	・民間部門における個人情報の保護に関するケベック州の法律、R.S.Q.、 c.P-39.1（以下「ケベック州民間部門法」という。） ・ CQLR c C-1.1（以下「ケベック IT 法」という。）
1.1 制定主体	連邦議会及びカナダプライバシーコミッショナー事務局（Office of the Privacy Commissioner of Canada）（「OPC」）	州議会及びケベック情報委員会（QuébecCommission d’accèsàl’information）（「CAI」）
1.2 規律対象	民間部門： PIPEDA 公的部門： Privacy Act, RSC 1985, c P-21	ケベック州民間部門法：民間部門 ケベック IT 法：民間部門及び公的部門双方
2. 利用目的		
2.1 顔識別を利用する場合の根拠を要する規定又は利用目的を制限する規定	民間部門のプライバシー法制の下では、組織は、合理的な人が状況に応じて適切と考える目的でのみ個人情報（顔認識データを含む）を収集、使用、又は開示することができ、そのような目的は収集時に特定する必要がある(PIPEDA, section 5 (3))。	民間部門のプライバシー法制の下では、組織は、深刻で正当な理由のためにのみ、個人情報（顔認識データを含む）を収集、使用、又は開示することができ、そのような目的は収集時に特定する必要がある(Quebec Civil Code, Article 37)。
2.1A 許容される利用目	－	

的		
2.1B 禁止される利用目的	－	
3. 撮影場所・撮影態様		
3.1 撮影場所を制限する規定	OPC は、監視をより一般的に扱う OPC の「Overt Video Surveillance Guidelines」において、(i) カメラは、カメラの使用及び視聴範囲を可能な限り制限するように配置されるべきであり、(ii) ビデオ監視が行われていることを個人に知らせるべきであり、(iii)公衆トイレや温泉療養室など、プライバシーの期待の濃度が高い場所では監視が不適切である、との立場をとっている。[1]	
3.2 許容される撮影場所	－	
3.3 許容される撮影態様	OPC によるいくつかの調査においては、セキュリティ目的の監視カメラの設置が民間セクターのプライバシー法令の下で許容されるとみなされた状況が記述されている。	
4. 撮影の事前同意を求める規定	一般に、顔認識データを含む個人情報を個人から収集するには同意が要求されている(PIPEDA, schedule 1, principle 4.3)。	一般に、顔認識データを含む個人情報を個人から収集するには同意が要求されている（Quebec Civil Code, article 35)。 さらに、ケベック IT 法第 44 条では、個人の身元は、当該個人の明示の同意がない限り、バイオメトリック特性又は測定値の記録を可能にするプロセスによって確認することは禁じられている。
5. 顔特徴量の取扱いに関する規定	一般に、顔認識データを含む個人情報を個人から収集するには同意が要求されている(PIPEDA, schedule 1, principle 4.3)。	一般に、顔認識データを含む個人情報を個人から収集するには同意が要求されている（Quebec Civil Code, article 35)。
6. 透明性・説明責任		
6.1 撮影の公表・掲示を求める規定	OPC は、OPC の「Overt Video Surveillance Guidelines」（民間団体に適用）において、ビデオ監視が行われていることを個人に知らせるべきであるとの立場をとっている。[2]特に、OPC は、組織は「個人が施設に入る前に、画像を撮影される可能性のある個人に対して、施設内のカメラの使用に関する明確で理解可能な通知を掲載すべきである」との立場を取っており、署名に	

[1] *Overt Video Surveillance Guidelines*, s.v., "10 things to do when considering, planning and using video surveillance."

[2] *Overt Video Surveillance Guidelines*, s.v., "10 things to do when considering, planning and using video surveillance."

