令和２年（ネ）第１０９号　マイナンバー離脱等請求控訴事件

控訴人　　坊真彦　外

被控訴人　国

控訴審第３準備書面

２０２１年8月２５日

名古屋高等裁判所金沢支部　御中

控訴人ら訴訟代理人

弁護士　　岩　淵　正　明

第１　はじめに

被控訴人である国は，EU に対し，国内の個人情報保護法制が憲法１３条の保障するプライバシー権を具体化したものであって，欧州における個人情報保護のルールである EU 一般データ保護規則（以下「GDPR」という。）と同等の保障を確保しているとの宣明を行っている。

したがって，国民の膨大かつ重要な個人情報を取り扱っているマイナンバー制度の合憲性を判断するに当たっては，少なくとも，GDPR が具体的に保障する自己情報コントロール権の内容が十分に保障されているか否かが問われなければならない。そして，もし GDPR が具体的に保障する自己情報コントロール権の内容が保障されていない場合には，マイナンバー制度は，被控訴人である国が EU に対して自ら宣明した内容（GDPR と同等の保障を確保している）に反するとともに，憲法１３条が保障するプライバシー権，具体的には自己情報コントロール権ないし情報管理システムに接続されない自由を制約・侵害する違憲な制度と言わざるを得ない。

しかし，以下に述べるとおり，マイナンバー制度を含む日本の個人情報保護法制では，GDPR が個人のプライバシー保護にとって最も重要とする本人同意の原則が十分に確保されておらず，またマイナンバー制度においては自己情報に関する削除権も保障されていないことから，マイナンバー制度は GDPR が

具体的に保障する自己情報コントロール権の内容を保障できていない。したがって，マイナンバー制度は，自己情報コントロール権ないし情報管理システムに接続されない自由を制約・侵害する違憲な制度である。

以下，詳述する。

第２　GDPR の内容

１　国際的にも，個人情報の取扱いについて情報主体の自己決定・同意（＝自己情報のコントロール）を保障すべきであるということは当然の前提とされており，EU においては個々人が自分の個人情報をコントロールする権利を保障することを目的に GDPR が定められた。その具体的な内容については，個人情報保護委員会作成の仮訳が公開されている（https://www.ppc.go.jp/files/pdf/gdpr-provisions-ja.pdf)。

２　GDPR においては，保護すべき個人情報の例として「氏名，識別番号，所在地データ，メールアドレス，オンライン識別子（IP アドレス等），クレジットカード情報，パスポート情報，身体的・生理学的・遺伝子学的・精神的・経済的・文化的・社会的固有性に関する要因」などが定められている（同４条)。

３　個人情報の取扱い（処理）の方法については，「個人データまたは個人データの集合に対して行われるあらゆる作業又は一連の作業をいう。この作業は，取得，記録，編集，構造化，保存，修正または変更，復旧，参照，利用，移転による開示，周知またはその他周知を可能なものにすること，整列または結合，制限，消去または破壊することをいう」（同４条）としており，「開示または公表」に止まらない，情報のあらゆる場面における規制が想定されている。

４　そして，GDPR はセキュリティ対策などの徹底を求めるとともに，同６条において，個人情報の取扱いに対して原則として当人の同意（しかも明確で，他の事項との区別もされ，かつ簡便に取消しが出来る手続）を求め，これに反すれば罰則（制裁金）を課す，という極めて厳格な同意原則を定めている（甲５２・５２～５６頁)。

5　また，GDPRは，本人（データ主体）に対し，個人データの収集・処理目的との関係で必要性がなくなった時や，個人データ処理に対する同意を撤回した場合など，所定の要件に該当する際には，個人データを管理者に削除させる権利を認めている（同１７条，甲５２・８２～８３頁）。

これにより，本人（データ主体）は，自分のデータのうち，どの情報をデータ処理の対象にするのかについて自ら主体的に選択できることになる。そして，ほぼすべての情報を提供することを拒否したり，または各データの結合を拒否することにより，情報管理システムからの事実上の離脱や，意に反するデータマッチングを回避することが可能となっており，まさに自己情報コントロール権が具体的に保障されているのである。

6　さらに，GDPRはデータ主体に対し，プロファイリングに対する異議を唱える権利を認めている。この権利が行使された場合，データ管理者は，データ主体の利益等を上回るようなやむにやまれぬ正当な理由を示さない限り，プロファイリングを中止しなければならない（２１条１項）。さらにデータ管理者はデータ主体に対し，こうした権利をもつことを明確な形で告知しなければならない（２１条４項）。こうした規定から，GDPRでは，プロファイリングについて，事実上のオプトアウト方式を採用しているといえる。

