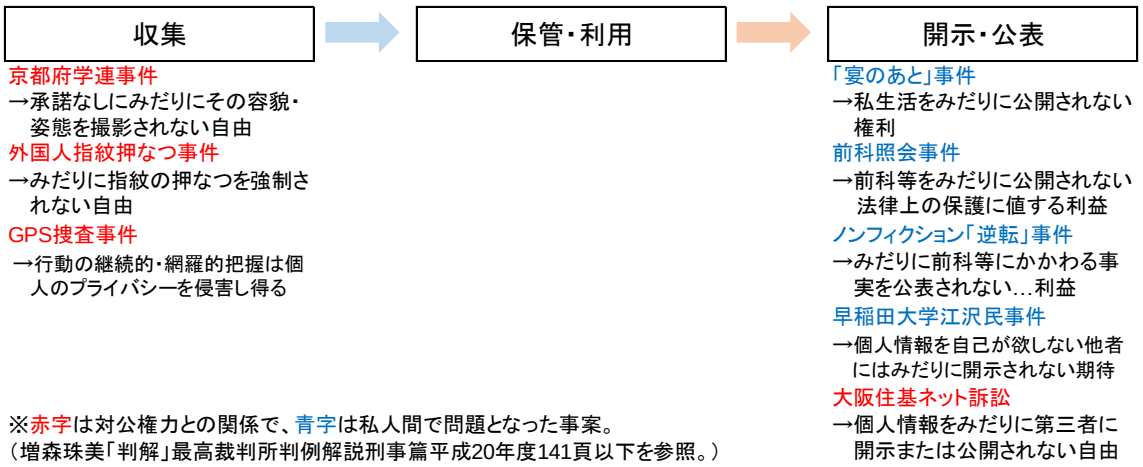
★　プライバシー権に関する基本判例の整理と保護範囲の考え方

・　判例の分類と「宴のあと」事件の判断枠組み概観

前述の通り、プライバシー権侵害の問題を考える場合には、①情報の取得段階、②情報の保管・利用段階、③情報の開示・公表段階が想定できる。プライバシー権について判断を下した著名な裁判例を整理すると、以下のように分類することができる。



「宴のあと」事件判決（東京地判昭和 39 年 9 月 28 日）は、国内におけるプライバシー侵害のリーディングケースとされている[※8]。同判決は、「個人の尊厳という思想」（憲法 13 条）を根拠として「**私生活をみだりに公開されない権利**」をプライバシーの権利と認めた。そして、プライバシー侵害として不法行為が成立する要件を次のように述べた。

> プライバシーの侵害に対し法的な救済が与えられるためには、公開された内容が（イ）**私生活上の事実または私生活上の事実らしく受け取られるおそれのあることがら**であること、（ロ）**一般人の感受性を基準にして当該私人の立場に立つた場合公開を欲しないであろうと認められることがら**であること、換言すれば**一般人の感覚を基準として公開されることによつて心理的な負担、不安を覚えるであろうと認められることがら**であること、（ハ）**一般の人々に未だ知られていないことがら**であることを必要とし、**このような公開によつて当該私人が実際に不快、不安の念を覚えたこと**を必要とする・・・

このうち、（ロ）の要件は「秘匿性」、（ハ）の要件は「非公知性」と換言できる（増森・前掲 152 頁）。（イ）の要件は、プライバシー権の問題が個人の私生活との関連で問題となることを示し[※8]、（ロ）の要件は公開による不利益の度合いを示す。（ハ）の要件は、未だ人に知られておらず要保護性が失われていないことを示していると整理できる。最後の部分は民事上の不法行為の成否という文脈で述べられていることに起因するものだろう。

ここで注目したいのは、（ロ）の要件で、情報公開がもたらす「**心理的な負担、不安**」が問題とされていることである。このことは以後の判例がいう「**私生活上の自由**」がそのような負担・不安のない私生活の全うをも包含していると解することの一助となる。