	は「個人が疑問を持っている場合や、個人に関連する画像にアクセスしたい場合の連絡先も含めるべきである」としている。[3]	
6.2A 通知公表や掲示が義務付けられている項目	上記 6.1 回答の OPC ガイダンスで推奨されている通知に加えて、PIPEDA では、同意が有効であるためには、個人情報の収集前又は収集時に個人の注意を喚起する 4 つの点が必要であるとの立場をとっている。具体的には、(i) どのような個人情報を収集しているか、(ii) 個人情報の提供先、(iii) どのような目的で個人情報を収集し、利用し、又は開示するか。(iv) 危害その他の結果となるおそれ、の 4 点である。[4]	Quebec Private Sector Act, s 8.
6.2B 通知の公表や掲示の方法に関する規律	－	
6.3 本人の同意取得時に示すべき事項	☒ 撮影主体 ☒ 撮影の目的 ☒ 問合せ先 ☒ 撮影した画像の処理の方法 ☒ その他	
6.4 保存に関する規定	顔認識データは一般的にセンシティブの程度が高いと考えられているため、より高度な保護が必要である。[5]	ケベック IT 法第 45 条では、当該情報が、個人を識別し、または身元を確認するために利用される場合、民間事業者は、生体認証情報のデータベースに登録しなければならない。
6.5 保存に関して規律される項目	☒ 登録された個人データの保存期間 ☒ その他（該当する場合）：アクセス及び訂正義務、正確性義務、保護義務	☒ 登録された個人データの保存期間 ☒ その他（該当する場合）：アクセス及び訂正義務、正確性義務、保護義務、生体認証情報のデータベースへの登録義務

[3] *Overt Video Surveillance Guidelines*, s.v., "Qs and As."

[4] PIPEDA, s 6.1; OPC, *Guidelines for obtaining meaningful consent*, May 2018, revised: August 13, 2021.

[5] OPC, *Interpretation Bulletin: Sensitive Information*, May 2022, s.v., "Health information as sensitive information", available online at https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations_10_sensible/.

7. 救済手段		
7.1 救済手段に関する規定	個人は、一定の制限を条件として、(i) 個人情報へのアクセスを要求する権利、(ii) 個人情報の継続的利用又は開示についての同意を撤回する権利、又は (iii) 組織によるプライバシー法令の遵守に異議を申し立てる権利を有する。OPC は、コンプライアンス違反の申し立てを調査し、組織に勧告を行うことができる。PIPEDA の下では、告訴及び調査プロセスの終了時に、告訴人は、告訴人に損害賠償を認める権限を有する連邦裁判所に訴えることができる。[6]	同左。 ケベック州では、2023 年 9 月から、CAI は、プライバシーに関する義務の遵守を怠った企業に対して、(自然人については 5 万ドルを上限とし、その他のすべての場合については、1000 万米ドル又は直前の会計年度の全世界の売上高の 2%相当額の、より高額の方を上限とする) 多額の行政制裁金を科すことができるようになる。
7.1A 適用される救済手段の項目	☒ 開示請求 ☒ 利用停止等請求 ☒ 苦情処理への対応 ☒ その他（該当する場合）：訂正請求	
8. DPA の免許、届出又は監査を求める規定	－	ケベック州では、ケベック IT 法第 45 条に従い、組織は生体認証情報 (顔認識データを含む) のデータベースを作成する前に、その存在を CAI に開示しなければならない。[7]
9. 外部監査を求める規定	該当規定なし。しかし、OPC からのガイダンスは、個人情報を適切に保護するためにプライバシー法の要件を遵守するために、情報セキュリティシステムの定期的な独立した監視と監査が必要であることを示唆している。[8]	
10. その他		

[6] See OPC, *Guide to the PIPEDA complaint process*, available online at https://www.priv.gc.ca/en/report-a-concern/file-a-formal-privacy-complaint/file-a-complaint-about-a-business/guide/.

[7] Quebec IT Act, section 45, as amended by Act 25.

[8] OPC, *PIPEDA Self-Assessment Tool*, July 2008, revised August 13, 2021, available online at: www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-compliance-and-training-tools/pipeda_sa_tool_200807.

10.1 PIA の実施を求める規定	公的機関及び民間機関を対象とした CAI 生体認証ガイドにおいて、CAI は、当該特性及び測定値はセンシティブな個人情報に該当することから、生体認証を利用する事業を行うことが確定した場合には、PIA を実施すべきであるとの立場をとっている。	州の公的部門について、プライバシー影響評価に関する要件を定める州がある。[9] ケベック州では、2023 年 9 月に、個人情報の収集、使用、通信、保持、又は破壊を含む情報システム又は電子サービス配信システムの取得、開発、又はオーバーホールを行うプロジェクトに対して PIA を実施することを組織に義務付ける新しい民間部門の要件が施行される。そのような PIA は、収集される個人情報の機密性に比例したものでなければならない。[10] PIA は、民間企業がケベック州外で個人情報を伝達する前にも必要となる。[11]
10.2 AI を使用した個人データの自動処理を規制する規定	新たに立法化された連邦法案 C-27 は、もし可決されれば、人工知能及びデータ法（Artificial Intelligence and Data Act, 「AIDA」）を制定することになる。	2023 年 9 月より、ケベック州民間部門法により、個人情報を使用する企業を経営する者は、専ら当該情報の自動処理に基づく意思決定を行い、その決定を個人に通知するまでにその事実を個人に通知することが義務付けられる。また、当該個人は、要請があった場合には、次の事項を通知することを含む追加情報を当該個人に提供しなければならない。 （1）決定を下すために使用される個人情報。 （2）決定に至った理由、主要なファクター及びパラメータ。 （3）決定を訂正するために使用される個人情報を関係者が取得する権利。
10.3 特記事項	－	

