【法律の基礎知識】

セキュリティとプライバシー

平成 20 年 10 月 13 日
文責　弁護士　六川浩明

2001 年 9 月 11 日以降のセキュリティ強化社会におけるプライバシー・個人情報保護

セキュリティ強化社会（社会の治安維持の必要性、「監視社会」と呼ぶ学者もいる）

↓　　↓

特定または少数の人間が集まる場所（企業ビル、家）（私的空間）におけるプライバシー	不特定多数の公衆が集まる場所（公共空間）（道路、駅、空港、デパート、野球場、競技場）におけるプライバシー

（１）セキュリティとプライバシー

2001 年（平成 13 年）9 月 11 日に米国で発生したテロ事件により、その後の社会は、社会の治安維持をより重視するセキュリティ強化社会（監視社会(surveillance society)）と呼ぶ学者もいる）に変容している。それに併せて、21 世紀に入り、人間のプライバシーは様々な局面において規制されようとしている。

（２）プライバシーと個人情報

概ね重なることが多い。

自宅の中に突然不法侵入：プライバシー侵害だが、個人情報保護法違反ではない。

民間企業に保管されている顔面のみの写真の漏洩：プライバシー違反はないが、個人情報保護法違反（顔画像も、個人の特定可能性があれば個人情報だから)。

（３）プライバシーの種類

①人間の特定・識別に関するプライバシー
②所持品のプライバシー
③情報通信の存在・内容のプライバシー

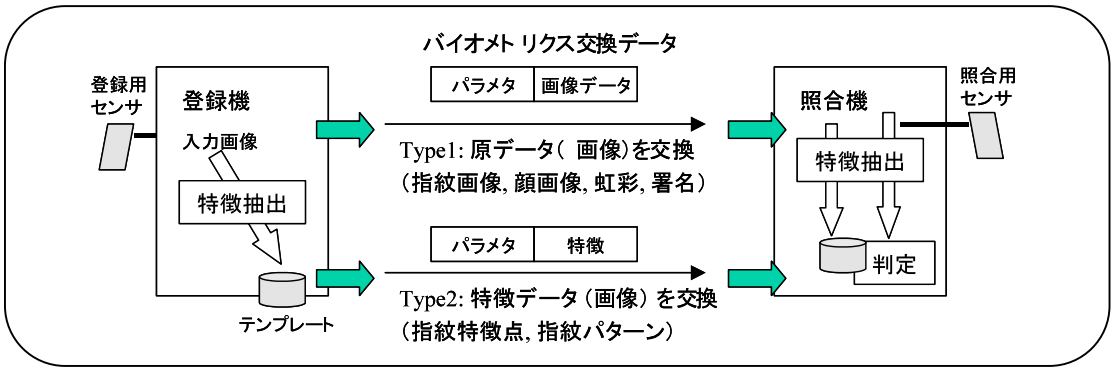
（４）人間の特定・識別に関するプライバシー

人間を他の人間と区別し特徴づける要素である「身体」（体型、人種的特長、髪型、髪色、指紋、虹彩等のあらゆる身体的特徴)、「思想」、「過去の行動歴・病歴」「身元・家族関係」等に関する情報がこれに含まれると考えられる。このプライバシーとの関連で日本において現在関心が高い分野として、(a)個人情報保護法、(b)人間の身体的特徴

による本人確認（バイオメトリックス）、(c)監視カメラと肖像権の問題がある。

(a) 個人情報保護法　省略

(b) 人間の身体的特徴・行動的特徴に基づく本人確認（バイオメトリックス）
（ｉ）



バイオメトリックスモデルにおける本人確認は、上図のように、センサからのデータ入力、特徴抽出などの前処理の後、事前に登録しておいた生体情報（テンプレートデータ）との照合処理により、類似度を算出する。

（ⅱ）現代社会にはさまざまな本人確認技術が考案されているが、大別すると：
(1)人間の記憶にもとづく技術（ATM におけるキャッシュカードによる預金払戻しの際に預金者が利用する暗証番号等）
(2)人間が所持する物品にもとづく技術（ATM におけるキャッシュカードによる預金払戻しの際に預金者が利用するキャッシュカード等）
(3)人間の身体的特徴情報にもとづく技術（高度なセキュリティが要求される場所に立ち入る際に必要とされる指紋、ATM におけるキャッシュカードによる預金払戻しの際に預金者が利用する静脈等）
があるが、バイオメトリックスのみを用いる本人確認技術においては、身体的特徴である指紋、掌形、顔、筆跡、虹彩等のパターンが認証情報として登録されるのみであるから、(1)と(2)の要素が不要となる。

