二第 18号

事　務　連　絡
平成１５年7月１０日

各都道府県
住民基本台帳ネットワークシステム担当部長　殿

総務省自治行政局市町村課長

住民基本台帳法第３６条の２及び第３０条の２９の解釈について

住民基本台帳ネットワークシステムの運営及び構築については、日ごろから御尽力を賜り、誠にありがとうございます。

住民基本台帳法（昭和４２年法律第８１号）第３６条の２及び第３０条の２９の解釈は下記のとおりであり、本日開催された第５回住民基本台帳ネットワークシステム調査委員会において説明しましたので、参考までにお送りいたします。

なお、貴都道府県内の市区町村にも御連絡いただきますようよろしくお願いいたします。

記

住民基本台帳法第３６条の２又は第３０条の２９の規定により住民基本台帳ネットワークシステムからの離脱又は不接続を行うことはできず、住民基本台帳法違反となる。

なお、住民基本台帳ネットワークシステム第一次稼働の際の緊急対策は、住民基本台帳ネットワークシステムからの離脱又は不接続を行ったものではない。（別添資料参照）

住民基本台帳法第３６条の２又は第３０条の２９の規定を根拠として住民基本台帳ネットワークシステムからの離脱又は不接続を行うことは違法

１　はじめに

市町村長（特別区の区長を含む。以下同じ。）は、本人確認情報の都道府県知事への通知（住民基本台帳法（昭和４２年法律第８１号。以下「法」という。）第３０条の５）、住所地以外の市町村における住民票の写しの交付（法第１２条の２）、転入転出手続の特例（法第２４条の２）等の事務を行うものとされている。また、都道府県知事は、市町村長から通知を受けた本人確認情報の磁気ディスクへの記録（法第３０条の５）、本人確認情報の指定情報処理機関への通知（法第３０条の１１）等の事務を行うものとされている。これらの事務は電気通信回線を通じて行うこととされており、市町村長及び都道府県知事は住民基本台帳ネットワークシステム（以下「住基ネット」という。）を運用し、法で定める上記の本人確認情報の通知等の事務を行う義務があるところである。

他方、法第３６条の２及び第３０条の２９の規定により、市町村長及び都道府県知事は、住民票等に記載されている事項又は本人確認情報の漏えい、滅失及びき損の防止その他の住民票等に記載されている事項又は本人確認情報の適切な管理のために必要な措置を講じなければならないとされている。

２　問題の所在とこれに対する考え方

(1) 住基ネットからの個人情報の漏えい等のおそれを理由として、法第３６条の２又は第３０条の２９を根拠として住基ネットから離脱又は不接続を行うことも合法であるとの見解が主張されている。しかしながら、これらの規定は、法に定める事務を実施することを前提として住民票等に記載されている事項又は本人確認情報の適切な管理のために必要な措置を講ずべきことを規定したものであり、また、住基ネットについては、制度面、技術面及び運用面において個人情報保護のための措置が講じられていることを考えあわせても、この規定を根拠として市町村長又は都道府県知事の判断で、住基ネットを運用せず、法に定める本人確認情報の通知等の事務を行わないとすること（いわゆる住基ネットからの離脱又は不接続）はできないものである。

(2) なお、電気通信回線を通じた送信又は磁気ディスクの送付の方法並びに磁気ディスクへの記録及びその保存の方法に関する技術的基準（平成１４年総務省告示第３３４号。以下「住基ネットセキュリティ基準」という。）においては、都道府県、市町村及び指定情報処理機関は緊急時対応計画を定め、ファイアウォールで不正アクセスの徴候を発見したときなど本人確認情報に脅威を及ぼすおそれの高い事象が確認され、本人確認情報の漏えい等の危険が具体的に発生した場合には、相互に連絡調整を行い、被害拡大を防止するための措置等を講ずることとされている。こうした場合の応急的

な措置として、市町村長又は都道府県知事が、住基ネットとの切断等の措置を講ずることまでは否定されないが、かかる具体的な危険性が現実化していない場合に、住基ネットを運用せず法に定める事務を行わないとすることはできないものである。

