(1) 他者に知られたくない個々人の私生活上の情報がみだりに他者に開示されたり，他者が私事に属する領域に侵入してくる場合には，個人の私生活における平穏が侵害されるのみならず，自らの生き方を自らが決定するという人格的自律を脅かされることとなるから，このような，私事の公開・私生活への侵入からの自由としてのプライバシーの権利は，憲法の基本原理の一つである「個人の尊重」を実現する上での要となる権利の一つであって，単に，不法行為法上の被侵害利益であるに止まらず，いわゆる人格権の一内容として，憲法１３条によって保障されていると解すべきである。

ところで，近年，ＩＴ（情報技術）の急速な発達により，コンピュータによる膨大な量の情報の収集，蓄積，編集，伝達が可能となり，またインターネット等によって多数のコンピュータのネットワーク化が可能となった。公権力や一般企業においては，これらを利用して広範な分野にわたる個人情報が収集，蓄積，利用，伝達されているところ，このようなデジタル情報は，半永久的に劣化しないで保存できること，瞬時に複製，伝達できて，短時間に爆発的に増殖させることができること，複製されても，そのことが容易には判らず，伝達先を把握することはほとんど不可能であること，書き換えも容易であり，書き換えられていることが外観上は判らないこと等の特性があり，一般の住民の間には，自己の個人情報が自己の知らぬ間に収集，利用されることについては，これが漏洩等によって拡散し，悪用され，自己の私生活の平穏が侵害されることへの不安が高まっており，実際に，個人情報の大量漏洩や個人データの不正な売買といった事案が相次いで社会問題化しており，住民の間に強い不安をもたらしている。このような社会状況に鑑みれば，私生活の平穏や個人の人格的自律を守るためには，もはや，プライバシーの権利を，私事の公開や私生活への侵入を拒絶する権利と捉えるだけでは充分でなく，自己に関する情報の他者への開示の可否及び利用，提供の可否を自分で決める権利，すなわち自己情報をコントロールする権利を認める必要が

あり，プライバシーの権利には，この自己情報コントロール権が重要な一内容として含まれると解するべきである。

ところで，コントロール権が認められる情報としては，思想，信条，宗教，健康等にかかわるいわゆるセンシティブな情報を挙げることができるが，その外延は明らかでない。しかし，それは，今後の具体的な事例の積み重ねの中で自ずと明らかになっていくもので，外延が明らかでないからといって，自己情報コントロール権自体を認めるべきではないとは解せられない。また，自己情報コントロール権から派生すると解されている開示請求権，訂正請求権がいかなる場合にいかなる要件で認められるかは困難な問題であるが，これも具体的な事例の中で検討されるべき問題であって，これが明確でないからといって，自己情報コントロール権自体を認めるべきではないとは解せられない。

(2) 住基ネットは，住民が，転入，転居等の事由が生じたために市町村長に届け出た情報のうち，氏名，住所，生年月日，性別の４情報と，市町村長が記載した住民票コード及びこれらの変更情報，以上の６情報（本人確認情報）を，市町村長が都道府県知事に通知し，更に都道府県知事がこれらを被告地自センターに通知し，同地自センターがこれを国の機関又は法人，当該都道府県の区域内の市町村の執行機関，他の都道府県の執行機関，他の都道府県の区域内の市町村の執行機関等に提供するシステムであって，住民は，市町村長に対して上記届出をしたときに，市町村長や都道府県知事によって上記の通知がなされることや被告地自センターによって上記提供がなされることを承諾していたものではないし，上記の通知や提供がなされる際に個別に同意を求められるものでもないから，上記システムは，本人確認情報が自己情報コントロール権の対象となるのであれば，住民が有している本人確認情報に対するコントロール権を侵害するものであるということができる。