GDPRはさらに進んで，データ主体に対し，プロファイリングのような自動処理のみに基づき重要な決定を下されない権利を認めている（２２条１項）。例外的にこれが認められる場面（２２条２項）においても，原則として人種・民族・宗教等の個人データの特別なカテゴリーに基づくものであってはならないと規定している（２２条４項）。

7　このようにGDPRは，現代のプロファイリングについて，厳しい警戒心をもって臨んでおり，データ管理者が，データ主体（個人）の意に反してプロファイリングすることを事前，事後にわたって厳格に規制している。

データ主体の同意原則を厳格に規定したうえで，削除権や，プロファイリン

グに対する異議を唱える権利や，プロファイリングのような自動処理のみに基づき重要な決定を下されない権利を認めているのは，まさに自己情報コントロール権を具体的に保障し，これらが現代のプライバシー保護のために必要不可欠であるからである。つまり，自己情報コントロール権を保障することなしに，現代のプライバシーを保障することが不可能であることを端的に示しているのである。

第３　日本政府の対応

１　EU 域外持ち出しのための「十分性認定」

GDPR における個人情報保護ないしデータ保護の観点は，既に述べたとおり，氏名等の本人識別情報を含む個人情報全般について，情報の流通，利用等のあらゆる場面において保護を及ぼすことを目的としており，その大前提として同意原則の徹底及び削除権等の事後的救済制度が認められているところである。

そして，GDPR ではＥＵ域内で取得した個人情報をＥＵ域外に持ち出すことを原則として認めておらず，欧州委員会が定める「十分性認定」（欧州委員会が，特定の国や地域が個人データについて十分な保護水準を確保していると決定すること）の要件をクリアしている国や地域に限って，個人情報の持ち出しが認められている。

２　日本政府による宣明

日本政府は，平成３０（２０１８）年９月１４日，欧州委員会宛に「法執行及び国家安全保障目的の日本の公的機関による個人情報の収集及び使用」を提出した（以下，「本書簡」という。甲５３）。その結果，２０１９年１月に日本に対しても十分性認定が認められ，これによってＥＵ域外への個人情報の移転が可能となっている。

そして，本件書簡における日本政府の宣明の内容は次のとおりである。

⑴　本書簡において，日本政府は，「以下の文書は，法執行及び国家安全保障目的のための日本の公的機関による個人情報（電子）の収集及び使用に関する

法的枠組み（以下「政府アクセス」という。）の概要を示したものであり，特に利用可能な法的根拠，適用条件（制限），独立した監督及び個人の救済の可能性を含む保護措置に関するものである。この書簡は欧州委員会に向けたものであり，EU から日本に移転された個人情報に対する政府アクセスが必要かつ相応な範囲に限定され，独立した監督の対象となり，当該個人はプライバシー及びデータ保護の基本的人権の侵害のいかなる可能性についても救済を受けられるというコミットメントを表明し，保証するものである。」としている（甲５３・１頁）。

(2) そのうえで，「A. 憲法の枠組み及び，法原則の留保」の章においては，「日本国憲法第 13 条及び判例にて，憲法上の権利としてのプライバシー権を認めている。この観点から，最高裁判所は，みだりに個人が他人に個人情報を知られたくないことは自然であり，この期待は保護されるべきであると判断した。」と宣明している（甲５３・１頁）。

(3) また，「B.個人情報保護に係る具体的規定」の章においては，「憲法に基づき，かつ憲法の規定を具体化する，個人情報保護法及び行政機関の保有する個人情報の保護に関する法律（行個法）は，民間部門及び公的部門における個人情報についての権利を保障している。個人情報保護法第７条は，個人情報保護委員会が『個人情報の保護に関する基本方針』（基本方針）を策定することとしている。日本国政府の中心機関（内閣総理大臣及びその他閣僚）たる内閣の決定を得るこの基本方針は，日本の個人情報保護の方向性を指し示すものである。このようにして，独立機関である同委員会が日本の個人情報保護法制の司令塔となっている。行政機関が個人情報を収集するときは，それが強制的な手段によるものか否かにかかわらず，原則として行個法の規定に従わなければならない。行個法は，（行個法第２条第１項で定義される）『行政機関』による『保有個人情報』の取扱いについて適用される一般法である。したがって，法執行分野及び安全保障分野における個人情報の取扱い