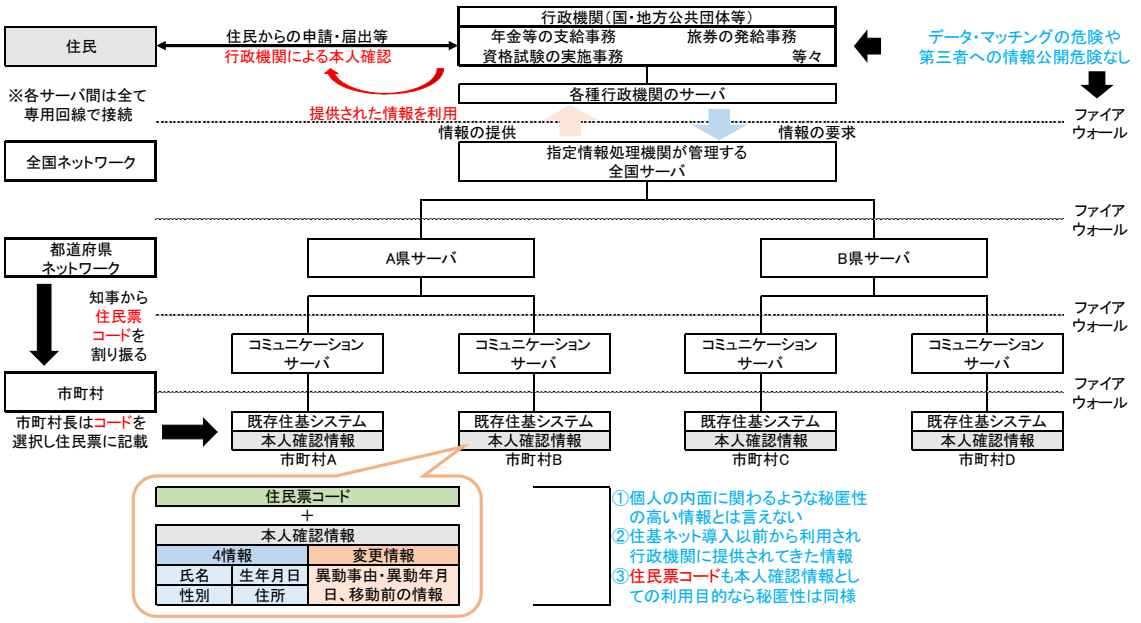
・　大阪住基ネット訴訟判決という壁

判例は、その後も**京都府学連事件判決**や**前科照会事件判決（最判昭和 56 年 4 月 14 日民集 35 巻 3 号 620 頁）**、**外国人指紋押なつ事件判決**、**早稲田大学江沢民事件判決（最判平成 15 年 9 月 12 日民集 57 巻 8 号 973 頁）**でプライバシー権ないしプライバシー利益の要保護性を承認してきた。そこで承認された利益内容は前掲の図の通りである。

このうち、**京都府学連事件判決**は個人の容貌・姿態撮影という点で、**外国人指紋押なつ事件判決**は押なつ強制による指紋採取という点で、情報取得段階（①段階）でのプライバシー利益の要保護性を認めている。また、後者の判例は、「**採取された指紋の利用方法次第では個人の私生活あるいはプライバシーが侵害される危険性がある。**」と述べて情報の保管・利用段階（②段階）でのプライバシー利益をも取り込んだ判断をしている。このことから、判例上、情報の取得、保管・利用段階でのプライバシー権も憲法上保障されるとの考えが確立したかに思われた（学説では自己情報コントロール権が認められたと説かれることもある）。

しかし、その後、この判例の潮流に待ったをかけた判決が現れた。それが**大阪住基ネット訴訟判決（最判平成 20 年 3 月 6 日民集 62 巻 3 号 665 頁）**である。

■　住基ネットシステムの仕組み概略図



※　木下昌彦・他編『精読憲法判例［人権編］』（2018年，弘文堂）13頁（山本龍彦執筆部分）に掲載されたイメージ図を基に情報を補足して作成

この事件は、住民基本台帳法の改正に伴い、従来、市町村ごとの住民基本台帳でのみ利用されていた本人確認情報が全国ネットワークシステム（住基ネット）で共有されることになったのを受け、住民が、プライバシー権その他の人格権侵害を理由として、国賠請求訴訟と、妨害排除請求としての住民票コード削除請求訴訟を提起した事案である。

原審は、住民らの同意なしに住基ネットで個人情報を管理・利用等することが、憲法 13 条が保障するプライバシー権の一内容としての自己情報コントロール権を侵害し得るとの

見解を示した。そして、行政機関に保管される個人情報が住民票コードをもってデータマッチングされたり、名寄せされて利用される具体的危険がある住基ネットは行政目的実現手段としての合理性を欠くとして、住民らの住民票コード削除請求を認容した。

これに対し、最高裁は、個人情報の秘匿性の低さ、外部不正アクセス等による情報流出の危険の不存在、情報の目的外利用（データマッチング）の危険の不存在を理由に権利侵害を否定した。また、最高裁は、情報の取得、保管・利用段階（①・②段階）のプライバシーに一切言及せず、情報の開示・公表段階（③段階）でのプライバシー権侵害のみを問題とした。