[9] See for example: Information and Privacy Commissioner of Ontario, *Planning for Success: Privacy Impact Assessment Guide*, May 2015, available online at https://www.ipc.on.ca/wp-content/uploads/2015/05/planning-for-success-pia-guide.pdf; *Freedom of Information and Protection of Privacy Act*, RSBC 1996, c 165 (British Columbia) s 69 (5).

[10] Quebec Private Sector Act, section 3.3-3.4, as amended by Act 25.

[11] Quebec Private Sector Act, section 17, as amended by Act 25.

令和 4 年度調査事業「主要国・地域における顔識別機能付カメラの利用に関する法制度」
第二次調査サマリー（カナダ）

1．裁判例、執行事例の調査結果

【主要な裁判例】

① R v. Wong, [1990] 3 SCR 36

- 事案の概要：古い判決ではあるが、ビデオ監視とそれが犯罪捜査や準犯罪捜査の文脈でどのように憲章の権利を侵害するかについての重要な判決である。この事件では、警察は、あるグループの違法な賭博行為を目撃するために、事前の司法許可なしに、ホテルの部屋内に密かにビデオ監視装置を設置した。
- 判旨：裁判所は、上記が憲章第 8 条違反に相当すると判断し、ビデオ監視から得られた証拠を排除したため、被告人は無罪となった。

主要な裁判例としては、以下も指摘されている。

② R v. Wong, 2017 BCSC 306 (B.C.S.C.)
③ R v. Yu, 2019 ONCA 942

【主要な執行事例】

① Clearview AI OPC Investigation

- 事案の概要：2020 年初頭、Clearview AI（以下、Clearview 社）がオンライン上の公開情報源から顔の画像を収集し、これらの画像の生体識別子を作成し、ユーザー（通常は法執行機関）が画像をアップロードして、一致したすべての画像とメタデータを示すコンパイル画像の顔を照合できるサービスを提供しているという報告がなされた。Clearview は、カナダ人個人を含む 30 億枚以上の顔画像とバイオメトリクス識別子を含むデータベースを蓄積していた。
  調査の概要：本件の調査では、カナダプライバシーコミッショナー、ケベック州情報アクセス委員会、ブリティッシュ・コロンビア州情報・プライバシーコミッショナー、アルバータ州情報・プライバシーコミッショナー（以下「オフィス」）が、民間企業によるオンラインデータベース（ソーシャルメディアアカウントを含む）からの顔認識データの無差別収集、使用、公開を評価した。

主要な執行事例としては、以下も指摘されている。

② Cadillac Fairview OPC investigation

③ Investigation Report F12-01, [2012] B.C.I.P.C.D. No. 5
④ Owners, Strata Plan BCS1964 (Icon 1 and 2) (Re), 2021 BCIPC 35
⑤ Grandin Manor Ltd. (Re), 2016 CanLII 11214 (AB OIPC)
⑥ Teck Coal Limited (Re), 2020 BCIPC 24

２．調査対象国における犯罪予防や安全確保のための顔識別機能付きカメラシステムの利用動向や主な設置主体の傾向（政府機関や自治体、民間事業者等）
該当する情報は見られなかった。