も含むものである。政府アクセスを実施する権限を有する行政機関のうち，都道府県警察以外の全ての機関は国の行政機関であり，全ての国の行政機関は『行政機関』の定義に該当する。」と宣明する（甲５３・２～３頁)。

⑷　すなわち，国は本書簡により，①「日本国憲法第１３条及び判例にて，憲法上の権利としてのプライバシー権を認めている」こと，及び，②行政機関個人情報保護法は「憲法に基づき，かつ憲法の規定を具体化する」ものであること，さらには③日本の個人情報保護法制がGDPRと同等の権利保障を実現していること（十分性認定に値すること）を宣明しているのである。

被控訴人国がこのように宣明している以上，これを前提とした判断がなされなければならない。

第４　日本の個人情報保護法制の欠点

１　同意原則の不十分（事前予防の不十分)

本書簡も踏まえたうえで，２０１９年１月，個人情報保護委員会によるEU指定及び欧州委員会による十分性認定がなされ相互承認がなされるに至ったが，日本の個人情報保護制度とGDPRについては，未だ齟齬があることが専門家からも指摘されている（甲５２・１６４～１６８頁)。

すなわち，日本における個人情報保護制度は，GDPRの基本原則である正当化事由（同意原則）が欠けており，GDPR相当の水準の個人情報保護とするためには本人の意思が反映される仕組みが求められると指摘されている。

そして，個人番号制度が本人同意を前提とせず，情報の収集・利用を行うものであることからすれば，公権力等によるプライバシー侵害に対する事前予防が十分に機能しないことになり，同制度が国際的な潮流であるGDPRと大きく矛盾するものであることが明らかである。

２　削除権の不存在（事後救済制度の不存在)

また，マイナンバー制度を含む日本の個人情報保護制度においては，GDPRでは明確に規定されている削除権（同１７条，個人データの収集・処理目的との

関係で必要性がなくなった時や個人データ処理に対する同意を撤回した場合などに個人データを管理者に削除させる権利）が認められていない。

したがって，マイナンバー制度を含む日本の個人情報保護法制では，本人（データ主体）は，自分のデータのうち，どの情報をデータ処理の対象にするのかについて自ら主体的に選択することができず，この点で，GDPR が具体的に保障する自己情報コントロール権が保障されていないことが明らかである。

3　小括

以上のとおり，マイナンバー制度を含む日本の個人情報保護制度は，GDPR が規定する自己情報コントロール権を実質的に保障するための重大な制度であるところの，事前予防としての厳格な同意原則と，事後救済制度としての削除権の，いずれをも欠いている。

このような状況は，日本の個人情報保護法制が GDPR と同等の権利保障を実現していること（十分性認定に値すること）を宣明する本書簡と矛盾しているのはもちろんのこと，市民のプライバシー権，具体的には自己情報コントロール権が保障されていないことが明らかである。

第5　まとめ

GDPR が，情報の様々な取扱いについて厳格な本人同意を求め，削除権やさらにはプロファイリングに対する厳格な規制を及ぼしているのは，自己情報コントロール権をプライバシー権の中核として捉えているからであり，逆にいえば，そのように理解しなければ，コンピュータネットワークが張り巡らされ，ビッグデータの活用が過度に進んでいる現代において，到底プライバシーの保護が図られないからである。

原判決のように，個人情報をみだりに「開示・公表されない」というごく限定された範囲でしかプライバシー権を捉えられないとすると，プロファイリング等によって，どのように私生活をのぞき見されようと，それはプライバシー権の範疇でなく，憲法はこうしたことにまったく無力でしかないということに

なる。これでは，国際水準にも，それに対する日本政府の対応とも矛盾するものであり，個人の尊重＝自律的生の実現という，憲法１３条の究極的目的の実現のためにも，プライバシー権を自己情報コントロール権，さらには自己の意思に反してシステムに接続されない自由を保障することが必要不可欠なのである。

そして，マイナンバー制度を含む日本の個人情報保護法制が，GDPR が個人のプライバシー保護にとって最も重要とする本人同意の原則を十分に確保しておらず，また自己情報に関する削除権も保障していないことから，マイナンバー制度は GDPR が具体的に保障する自己情報コントロール権の内容を保障できていないのであって，マイナンバー制度が自己情報コントロール権ないし情報管理システムに接続されない自由を制約・侵害する違憲な制度であることが明らかである。

以上