(3) そこで，本人確認情報が自己情報コントロール権の対象となるか否かを検

討するに，個人情報といっても，上記のセンシティブな情報から単なる個人識別に使われる情報まで様々なものがあり，その秘匿を要する有無，程度も様々であって，すべての個人情報がプライバシーにかかる情報として法的保護の対象となるとは解せられない。そして，上記４情報は，一般的には個人識別情報であって，その秘匿の必要性が高いものではないということはできる。しかし，このような個人識別情報であっても，これを他者にみだりに開示されないことへの期待は保護されるべきものである上，秘匿の必要性は，個々人によって様々である。すなわち，ストーカー被害に遭っている人にとっては住所について秘匿されるべき必要性は高いし，性同一性障害によって生物学的な性と異なる性で社会生活を送っている人にとっては性別について秘匿されるべき必要性は高いといわなければならない。通名で社会生活を送っている人のうちには，それが戸籍上の氏名でないことを知られたくない人がいるであろうし，生年月日をむやみに人に知られたくないと思う人は少なくあるまい。また，住民票コードは，それ自体は数字の羅列に過ぎないが，住民票コードが記録されたデータベースが作られた場合には，検索，名寄せのマスターキーになるものであるから，これを秘匿する必要性は高度である（住基法３０条の４３によって，民間において，住民票コードの告知を求めることや，他に提供されることが予定されているデータベースを構成することが禁止されているが，本人が自主的に住民票コードを開示し，これをもとに特定の企業内部で利用するためにデータベースを構成することは禁止されていないから，民間においても，住民票コードの利用が広まっていく蓋然性は高い。）。更に，上記変更情報は，婚姻，離婚，養子縁組，離縁，氏名の変更，戸籍訂正等の身分上の重要な変動があったことを推知させるものであるから，これらを秘匿する必要性も軽視できない。そうすると，本人確認情報は，いずれもプライバシーにかかる情報として，法的保護の対象となるというべきであり（早稲田大学事件最高裁判決参照），自己情報コントロール

権の対象となるというべきである。

(4) なお，本人確認情報のうち４情報については，住基ネットシステムの導入前から，何人も，不当な目的によることが明らかである等として市町村長から拒まれない限り，住民基本台帳の一部の写しの閲覧（住基法１１条），住民票の写し等の交付（同１２条）の手続によって入手することができ，本人にはこれをコントロールするすべがなかったから，もともと４情報については，その情報の本人には，これをコントロールできる可能性がなかったということはできる。しかし，だからといって，上記４情報が法的保護の対象にならないということはできない。なぜなら，住基ネットシステムにおける市町村長，都道府県知事及び被告地自センターによる本人確認情報の通知，保存，提供は，本人確認情報の新たな，しかも甚だしい拡散であるし，そもそも現代社会に於けるプライバシーの権利の重要性に鑑みると，住基法による上記閲覧及び写し等の交付を定めた規定自体の相当性を再検討すべきものと考えられるからである。

(5) そうすると，住基ネットは，住民らの本人確認情報に対する自己情報コントロール権を侵害しているというべきところ，自己情報コントロール権も無制限に保護されるわけではなく，公共の福祉のため必要ある場合には相当の制限を受けることはやむを得ない。

そこで，行政上の目的を実現するために，立法によって，自己情報コントロール権の対象となる本人確認情報を本人の承諾なく通知，保存，提供するシステムを運用することがいかなる場合に許されるかを検討する必要があるが，そのためには，①本人確認情報の秘匿を要する程度（社会通念上，誰もが，自ら開示する以外には強く秘匿を望む情報か，できれば秘匿したいという程度の情報か），②システムのセキュリティ（通知，保存，提供することによって第三者が本人確認情報に不正にアクセスしたり，情報が漏洩する危険がどの程度あるか），③通知，保存，提供の態様が個人の人格的自律を脅

かす危険の有無，程度を検討する必要がある。そこで，以下，(6)ないし(8)において，上記①ないし③について検討する。

(6) 本人確認情報の秘匿を要する程度について

前記のとおり，本人確認情報のうち，４情報は，個人によって異なるものの，社会通念上，一般的には秘匿を要する程度が高いということはできない。しかし，住民票コード及び変更情報は，その程度は相当高いというべきである。

(7) システムのセキュリティについて

ア 証拠（各項記載）によれば，次の事実が認められる。

(ア) 住基ネットのハード面におけるセキュリティについて（乙１０，１１）

a ＣＳ，都道府県サーバ，全国サーバ間の通信は，専用回線及び専用交換装置で構成されたネットワークを介して行われ，また，全国サーバと国の機関等のサーバ間では，専用回線ないし記憶媒体のやりとりによる情報交換が行われる。

上記専用回線は，ＶＰＮ（バーチャル・プライベート・ネットワーク）によるもので，物理的に独立した回線ではなく，他の通信と共用の通信回線において，暗号により他の通信と独立した回線を形成するものである。

b 住基ネットにおける情報通信に際しては，暗号技術評価委員会において安全性が確認されている公開鍵方式による通信相手の認証を行っている。

c 住基ネットにおいては，住基アプリケーションによる独自の通信プロトコル（データ通信におけるデータ受送信のための手順や規則のこと）による通信を行っており，インターネットで用いられている汎用のプロトコルを使用していない。そして，指定情報処理機関監視ＦＷ

においてインターネットで使用されるプロトコルの通過を遮断する措置がとられている。

d　被告地自センターは，指定情報処理機関監視ＦＷについて，ネットワーク側への不正通信，ネットワーク側からの不正通信の有無につき２４時間の監視体制をとり，また，ネットワーク内にＩＤＳ（侵入検知装置）を設置して常時監視を行っている。

e　ＣＳ端末において住基ネットアプリケーション（以下「住基アプリ」という。）を立ち上げるためには，ＣＳ端末のＯＳの権限のほかに，住基アプリの専用カードと暗証番号が必要とされている。