３．調査対象国内における顔識別機能付きカメラに係る政策立案の状況（法令整備を含む。）や世論の動向等
研究報告やガイダンス等、複数のレポートが公表されている。

第 14 章　アメリカ合衆国（連邦）

主要国・地域における顔識別機能付カメラシステムの利用に関する法制度に関する調査

第一次調査サマリー（アメリカ合衆国（連邦））

法域	アメリカ合衆国
1. 調査対象の法令・ガイドラインの名称	FTC 法第 5 条（15 U.S.C.§45）
1.1 制定主体	合衆国議会
1.2 規律対象	FTC 法第 5 条 は、運送業者、非営利団体、銀行、貯蓄貸付組合及び連邦信用組合を除き、商業活動に従事するすべての人に適用される。 州や市は、政府による顔認識技術の利用を規定する地方法を制定している。サンフランシスコとオークランド、カリフォルニア州バークレー、マサチューセッツ州ボストンとサマービルは、法執行を理由として、政府機関が顔認識を使用することを禁止している。
2. 利用目的	
2.1 顔識別を利用する場合の根拠を要する規定又は利用目的を制限する規定	FTC 第 5 条は「商業における、又は商業に影響を及ぼす不公正又は欺瞞的な行為又は慣行」を禁止する。
2.1A 許容される利用目的	☒　要保護者保護（行方不明者、認知症患者等） ☒　公衆衛生の維持・向上（感染症対策のための発熱者の行動履歴の把握等） ☒　商業利用 ☒　その他（該当する場合）
2.1B 禁止される利用目的	一般に、人種、肌の色、宗教、国籍、性別、婚姻状況等に基づく差別は、他の連邦法により禁止されており、肌の色、人種、宗教又は他の特徴又は性格特性を識別するために顔認識技術を使用することは、差別的であり得るため、以下の利用目的は禁止されると考えられる。 ☒　違法行為もしくは、不法行為であるもの、また又はそれらを助長するもの ☒　差別的な取扱いを目的とするもの。 ☒　性格特性、内的感情、精神状態の特定

	☒　　人の肌の色、人種の判別
3. 撮影場所・撮影態様	
3.1 撮影場所を制限する規定	－
3.2 許容される撮影場所	－
3.3 許容される撮影態様	－
4. 撮影の事前同意を求める規定	FTC は、顔認識の対象となるすべての人に通知を行い、同意する機会を与えるよう求めている。
5. 顔特徴量の取扱いに関する規定	FTC は、顔認識の対象となるすべての人に通知を行い、同意する機会を与えるよう求めている。
6. 透明性・説明責任	
6.1 撮影の公表・掲示を求める規定	ガイダンスによると、FTC 法は顔認識技術の利用者に、顔認識技術と収集データの目的と使用方法を開示するよう求めている可能性が高い。
6.2A 通知公表や掲示が義務付けられている項目	FTC の過去のアクションを踏まえると、顔認識技術のユーザーは、収集されたデータを削除する機会と方法を消費者に提供しなければならないように思われる。 ☒　利用目的 ☒　処理方法 ☒　管理者の身元 ☒　管理者への連絡先 ☒　その他（該当する場合）
6.2B 通知の公表や掲示の方法に関する規律	－
6.3 本人の同意取得時に示すべき事項	☒ 撮影主体 ☒ 撮影の目的☒ その他
6.4 保存に関する規定	☒　個人データの登録基準 ☒　登録された個人データの保存期間 ☒　登録された個人データの削除手続
6.5 保存に関して規律される項目	☒ 個人データの登録基準 ☒ 登録された個人データの保存期間

	☒ その他（該当する場合）:情報セキュリティ対策
7. 救済手段	
7.1 救済手段に関する規定	FTC 法は、商取引における詐欺的行為又は慣行に対し、是正を求める FTC の権限を規定している。1926 年以来、連邦裁判所は、FTC 第 5 条の下では民間の訴権は存在しないと判断しており、FTC だけが違反に対して訴訟を起こすことができる。
7.1A 適用される救済手段の項目	☒ 利用停止等請求 ☒ 苦情処理への対応：損害賠償（法定賠償）
8. DPA の免許、届出又は監査を求める規定	－
9. 外部監査を求める規定	－
10. その他	
10.1 PIA の実施を求める規定	FTC 第 5 条は、プライバシーを保護するための特定の権限を FTC に付与するものではないものの、ここ数年、詐欺に基づく特定のプライバシー侵害を禁止するものと解釈されてきた。したがって、企業が自社のウェブサイトやその他の文献で、特定の慣行に従うことを書面で約束し、その後その約束に違反したり、その約束を守らなかったりした場合、その企業は、FTC 法第 5 条に違反して不公正かつ欺瞞的な慣行を犯したとして FTC から起訴されるとされる。
10.2 AI を使用した個人データの自動処理を規制する規定	企業は、特に顔認識に関して、AI モデルを動かすデータをどのように取得するかに該当規定なし。近い将来、自動化された意思決定技術（顔認識技術に特有のものではない）の使用が規律される可能性がある。これらは 2022 年秋冬に最終決定される予定である。
10.3 特記事項	－