（ⅲ）暗証番号が第三者に認識された場合は直ちにそれを変更する方法があり、キャッシュカードが盗難された場合は直ちにそれを無効化し新たなカードを再発行する方法があることから、万一暗証番号が第三者に認識されても、また、カードが盗難にあったとしても、利用者は引き続き、(1)と(2)の方法に基づく本人確認技術に依拠する商品やサービスを利用することが可能である。

しかしながら、指紋、虹彩、静脈等に関する情報が、第三者にコピーされてしまった場合、これらの本人確認技術に基づくサービスを利用するについては、形成外科において自己の指紋を変更する外科手術を受けたり、眼科において自己の虹彩を変更する外科手術を受けない限り、もはやその利用を事実上断念するか、あるいは、外科手術を受け

ることなく当該サービスを利用したい場合には第三者による成りすましを甘んじて受け続けなければならないこととなってしまう。

このように人間の身体的特徴情報は取り替えがきかないことから、“究極の個人情報”であると言われることがある。

また、人間の身体的特徴情報は、人間の健康状態（網膜の血管パターンなどから糖尿病などの病歴を知ることができる）や人種情報（皮膚の色から人種が把握できる。人種情報は、いわゆるセンシティブ情報に該当し、平成 16 年の総務省個人情報ガイドライン等においても原則として取得が禁止されている。）等の副次的情報を抽出するため利用されるおそれがあり、また、犯罪調査等のために二次的に利用されるおそれがあるとも言われている。これらの理由から、人間の身体的特徴情報の取扱いについては、最大限の配慮が強く要求されている。

そこで、生体情報についての個人情報データベースを構築せず、中央管理型を否定するという方法もあり得るだろうが、生体情報は常に微妙に変化することがあることから、中央管理型の方がテンプレート情報を変更しやすいという利点もあると考えられる。

（ⅳ）2002 年 5 月には米国において国境警備強化・ビザ入国改正法（Enhanced Border Security and Visa Entry Reform Act of 2002）が成立し、入出国管理の強化を目的とし、外国人にバイオメトリックスデータの提示を求めること等を内容とする US VIST（US Visitor and Immigration Status Indicator =米国出入国状況表示技術）プログラムが開始され、2004 年 9 月より米国入国の際、顔面及び指紋情報を採取することが試験的に運用されている。

（ⅴ）日本においては、米国の要請により平成 17 年（2005 年）4 月より電子パスポートの実証実験が開始される予定であり、平成 17 年 6 月旅券法改正。→これは「顔写真」のみ。プライバシー侵害度はあまり高くない。

また、2002 年 6 月より運転免許証記載事項の電子記録化等を旨とする道路交通法改正法が施行されたことに伴い、2006 年より運転免許証が IC カード化され顔写真等がＩＣチップに格納される予定である。

銀行カードの IC カード化と静脈認証：生体情報・・・金融庁の個人情報保護ガイドライン

- 厳重な管理
- 二次的情報の収集のおそれ
- 交通事故で手を失った人に対する差別・・・代替措置を提供

（ⅵ）バイオメトリックスとプライバシーに関する世界の取組み

・日本

2005 年 1 月現在、日本では、個人情報保護法及び金融庁の個人情報保護ガイドライン等に若干記述があるほかは、人間の身体的特徴に基づく個人情報・個人データの収集及び管理に関して直接規律する法令もしくはガイドラインは制定されていない。