(イ) 総務省告示による住基ネットのセキュリティ基準について（乙１の１ないし３）

総務省は，施行規則２条，６条，７条，１０条ないし１４条及び１８条ないし２０条までの規定に基づき，セキュリティ基準を定めて平成１４年８月５日から適用し，その後，同基準を総務省告示第３９１号及び同６０１号で改正し，同６０１号は平成１５年１０月１日から適用された（以下，同６０１号による改正後の上記基準を「現行セキュリティ基準」という。）。

現行セキュリティ基準により，住基ネットにおいては，秘密保護措置として，上記第２の2(6)記載のほか，都道府県，市町村及び指定情報処理機関において次のような措置が講じられている。

a　体制，規程等の整備

都道府県知事，市町村長及び指定情報処理機関に対し，住基ネットにおけるセキュリティ対策のための連絡調整の場の設置，異常の早期発見，連絡のための体制整備，住基ネットの企画，開発，運用に関する規程及び住基ネットシステム設計書，操作手順書，緊急時の作業手順書の整備，住基ネット運用のための職員配置及び適切な人事管理，

同職員に対する教育・研修計画の策定・実施，住基ネットのセキュリティ対策の評価及び改善努力をそれぞれ義務づけ，また，緊急時の体制として，住基ネットが構成機器やソフトウェアの障害により作動停止した際やデータ漏洩のおそれがある場合の行動計画，住民への周知方法及び相互の連絡方法の策定，そのための連携及び研修の実施を義務づけている。

b　重要機能室について

電子計算機室や磁気ディスク保管室は専用の部屋を確保し，確保できない場合は電子計算機及び電気通信関係装置を厳重に固定し，磁気ディスク等を専用保管庫で施錠保管することとしたほか，電子計算機室や磁気ディスク保管室等の重要機能室について，侵入防止のための各種措置をとることとされている。

c　住基ネットシステムの管理

(a)　入退室管理

重要機能室への入室者の限定及び管理，鍵または入退室管理カードの管理，重要機能室への搬入物品の確認や，事務室における職員不在時の施錠等の措置が義務づけられている。

(b)　ソフトウェア開発等の管理

住基ネットシステムの開発，変更時におけるセキュリティ確保，不正行為の防止等が義務づけられている。

(c)　住基ネットシステムの管理

住基ネットを運用する職員には必要なアクセス権限を付与し，電気通信関係装置の管理に付き不当な運用防止のため厳重な確認を行い，管理者権限がない者の操作を防止する措置を講じ，ネットワーク経由の模擬攻撃を適宜実施してその結果に基づき必要な措置を講じ，また，セキュリティ対策に関する情報の収集，分析を実施して

必要な措置を講じることとされている。

(d) 端末機，電子計算機の管理

端末機の取り扱いは，管理責任者の指示ないし承認を受けた者のみが行うこととし，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る確認，操作者確認カード及び暗証番号の適切な管理，電子ファイルの利用制限，操作履歴の記録保存，本人確認情報照会の条件設定，複数回のアクセス失敗による端末機の強制終了等の措置を講じることとされ，また，各サーバについて住基ネットシステムの管理及び運用に必要なソフトウェア以外のソフトウェアを作動させないこととされている。

(e) 磁気ディスクの保管

磁気ディスクについては保管庫等を設置して保管し，磁気ディスク盗難防止のため，持ち出し及び返却の措置，磁気ディスクによる本人確認情報の送付の際の保管状況の確認等の措置を講じることとされている。

(f) 構成機器及び関連設備の管理

構成機器及び関連設備についても，管理方法の明確化，保守の実施，稼働状況の監視，不正プログラムの混入防止等の措置を講じることとされている。

(g) データ等の管理

データやプログラム，ドキュメントの管理についても，使用，複写，消去，廃棄等における適切な管理体制，データの入出力時の適切な管理等が要求されている。

(h) 障害時の対応

住基ネットシステムの障害及び不正アクセスの早期発見機能の整備，不正アクセス判明時の相互の連絡調整及び被害拡大防止のため

の必要な措置を講じることとされている。

(i) 委託を行う場合の措置

住基ネットシステムの開発，変更，運用，保守等について，業者に委託する際には，委託先事業者の社会的信用と能力を確認し，セキュリティ対策実施や不正行為防止のための監督を行い，再委託の制限，分担範囲の明確化等の措置を講じることとされている。

d 既設ネットワークとの接続

住基ネットと既設のネットワークを接続する場合には，既設ネットワークについてもセキュリティ対策を行い，接続状況について相互に連絡調整を行うこととされている。

e 住基ネットの運用

(a) 市町村においてＣＳに記録された本人確認情報について，新たな本人確認情報が記録された場合，従前の本人確認情報は，５年経過後に確実に消去することとされ，また，都道府県サーバ及び全国サーバにおける本人確認情報についても，施行令３０条の６又は３０条の１１規定の期間経過後に確実に消去することとされている。