令和４年度調査事業「主要国・地域における顔識別機能付カメラの利用に関する法制度」
第二次調査サマリー（アメリカ合衆国）

１．裁判例、執行事例の調査結果
該当なし。

２．調査対象国における犯罪予防や安全確保のための顔識別機能付きカメラシステムの利用動向や主な設置主体の傾向（政府機関や自治体、民間事業者等）
該当する情報は見られなかった。

３．調査対象国内における顔識別機能付きカメラに係る政策立案の状況（法令整備を含む。）や世論の動向等
以下の３つのレポート等が公表されている。

① Aiming for truth, fairness, and equity in your company’s use of AI
② Best Practices for Common Uses of Facial Recognition Technologies
③ Summary FTC Guidance

第 15 章　アメリカ合衆国（カリフォルニア州）

主要国・地域における顔識別機能付カメラシステムの利用に関する法制度に関する調査

第一次調査サマリー（米国（カリフォルニア州））

法域	米国（カリフォルニア州）
1. 調査対象の法令･ガイドラインの名称	・カリフォルニア州消費者プライバシー法（Cal.Civ。Code Sections 1798.100 et seq.）（CCPA） ・カリフォルニア州などの一部の地域では、民間及び公的機関による顔認識技術の使用が禁止されていることに注意が必要である。[12]
1.1 制定主体	カリフォルニア州議会
1.2 規律対象	カリフォルニアの消費者の個人データを収集、共有、または販売するカリフォルニアで事業を行う営利団体で、一定の要件を充足するもの。
2. 利用目的	
2.1 顔識別を利用する場合の根拠を要する規定又は利用目的を制限する規定	CCPA は、「センシティブな個人情報」（生体認証情報を含むものと定義される。）を、消費者に開示される収集目的に適合する目的のためにのみ使用することを要求している。消費者がその後、追加的な目的のために消費者のセンシティブな個人情報を使用又は開示することに同意しない旨の通知を行った場合、企業は、消費者の機微な個人情報を他の目的のために使用又は開示することを禁止される可能性がある。
2.1A 許容される利用目的	－
2.1B 禁止される利用目的	－
3. 撮影場所・撮影態様	
3.1 撮影場所を制限する規定	－
3.2 許容される撮影場所	－
3.3 許容される撮影態様	－

[12] カリフォルニア州サンフランシスコ市は最近、警察などの公的機関による顔認識ソフトウェアの使用を禁止した。その理由は、https://sfgov.legistar.com/View.ashx?M=F&ID=7206781&GUID=38D37061-4D87-4A94-9AB3-CB113656159A だ。ロサンゼルス、カリフォルニア州警察委員会は、ロサンゼルス警察による顔認識技術の使用を制限する方針を持っているが、その使用を禁止していない。https://www.latimes.com/california/story/2021-01-12/lapd-panel-approves-new-oversight-of-facial-recognition-rejects-calls-to-end-program.。

4. 撮影の事前同意を求める規定	個人情報を収集する際に明示的な同意要件を設けていない。ただし、消費者は顔の画像や特徴量の使用を禁止する権利を有する。
5. 顔特徴量の取扱いに関する規定	顔特徴量の処理について具体的に規定する法律、規則、ガイドラインはない。ただし、顔特徴量の処理には CCPA が適用される。
6. 透明性・説明責任	
6.1 撮影の公表・掲示を求める規定	CCPA は、生体認証情報の保持に関する開示を要求し、データが共有されるエンティティの種類、データに対する消費者の権利（例:アクセス、削除)、個人情報の共有又は販売など、プライバシーポリシーの他のコンテンツを列挙する。
6.2A 通知公表や掲示が義務付けられている項目	☒ その他（該当する場合）:上記参照のこと。
6.2B 通知の公表や掲示の方法に関する規律	－
6.3 本人の同意取得時に示すべき事項	☒ 撮影主体 ☒ 撮影の目的 ☒ その他
6.4 保存に関する規定	個人情報（生体認証情報を含む）の保持は、当該情報が収集された目的又は消費者に開示されたその他の目的を達成するために合理的に必要かつ相応な範囲に限り認められる。情報セキュリティ対策は、情報を保護するために「合理的」である必要がある。
6.5 保存に関して規律される項目	☒ 個人データの登録基準 ☒ 登録された個人データの保存期間 ☒ その他（該当する場合）:情報セキュリティ対策
7. 救済手段	
7.1 救済手段に関する規定	顔認識システムに関する具体的な救済手段はみあたらない。データセキュリティ侵害を受けた場合に私人による提訴が可能となる。それ以外の場合、カリフォルニア州司法長官によって、通知及び消費者の権利に関して法律が執行される（「administrative enforcement」)。
7.1A 適用される救済手段の項目	☒ 利用停止等請求 ☒ その他（該当する場合)：損害賠償（法定賠償）

