陳　述　書

2016 年　４月１２日
原告　　関口　　博

私は、「地方から平和を」「市民参加によるまちづくり」を標榜し、1999 年（平成 11 年）より国立市議会議員を２期８年、2007 年（平成 19 年）より国立市長を１期４年務め、現在議員として再び国立市議会に在籍しています。

教育、環境、福祉の分野において市民との対話を重視し、命とその尊厳を守ることを中心に据え、市議会議員時代は政策提言を、市長時代は政策決定と予算編成を行ってきました。

私は、議員活動を始める前は、コンピュータのシステムエンジニアとして働いていました。製鉄所や上下水道システム、電力会社のコンピュータシステムプログラムの設計、製作、試験、現地調整まですべての工程をまとめていました。私は、システムエンジニアとしての知識と経験から、コンピュータの利便性とその脆弱性を熟知しています。

コンピュータシステムは、人間が作るプログラムからなり、完全なプログラムというものは存在しないこと、さらに、コンピュータが扱うデータは、人間の手によって漏えいすることは避けられないこと。これらのことは、システムエンジニアであればだれでも知っていることであり、システムを作る上での大前提です。

2013 年 5 月 24 日に所謂マイナンバー法（共通番号制）が成立し、住基ネットがそのインフラとして利用されることになりました。マイナンバー制度では、年金、医療、福祉、財産、保険等、個人のもっとも秘匿されるべき個人情報がマイナンバーという１つの番号で管理されます。

税の公平性と社会福祉の充実という名目で始まったマイナンバー制度ですが、その用途は、当初の目的とはまったくかけ離れたものになり、多くの分野でマイナンバーがキーとなって個人情報が検索され、収集された個人情報は、民間にも開放される予定です。

国は、マイナンバーを使うことによって、行政事務が効率的になると宣伝していますが、市長時代の経験からお話しますと、各自治体は、福祉、税金など各分野ですでに、独自の番号を使用して効率化を図っており、マイナンバーで管理することによって効率化がさらに図られることはありません。むしろ新たな情報セキュリティ対策をすることや国からのシステム不具合対策やデータ更新の指示などで、職員は、センシティブな情報の扱いに神経を使い、その対応に追われます。

行政が行う住民サービスは、住民が幸せな生活を送る為のものであり、それを享受するために、住民は、本来他者に知らせる必要のない自己情報を行政に預けるのです。行政や民間企業の事業運営の効率化のために、個人情報を与えるのではありません。しかも、自分の知らないところで、自己情報が改ざんさ

れていても、また、誤って記録されても、他者に利用される危険性があります。自己情報がどのようになっているか知る方法がなく、事実と異なっていてもデータを変更することもできない、つまり自己情報コントロール権がまったくないシステムに、個人情報を与えなければならないということです。

自治体が、住民の要求を満たし、不満を解消する窓口として機能できたのは、自治体が住民に信頼され、個人情報を預けられたからです。マイナンバー制度は、自治体が把握しきれない個人情報をマイナンバーのもとで一元管理されるため、自治体は、住民の生活を守ることができないばかりか、住民も安心した生活を送ることができなくなります。

2008 年（平成 20 年）3 月 6 日にマイナンバー制度のインフラとなっている住基ネットに対する最高裁の判決がでました。

住基ネットシステムで可能なデータマッチングの危険性について、最高裁は、次のように判断しています。「データマッチングは本人確認情報の目的外利用にあたり、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る」とし、「データマッチングには、罰則があるから危険はない」と結論づけています。しかし、マイナンバー制度は、まさにそのデータマッチングをする制度です。

また、最高裁は、次のようにも判断しています。

「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機関又は主体は存在しない」だから危険はないとしました。しかし、マイナンバー制度では、地方公共団体情報システム機構（Ｊ－ＬＩＳ）という個人情報を一元管理する機関があり、同機構が管理する中間サーバーには、個人情報が一元管理されています。

これらの点で、マイナンバーシステムは、住基ネットシステムは安全であるとした最高裁の判断根拠と合致しないシステムであることが明白です。

国は、個人情報は、分散管理しているので、安全ですとしています。

つまり個人情報は、日本年金機構や銀行など各機関がそれぞれ管理しているから名寄せされることがなく安全ということのようです。しかし、各機関が保有している個人情報のデータには、マイナンバーが付番されているため、各機関毎に情報漏洩されたらマイナンバーによって名寄せが可能であり、マイナンバーによって名寄せされた巨大な個人情報データが闇のデータベースとして構築される危険性が極めて高くなります。日本年金機構から 125 万件の個人情報が漏えいした事件で、もしマイナンバー制度開始後に起きていれば、マイナンバーが付番された年金情報が流出したことになり、他の機関で情報が漏えいしたデータと名寄せをすることが可能となり、大変危険なデータベースとなるのです。つまり、マイナンバーが付与されているデータは、マイナンバーで紐付けされて一元管理されているのと同じで、分散管理されているから安全とはならないのです。

2016 年 4 月 7 日(木)、時事通信によれば、トルコで国民の約３分の２に当たる約５０００万人の個人情報がインターネット上に流出する事件が起き、同国の検察当局は６日、捜査を開始しました。個人の住所、生年月日、国民ＩＤなどを含む大量のデータが流出し、その中には、エルドアン大統領やダウトオール首相のデータも含まれているとされています。
このような、個人情報流出は、大きな犯罪に結びつく恐れがあり、平和な市民生活を脅かすものです。

また、2013 年 6 月エドワード・ジョセフ・スノーデン氏は、国家安全保障局 の局員として、アメリカ政府による情報収集活動に関わった手口を告発しました。マイナンバー制度は、国家による個人情報の管理、監視を可能にするシステムであり、アメリカと同様に、国家による情報収集活動の道具として機能することが可能です。個人情報が、本人の知らないところで管理、監視される息苦しい社会を創出してはならないと考えます。

コンピュータの利便性を享受するためには、個人の尊厳、自由を守りつつシステムを構築しなければならないと考えます。
それには、すでに自治体では、固有の番号で効率化を図っているように、各分野でつまり、医療の分野、保険の分野等それぞれの分野で固有の番号を使用して効率化を図り、たとえ情報漏洩が起きても、被害を最小限度にとどめることができるシステムにするように努めるべきです。

以上、システムエンジニアとしての経験から、コンピュータの脆弱性を指摘し、市長としての経験からマイナンバー制度は、自治体にとってまったく効率を上げることはなく、むしろリスクが高まり、経費がかかるシステムであること、また、住民の安全、安心な生活を守ることができないシステムであることを申し上げました。マイナンバー制度は、人々の社会生活を脅かし、国家による管理、監視システムになり得るシステムであり、公共の福祉に寄与しない制度です。

よって、マイナンバー制度は、個人の幸福を追求する権利を保障した憲法 13 条に違反すると考えます。