以下、各ポイントについての判決内容を引用する。

▷ **保護範囲**

憲法１３条は，**国民の私生活上の自由**が公権力の行使に対しても保護されるべきことを規定しているものであり，**個人の私生活上の自由の一つ**として，**何人も，個人に関する情報をみだりに第三者に開示又は公表されない自由**を有するものと解される…。

▷ **情報の秘匿性**

住基ネットによって管理，利用等される本人確認情報は，**氏名，生年月日，性別及び住所から成る４情報**に，**住民票コード**及び**変更情報**を加えたものにすぎない。このうち**４情報は，人が社会生活を営む上で一定の範囲の他者には当然開示されることが予定されている個人識別情報**であり，**変更情報も，転入，転出等の異動事由，異動年月日及び異動前の本人確認情報にとどまるもの**で，これらはいずれも，**個人の内面に関わるような秘匿性の高い情報とはいえない**。これらの情報は，**住基ネットが導入される以前から…利用されてきたもの**である。そして，**住民票コード**は，住基ネットによる本人確認情報の管理，利用等を目的として，都道府県知事が無作為に指定した数列の中から市町村長が一を選んで各人に割り当てたものであるから，**上記目的に利用される限りにおいては，その秘匿性の程度は本人確認情報と異なるものではない**。

▷ **情報の外部流出の危険**

住基ネットのシステム上の欠陥等により外部から不当にアクセスされるなどして本人確認情報が容易に漏えいする具体的な危険はないこと，**受領者による本人確認情報の目的外利用又は本人確認情報に関する秘密の漏えい等は，懲戒処分又は刑罰をもって禁止されている**こと…などに照らせば，**住基ネットにシステム技術上又は法制度上の不備があり，…本人確認情報が法令等の根拠に基づかずに又は正当な行政目的の範囲を逸脱して第三者に開示又は公表される具体的な危険が生じているということもできない**。

▷ **データマッチングの危険**

データマッチングは本人確認情報の目的外利用に当たり，それ自体が懲戒処分の対象となるほか，**データマッチングを行う目的で個人の秘密に属する事項が記録された文書等**

を収集する行為は刑罰の対象となり，さらに，秘密に属する個人情報を保有する行政機関の職員等が，正当な理由なくこれを他の行政機関等に提供してデータマッチングを可能にするような行為も刑罰をもって禁止されていること，現行法上，本人確認情報の提供が認められている行政事務において取り扱われる個人情報を一元的に管理することができる機関又は主体は存在しないことなどにも照らせば，住基ネットの運用によって原審がいうような具体的な危険が生じているということはできない。

- **情報秘匿利益の程度とマッチングの危険性から読み解く**

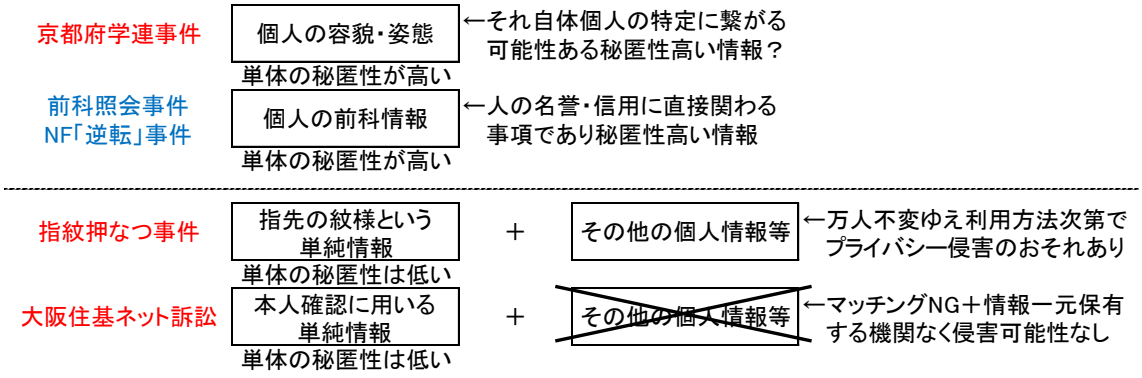
前記の通り、**大阪住基ネット訴訟判決**は、情報の取得、保管・利用段階（①・②段階）のプライバシー利益を全く問題としていない。情報の開示・公表段階（③段階）の権利性を認めた点は評価されているが、一方で原審が両段階のプライバシー利益を正面から認め、自己情報コントロール権として憲法 13 条により保障される旨判示していたこととの対比から、当該最高裁判決が自己情報コントロール権を排斥したのではないかと評する文献もある※9。