8. DPA の免許、届出又は監査を求める規定	CCPA は、顔認識に関連して、監督機関からのライセンス、監督機関への通知、又は監督機関による監査を必要としない。ただし、CCPA を実施する規則において、将来、監査その他の要件が定められる可能性はある。[13]
9. 外部監査を求める規定	該当規定なし。事業の請負業者（contractor）は、事業が請負業者によるデータプライバシー/データ保護契約の条項の遵守を監視することを可能にする評価又は監査に提出することを、契約上義務付けられなければならない。
10. その他	
10.1 PIA の実施を求める規定	該当規定なし。上記セクション VIII への回答を参照のこと。
10.2 AI を使用した個人データの自動処理を規制する規定	該当規定なし。近い将来、自動化された意思決定技術（顔認識技術に特有のものではない）の使用が規律される可能性がある。これらは 2022 年秋冬に最終決定される予定である。
10.3 特記事項	－

[13] 2023 年に施行予定の他の州のプライバシー法では、生体認証情報の処理など、特定のデータ処理の活動に関するデータ保護の影響評価/プライバシー影響評価の完了が求められている。当該評価は、調査に着手する当局又は強制措置が見直すことができる。

令和４年度調査事業「主要国・地域における顔識別機能付カメラの利用に関する法制度」
第二次調査サマリー（カリフォルニア州）

１．裁判例、執行事例の調査結果
該当なし。

２．調査対象国における犯罪予防や安全確保のための顔識別機能付きカメラシステムの利用動向や主な設置主体の傾向（政府機関や自治体、民間事業者等）
該当する情報は見られなかった。

３．調査対象国内における顔識別機能付きカメラに係る政策立案の状況（法令整備を含む。）や世論の動向等
該当する情報は見られなかった。

第 16 章　アメリカ合衆国（イリノイ州）

主要国・地域における顔識別機能付カメラシステムの利用に関する法制度に関する調査

第一次調査サマリー（イリノイ州）

法域	イリノイ州
1. 調査対象の法令・ガイドラインの名称	・Illinois Biometrics Information Privacy Act（740 ILCS 14/1 以下）（「BIPA」）
1.1 制定主体	イリノイ州議会
1.2 規律対象	民間部門
2. 利用目的	
2.1 顔識別を利用する場合の根拠を要する規定又は利用目的を制限する規定	BIPA は、生体認証識別子又は生体認証情報を販売、リース、取引すること、及びこれらから収益をあげることを禁止している。さらに、BIPA は、生体認証識別子又は生体認証情報を保有するいかなる者も、本人の同意を得ている場合を除き、法的に要求される有効な令状又は罰金付き召喚令状に従う場合、又は要求された金融取引を完了するためでない限りは、かかる識別子又は情報を開示、再開示又はその他の方法で流布することを禁止する。最後に、生体認証情報の利用は、情報利用の目的にかかわらず、該当する本人への適切な通知とその同意がある場合にのみ許容される（740 ILCS 14/15(b)、(c)及び(d)）。
2.1A 許容される利用目的	☒ 許容される利用目的を限定する規律はない。
2.1B 禁止される利用目的	☒ その他（該当する場合）：販売、リース、取引すること、及びこれらから収益をあげることを禁止。
3. 撮影場所・撮影態様	
3.1 撮影場所を制限する規定	－
3.2 許容される撮影場所	－
3.3 許容される撮影態様	－
4. 撮影の事前同意を求める規定	BIPA では、生体認証情報及び生体認証情報の収集及び使用について、事前に同意を得る必要がある（740 ILCS 14/15(b)）。
5. 顔特徴量の取扱いに関する規定	顔特徴量の処理について具体的に規定する法律、規則、ガイドラインはない。ただし、顔特徴量の処理には CCPA が適用される。
6. 透明性・説明責任	