・ＯＥＣＤ

情報セキュリティとプライバシーに関する作業部会が、2004 年 4 月、

「Biometric-Based Technologies」を公表した。
・北米
IBIA(International Biometric Industry Association 米国の業界団体)が、プライバシー原則を公表している。その内容は、①バイオメトリクスデータに関する指針（データの誤用・悪用や同意なきデータ公開防止)、②民間部門に関する指針（データ収集、保存、アクセス、利用に対する明示的ポリシー開発を推奨)、③公的部門に関する指針（データ収集、保存、アクセス、利用に対する法的基準の規定の必要性)、④官民両部門に対する指針（データベースのセキュリティ確保のための適切な運用及び技術的管理手法の適用）等である。
・欧州
欧州では、2003年8月、BIOVision Privacy Best Practices in Deployment of Biometric Systems が公表されている。①データ提供者の同意のみに基づくデータ処理、②センシティブなデータ使用時の明示的同意、③事前説明に基づく目的に特化したデータ収集および使用、④データ提供者の同意の範囲内での第三者へのデータ提供、⑤司法判断による場合に限定した法執行機関へのデータ提供、⑥取扱いデータに関するプライバシーポリシーの告知（セキュリティレベル、システムへのアクセス制限、バイオメトリクデータの他の個人情報との分離保存等)、⑦精度維持のためのバイオメトリクスデータの更新、⑧バイオメトリクスデータ取扱いに関する監査当局の通知、⑨監査局による事前検査等が定められている。
・ＩＳＯ
ＩＳＯ/ＩＥＣ　ＴＲ２４７１４も、ガイドラインを策定しようとしている。

(C)監視カメラと肖像権・個人情報

（ⅰ)肖像権（撮影拒絶権と公表拒絶権）

最高裁大法廷判決 1969 年（昭和 44 年）12 月 24 日）は、憲法 13 条の趣旨に基づき「個人の承諾なしにみだりにその容貌・姿態を撮影されない自由」が保障されていると判示した。この大法廷判決は、「撮影されない自由」について判示しているのみであり、「公表されない自由」については触れていない。
ただ、国民は少なくとも「みだりに容貌等を撮影されない自由」を有することを認めているのであるから、本書ではこれを肖像権と称することとする。「みだりに」とういことは、「正当な理由がなく」という意味であるので、正当な理由があれば承諾のない撮影も違法ではないこととなる。

（ⅱ)私人（私企業を含む）が市民を防犯監視カメラにより撮影する場合
セキュリティ強化社会においては街中の多くの場所で防犯監視カメラが設置されている。設置者として、①警察機関（例：新宿区歌舞伎町地区に設置されるもの)、②地方公共団体・商店街（例：繁華街に設置されるもの)、③民間企業（例：銀行の ATM に設置されるもの)、④個人（例：ホームセキュリティカメラ）が挙げられる。これらは、

犯罪発生の抑止及び犯罪発生時の証拠収集という目的に基づき設置される。他方、防犯監視カメラには、多くの場合常時、通行人や利用者の映像が撮影され、モニタリングされることもあり、録画されることも多い。このうち、警察機関による監視カメラの設置については前述した。

防犯監視カメラによる撮影の場合においても、被撮影者の肖像権が侵害されるおそれがあるのであるから、原則として被撮影者の承諾が必要である。

そこで、被撮影者による承諾のない防犯監視カメラによる撮影の場合、いかなる場合に違法性阻却が認められるかが問題となる。

写真の撮影及び公表に関する前掲東京高裁判決（2000 年 4 月 28 日）の採用する総合判断説を参考にして私企業や商店街等が設置する防犯監視カメラについてみると、①純然たる私的な生活領域に属するものではない空間に設置すること、②一般人の感受性を基準として、撮影を望まない形態のものではないこと、③一般人が通常とっている行動であって、その行動自体が撮影されることに心理的負担を覚えないこと等の事情を総合して、違法性阻却を考えるべきこととなり、具体的には、次のように考えられる。

第一に、原則として、当該空間を訪れた一般人が防犯監視カメラの存在を容易に認識できるような態様で当該カメラを設置し、または、「防犯カメラ作動中」もしくは社会通念上これと同等の機能を有する表示（例：セキュリティ製品またはシステムに関する商標の明示）をし、防犯監視カメラの設置がされている事実を被撮影者に認識せしめることが適当であると考えられる。なぜなら、第一に、私企業が管理支配する空間においてそのような表示があればこれを認識した被撮影者の推定的同意を得やすい。

第二に、防犯監視カメラは市民の肖像権を侵害するおそれのあるものであることから、肖像権を侵害されたくないと考える市民は当該カメラに撮影されるのを拒絶する機会を与えることが妥当である。

第三に、防犯監視カメラは犯罪発生抑止と犯罪発生時における証拠収集の目的で設置されるものであることからすると、そのような表示があってはじめて被撮影者が「見られているという意識」を抱き犯罪抑止目的を実現することが可能となるからである。

第四に、撮影後録画された画像データは、被撮影者である個人の識別可能性があれば個人情報となるところ、個人情報保護法第 17 条に定める不正な手段による個人情報の取得に抵触するという疑義を可及的に避けるためである。