ただ、この点については、従来の判例の具体事案と比較することで、別の読み方をすることも可能であると思われる。まず着目すべきは、問題となる**情報の秘匿利益の程度**と**情報のマッチングの危険性**の有無である。

従前判例がストレートに認めたと考えられている情報取得、保管・利用段階（①・②段階）でのプライバシー権の内容は、**個人の容貌・姿態**や**前科情報**など、それ自体が個人特定や名誉・信用等に影響する秘匿性の高い情報に関連しているものが多い。

他方で、単体での情報秘匿性が低い指紋などについても、データマッチングの危険があることを理由として、当該段階での要保護性を認めているものがある※10。

後者の類型と比較してみると、**大阪住基ネット訴訟**の事案では、情報自体の秘匿性の低さ（「**個人の内面に関わるような秘匿性の高い情報とはいえない**」こと）に加えて、データマッチングの具体的危険が存在しなかったことが、過去の判例との間で明暗を分けたとも考えられる。つまり、扱われる情報の秘匿性が低いため、単体では人格的利益たり得ず、データマッチングの危険がないために権利重要性が修正されなかった可能性がある。このことが情報の取得、管理・利用段階（①・②段階）の権利性に言及しなかった原因ではないか。

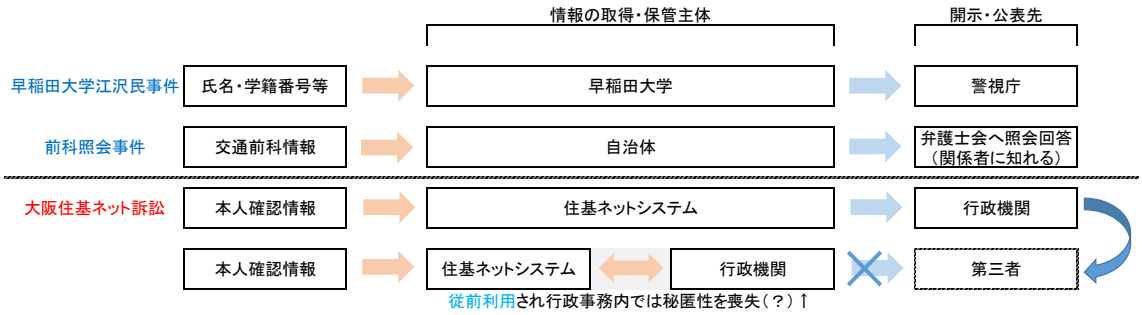


・　**情報流出の危険度と情報流出先（又は情報保有者）の属性から読み解く**

また、**大阪住基ネット訴訟判決**が情報の開示・公表段階（③段階）でのプライバシー権侵害さえも否定したのには、情報流出の危険がないことだけではなく、**情報の非広知性**（**「宴のあと」事件判決**の（ハ）の要件）が失われていたことも影響したと考えられる。情報が第三者に開示された事案としては**早稲田大学江沢民事件**と**前科照会事件**が挙げられる。2 つの判例を前提にすると、情報が管理主体以外の第三者に開示されれば、それが公的機関であっても、情報の開示・公表段階（③段階）でのプライバシー侵害が起こり得たはずである。

大阪住基ネット訴訟の事案では、情報が行政機関以外の第三者に開示される危険は排除されていた。しかし、従前各市町村しか保有できなかった本人確認情報を全国サーバに共有し、他の自治体や行政機関が容易に利用できる状態に置いており、その意味では第三者への情報の開示が行われていたのである。ただし、そこで共有される情報は、従前、本人確認という行政目的の基に個別開示され、利用されてきた情報である（前記判旨参照）。

したがって、その目的で利用する限りは、**情報の非公知性**が解除される結果、情報の秘匿性が完全に失われ、それ故にプライバシー権侵害が否定されたのだと考えられる。