(b) また，国の機関等に本人確認情報を提供する際には，都道府県知事に，国の機関等と，本人確認情報の漏洩，滅失，毀損の防止その他適切な管理のための措置について協議することとされ，本人確認情報の提供を受ける国の機関等についても，本人確認情報の適切な管理のための措置を講じることとされる。

(c) 必要に応じて，都道府県知事（この項において，指定情報処理機関に対し委任した都道府県知事を含む）は国の機関等及び当該都道府県の執行機関に対し，都道府県知事及び指定情報処理機関は区域内の市町村，他の都道府県その区域内の市町村の執行機関に対し，市町村長は，他の市町村の執行機関及び都道府県知事，都道府県の

執行機関に対し，提供が行われた本人確認情報の適切な管理のための措置の実施状況について説明を求め，その実施の要請を行うこととされている。

(d) 自己に係る本人確認情報の提供又は利用の状況に関する情報の開示請求に適切に対応するため，都道府県知事は，本人確認情報を提供した際及び自己が利用した際には，その状況に係る情報を必要な期間保存することとされる（指定情報処理機関に対し事務委任をした都道府県知事は，指定情報処理機関に上記状況の報告を求めた上で，同様の措置をとることとされる）。上記期間経過後は同情報を確実に消去することとされている。

(ウ) 各市町村のセキュリティ対策に対する自己点検

各市町村は，「住民基本台帳ネットワークシステム及びそれに接続している既設ネットワークに関する調査票」に基づき，住基ネットにおけるセキュリティ確保について，各項目ごとに３点満点とする数十項目の自己点検を実施した。その結果は，平成１５年５月１２日時点で計３２０７団体の平均点が２．４８点，同年８月２５日時点で同じく２．８３点，平成１６年１１月２４日時点で計２９５９団体の平均点が２．８８点であった。（乙１１，３３）

(エ) 住基カードに関する情報について（乙１３）

総務省は，平成１５年５月２７日，施行規則４６条の規定に基づき，住基カード技術的基準を定め，同基準は平成１５年８月２５日から適用された。同基準によれば，住基カードの運用に際し，次のとおり，住基カードに関する情報が通知ないし提供されることとなっている。

a 市町村長は都道府県知事に対し，委任都道府県知事は指定情報処理機関に対し，市町村長，都道府県知事又は指定情報処理機関は，国の機関等に対し，それぞれ，住基ネットを通じ，当該住民の住基カード

の運用状況が運用中，一時停止又は廃止の状況にあることを通知する。

b　住基カードの発行を受けている住民の住民基本台帳がある市町村以外の市町村が本人確認情報の提供を受ける際には，都道府県知事又は指定情報処理機関は，住基カードの有無について通知する。

(オ)　長野県侵入実験について（乙１９，甲共３２の１ないし４，甲共３３の１ないし４，甲共３９，４１）

a　長野県は，平成１４年１２月に発足した長野県本人確認情報保護審議会が，平成１５年８月に県に提出した「長野県本人確認情報保護審議会第１次報告」を受け，住基ネットにおいて，インターネット側から市町村の庁内ネットワークを経由した住基ネットシステムへの不正アクセス及び住基ネットシステムからの本人確認情報漏洩の可能性を確認し，有効な対策を講ずるための資料を得ることを目的として「住基ネットに係る市町村ネットワークの脆弱性調査」を実施することとし，平成１５年９月２２日から同月２４日まで第一次調査を，同年１１月２５日から同月２８日まで第二次調査を実施した（以下，第一次，第二次調査をあわせて「長野県侵入実験」という。）。

長野県侵入実験及びその調査結果の概要は次のとおりである。

b　調査方法

(a)　市町村の庁内ＬＡＮから住基ネットへの侵入（内部からの侵入）とインターネットから庁内ＬＡＮへの侵入（外部からの侵入）の２種類の調査を行った。

(b)　内部からの侵入調査

庁内ＬＡＮに調査用コンピュータを接続して庁内ＬＡＮ及び庁内ＬＡＮ上に存在する各種サーバについての情報を収集し，その情報をもとにサーバの管理者権限奪取を試みた。管理者権限を奪取した既存住基サーバから既存住基サーバ・ＣＳ間の市町村設置ＦＷにつ