第五に、個人情報取扱事業者が個人情報を取得した場合は、あらかじめその利用目的を公表している場合を除き、速やかに、その利用目的を、本人に通知し、又は公表しなければならない（個人情報保護法第 18 条第 1 項）ところ、防犯監視カメラの設置の表示があれば、被撮影者に対してあらかじめ利用目的を公表していることとなり、同法第 18 条第 1 項に抵触する疑義を払拭できるからである。

一流ホテルのフロント、高価なブティック等には、当該空間を訪れた顧客が防犯監視カメラの存在を容易に認識できるような態様で当該カメラを設置することもなく、または、「カメラ作動中」もしくは社会通念上これと同等の機能を有する表示（例：セキュ

リティ製品またはシステムに関する商標の明示）もなく、天井に埋め込まれた小さなドーム型の防犯監視カメラが設置されていることが多い。このような場合には、当該空間の美観を維持する必要性があると管理者が考え、かつ、当該空間を訪れる顧客も当該美観の維持を望んでいることが通常であろうし、カメラの存在を明確に示すことによって犯罪抑止効果を予め創り出す必要性も高くない場合が多いであろう。

また、当該空間を訪れる顧客が、天井に埋め込まれた小さなドーム型の防犯監視カメラを現実には認識していないにせよ、その存在を知った場合にもそれによる撮影を拒絶することがないと考えられる場合には、個人情報保護法 17 条への抵触はないと思われる。

また、同法 18 条への抵触の点については、ホテルや高級ブティックのＨＰで、フロントや店内における防犯監視カメラの設置の利用目的で公表しておくことによって対処が可能であると考えられる。

個人情報取扱事業者に該当する私企業等が防犯監視カメラによる撮影によって取得した市民の画像データについては、個人情報保護法の定める管理義務を負うこととなる。

(ⅲ)地方自治体による防犯監視カメラについての条例制定の例

・東京都杉並区　2004 年（平成 16 年）7 月より「防犯カメラの設置及び利用に関する条例」を施行している。対象場所は、鉄道の駅の自由通路、売場面積が 3000m2 を超えるスーパー、定員が 500 人以上の劇場など。これらの場所に設置する鉄道事業者や自主的な防犯活動をする団体等に届出義務が生じる。
・滋賀県　店舗や駐車場で設置される防犯カメラの運用に関する指針案
・神戸市　自治会などが道理上に防犯カメラを設置する際、近隣とのトラブルを避けるためのガイドラインを策定

（５）サイバー上での個人情報の窃取・・・スパイウエア

スパイウエアとは、PC の利用者が認識しないまま当該 PC にインストールされ、当該利用者の行動等の個人情報を収集し、マーケティング会社等のスパイウエアの作成元に送信されるプログラムのことである。スパイウエアは他のアプリケーションソフトとセットで販売・配布され、インストール時にはそのソフトと一括して利用条件の承諾などを求められる。また、スパイウエアは、利用者に気づかれないよう、ウインドウなどを出さずにバックグラウンドで動作するため、利用者はスパイウエアがインストールされていることに気づきにくい。

スパイウエアが行う活動の内容は、実はインストール時に表示される利用条件のなかに書かれているため、インストール時にその利用条件を承諾してしまっている以上、スパイウエアの活動は直ちに違法となるものではない。しかし利用条件を読む利用者はほとんどいないのが現実であることから、ほとんどの利用者はスパイウエアを認識することなく、スパイウエアを含めたソフトをインストールしてしまう。このため、スパイウエアは、事実上、利用者の承諾なく、当該利用者の個人情報を収集しているおそれがあることとなる。

このような事情に基づき、米国ユタ州議会は 2004 年 3 月スパーウエア管理法(Spyware Control Act）を可決した。また、米国連邦下院は 2004 年 10 月、利用者の PC に権限を

超えてアクセスし、詐欺等の目的で個人情報を取得する等の行為等を禁止する旨のインターネットスパイウエア防止法案（Internet Spaware Prevention Act of 2004)を可決し、連邦上院に同法案を送った。

なお、2004年9月にシンガポールで開催されたAPEC-TEL国際会議のeSecurity Task Working Groupでの主要討議課題は、スパイウエアに関するものであり、スパイウエア検討小委員会が組織されることが決定された。

以上