・　**継続的な位置情報の秘匿利益の考え方―GPS 捜査違法判決を活用する**

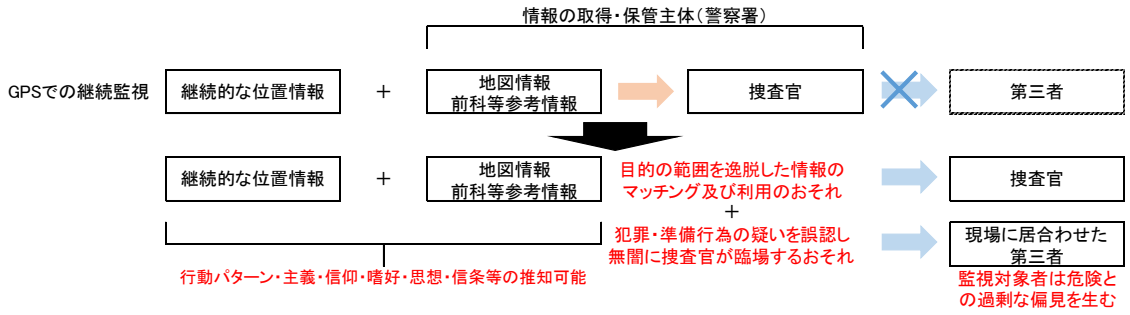
以上より、**大阪住基ネット訴訟判決**は、情報の取得、保管・利用段階（①・②段階）でのプライバシーの要保護性を完全に否定したわけではなく、事案の特殊性が結論に影響したものだと整理できる。すると、継続的な位置情報の取得が問題となる本問の継続監視についても、情報の取得、保管・利用段階（①・②段階）でのプライバシー権を保護範囲に含むと構成できる可能性がある。

位置情報は、従来の判例との関係では単純情報に位置付けられるものと思われるが、前記注 3 で触れた **GPS 捜査違法判決**は、次のように述べて継続的な位置情報の取得がプライバシー侵害に繋がる可能性を示唆する。

> ＧＰＳ捜査は，対象車両の**時々刻々の位置情報を検索し，把握す**べく行われるものであるが，その性質上，**公道上のもののみならず，個人のプライバシーが強く保護されるべき場所や空間に関わるものも含めて，対象車両及びその使用者の所在と移動状況を逐一把握することを**可能にする。このような捜査手法は，**個人の行動を継続的，網羅的に把握することを必然的に伴うから，個人のプライバシーを侵害し得る**ものであり…

この判決自体は、上記のような性質をもつ GPS の無断設置が捜査官による私的領域への侵入にあたり、憲法 35 条に抵触することを問題としていたが、その侵入行為とプライバシー侵害とを概念上区別している。したがって、位置情報の継続的・網羅的把握自体がプライバシー侵害に当たり得ると言っているようにも解釈できる。

そこで、位置情報の継続的・網羅的な把握が具体的にどのようなプライバシー侵害を招くのかを、本問の事案に即して検討すると、以下の図のように整理できる。



ポイントはデータマッチングの危険の有無とマッチングにより推知される個人情報の性質、及び第三者への情報開示・公表の危険である。また、そこで見た「危険」を保護範囲に含むかどうかは、**「宴のあと」事件判決**の（ロ）の要件もヒントになる。

GPS から取得された監視対象者の位置情報は、警察署のモニターで地図情報、前科等の参考情報とマッチングされる。マッチングされた情報は再犯防止のため、初動捜査の要否判断に用いられる。ただ、そこでマッチングされる情報は危険地域以外の位置情報にも広く及び、上記目的を超えたデータマッチングが行われてしまう可能性を否定できない。そうしてマッチングされた結果推知される情報は、単なる行動パターンにとどまらず、地図情報も相まって、個人の主義や信仰、嗜好、思想・信条等にまで及び得る。これらの情報は「個人の内面に関わるような秘匿性の高い情報」を含み、みだりに第三者に公開されたくないと欲するのが通常と言える。そのような情報が捜査官に推知されてしまうという不安感は相当大きく、その「**心理的負担**」は自由な私生活を阻害するのに十分と言える。

加えて、取得される位置情報は画像や映像など、監視対象者の姿態の把握を伴わないため、なんでもない行動が犯罪ないしその準備行為と誤認される危険を潜在的に抱える。そして、その誤認が現実化すると、初動捜査に臨場した捜査官の対応によっては、その場に居合わせた第三者に対し、監視対象者が前科者ないし危険人物であるとの偏見を植え付けてしまう可能性がある。つまり、位置情報をてこにして、監視対象者の前科情報等が第三者に間接的に公開されるおそれもあるというわけである。

以上のことを踏まえれば、本問でも、情報の取得、保管・利用段階（①・②段階）でのプライバシー権が保障されることを導出可能であると思われる。ここまでの論証は一つの考え方に過ぎないが、構成に悩んだときは、是非参考にされたい。