6.1 撮影の公表・掲示を求める規定	BIPA は、撮影によって生成されたデータを含む可能性のある生体認証情報及び生体認証情報の収集について、事前の通知及び同意を必要とする。
6.2A 通知公表や掲示が義務付けられている項目	BIPA は、生体認証情報の保持、保存及び送信に関する開示を行う場合は、他の機密情報やセンシティブ情報に使用されるものと同等以上の、相当の注意をもって行うことを要求している。 ☒ 利用目的 ☒ 処理方法 ☒ 管理者の身元 ☒ 管理者への連絡先 ☒ その他（該当する場合）：収集期間、保存期間、使用期間
6.2B 通知の公表や掲示の方法に関する規律	☒ その他（該当する場合）：書面による通知が必要。
6.3 本人の同意取得時に示すべき事項	BIPA は、生体認証識別子又は生体認証情報を収集する前に、事前の同意を必要とし、同意は、生体認証情報の対象者本人又は本人から法的に授権された代理人により作成された「書面による公開」により受領されなければならない。 BIPA は特に撮影にはコミットしていないが、IV で述べたように、同意を得る前に生体認証収集についての通知が必要である。実際には、これは「通知と同意」制度と呼ばれ、上記の通知は、同意が提供された時点で、生体認証識別子又は情報が収集される前に提供される。 ☒ その他：上記参照のこと。
6.4 保存に関する規定	生体認証識別子及び生体認証情報は、情報を収集又は取得するための当初の目的達成のために必要な期間、又は本人と事業者との最後のやり取りから 3 年以内のいずれか早い方の期間に限り保持することができる。生体認証の実際の保存期間は、収集の前に開示されなければならない。生体認証情報の保存及び送信は、相当な注意をもってかかる情報を開示から保護するものでなければならず、その他の機密情報及びセンシティブ情報の保存及び送信と一貫したものでなければならない。
6.5 保存に関して規律される項目	☒ 登録された個人データの保存期間 ☒ その他（該当する場合）：VI.4 参照のこと。
7. 救済手段	
7.1 救済手段に関する規定	BIPA は、BIPA 違反によって被害を受けた人の私的な訴権をさだめている。損害賠償予定額は$1, 000~$5000 米ド

	ル又は実際の損害額のいずれか大きい方とし、弁護士費用、及び差止命令による救済又はその他の司法判断による適切な救済を提供する。
7.1A 適用される救済手段の項目	☒ 利用停止等請求 ☒ その他（該当する場合）：損害賠償
8. DPA の免許、届出又は監査を求める規定	BIPA では、顔認識に関して監督機関への通知又は監督機関による監査を必要としない。[14]
9. 外部監査を求める規定	－
10. その他	
10.1 PIA の実施を求める規定	該当規定なし。上記セクション VIII に対する回答を参照のこと。
10.2 AI を使用した個人データの自動処理を規制する規定	－
10.3 特記事項	－

[14] 2023 年に施行予定の他の州のプライバシー法では、生体認証情報の処理など、特定のデータ処理の活動に関するデータ保護の影響評価/プライバシー影響評価の完了が求められている。当該評価は、調査手続きまたは執行手続きを担当する規制当局によるレビューがなされる可能性があります。

令和４年度調査事業「主要国・地域における顔識別機能付カメラの利用に関する法制度」
第二次調査サマリー（イリノイ州）

１．裁判例、執行事例の調査結果
【主要な裁判例】
イリノイ州については、Illinois Biometric Information Privacy Act (BIPA)に関連して、多数の裁判例が存在する。これらは、Illinois-Review of BIPA court decisions (3.14.23)にリストアップしている。個別の裁判例の全文を参考資料に収納している。

【主要な執行事例】
同上

２．調査対象国における犯罪予防や安全確保のための顔識別機能付きカメラシステムの利用動向や主な設置主体の傾向（政府機関や自治体、民間事業者等）
該当する情報は見られなかった。

３．調査対象国内における顔識別機能付きカメラに係る政策立案の状況（法令整備を含む。）や世論の動向等
該当する情報は見られなかった。