したがって、単に庁内ＬＡＮがインターネットに接続していること等をもって、住基ネットを運用せず法に定める事務を行わないとすることは違法である。

３　住基ネット第一次稼働の際の緊急対策について

総務省においては、昨年８月５日の住基ネットの第一次稼働に際し、全市町村を対象に住基ネットと接続する既設ネットワークの安全性について点検を実施し、一定のセキュリティ対策を講じていることを確認できなかった市町村に対しては、改善のための支援を実施したところであるが、この緊急対策について、法第３６条の２に基づき市町村長の判断で住基ネットからの一時的な離脱又は不接続を行ったものであるとの見解がある。

しかしながら、この緊急対策は、一定のセキュリティ対策を講じていることを確認できなかった市町村に対して、

① 住基ネットと接続した既設ネットワークについて、外部のネットワークとの接続を遮断する措置を講じること

② ①の措置を講じることが困難な場合には、既存住基システムとコミュニケーションサーバの間を業務時間中遮断し、業務時間終了後、本人確認情報の更新を行うときのみ、接続を行う措置を講じること

を要請したものである。

特に②の措置については、住基ネットの運用を前提として、各市町村のコミュニケーションサーバと既存住民基本台帳システムとの接続方式の一つである媒体交換方式と同様の対応がとられるよう（市町村のコミュニケーションサーバと既存住民基本台帳システムとの接続方式には、回線接続方式と媒体交換方式の２種類がある）、各市町村のコミュニケーションサーバと既存住民基本台帳システムの間の電気通信回線の接続時間を限定し、その中で法に定める事務を実施するべきことを、法第３１条第１項の規定により指導したものである。

したがって、コミュニケーションサーバを停止したり、また、コミュニケーションサーバと住基ネットを切断したりすることなどにより、住基ネットを運用せず、法に定める事務を行わないとすること（いわゆる住基ネットからの離脱又は不接続）としたものではない。

（参考）

住基ネットの個人情報保護のための措置は以下のとおりである。

① 制度面の措置

法において、都道府県や指定情報処理機関が保有する情報を本人確認情報に限定している（法第３０条の５及び第３０条の１１）。なお、本人確認情報のうち、氏名、出生の年月日、男女の別及び住所については、何人でも閲覧を請求することができる情報であり（法第１１条）、住民票コードについては、理由のいかんを問わず、その変更を請求することができるものであること（法第３０条の３）。

また、法においては、住基ネットから本人確認情報の提供を受ける行政機関及び事務は、法に規定されているものに限定し、受領した本人確認情報の目的外の利用を禁止すること（法第３０条の７、第３０条の８及び第３０条の３４）、市町村、都道府県、指定情報処理機関及び本人確認情報の提供を受けた行政機関のシステム操作者等（委託業者を含む。）に対し守秘義務を課するとともに、当該義務に違反した場合の罰則を国家公務員法（昭和２２年法律第１２０号）第１０９条及び地方公務員法（昭和２５年法律第２６１号）第６０条に規定する罰則（１年以下の懲役又は３万円以下の罰金）に比して加重すること（２年以下の懲役又は１００万円以下の罰金）（法第３０条の１７、第３０条の３１及び第３０条の３５並びに第４２条）等の措置を講じている。

② 技術面及び運用面の措置

市町村、都道府県、指定情報処理機関及び本人確認情報の提供を受けた行政機関は、住基ネットセキュリティ基準等に基づき、住基ネットに係る事務処理体制や環境・設備の整備、管理及び運用の適正化等の措置を講じている。具体的には、市町村におけるコミュニケーションサーバ、都道府県サーバ又は指定情報処理機関サーバを結ぶ電気通信回線は、専用回線を使用すること、必要な部分にファイアウォールを設置し通信制御を行うこと、通信相手相互の認証を行うこと、交換するデータの暗号化を実施すること、端末機の取扱いに際し、操作者が正当なアクセス権限を有していることを操作者識別カード及び暗証番号により確認すること等の措置を講じている。