特集・自主研究レポート'97❽

◎高度情報通信社会における地方自治体のサービス

■佐倉康之

1―はじめに

近年の情報処理技術や情報通信技術は、日進月歩ならぬ秒進分歩で急速な発展を遂げており、数年前までは夢物語であったことが、今や現実の世界でごく普通に扱えるようになっている。研究者以外の者が、米国の政府機関や大学が公表した文献などを容易に自宅のパソコンで見ることができるなど誰が想像できたであろうか。インターネット等の持つマルチメディア性やその他の関連技術の発達と相まって多種多様なサービスが一般の利用者にも提供されるようになっている。インターネットに代表されるネットワークが拡大・普及するとともに、利用の形態も多様化し、特に通信販売や情報提供など商取引を伴う利用が拡大している。そのサービスの形態は、電子マネー等のさらに利便性の高いサービスへと高度化していくものとみられる。しかし、一般の利用者が安心してネットワークを利用できるようになるには、さまざまな課題を解決しなければならないことがあるのも事実である。

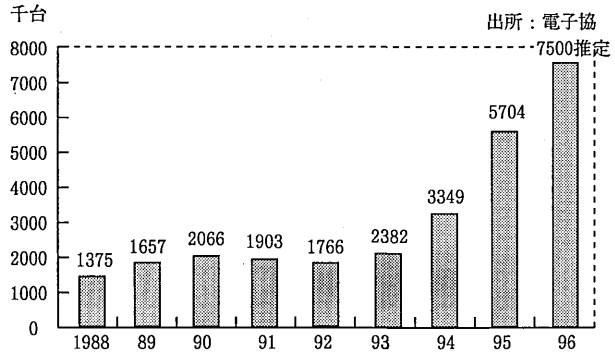
中央政府では、「行政情報化推進計画」を策定し、国民の立場に立った効率的・効果的な行政の実現を目指している。特に、法務省、通商産業省及び郵政省はそれぞれの立場で、ネットワーク上の情報の安全性を確保するための暗号技術の活用や、ネットワーク上で通信の相手方や通信内容の真正性を確認するいわゆる認証に関する制度の検討や実証を行っている。同様に、警察庁でも、ネットワーク犯罪を未然に防止するための研究も行い、来るべきネットワーク社会に対応し始めている。これに対し、地方自治体の情報化は、ただやみくもにWWWサーバを開設したことで情報化に対応したと勘違いし、ネットワークを安全に利用するためのサービスとネットワークを通じて提供するサービスについて、ほとんど検討がなされていない。

2―高度情報通信社会の現状

❶―パソコンの普及

パソコンは、九四年の総務庁の「全国消費実態調査」によると二人以上の一般世帯の情報関連の耐久消費財の普及率は、一六・六%となっており、約六世帯に一台の割合で普及している。十年前の調査では五・八%にすぎなかった普及率が八四年の調査では一二・四%となり、また、経済企画庁の「消費動向調

図―1　パソコン国内出荷台数

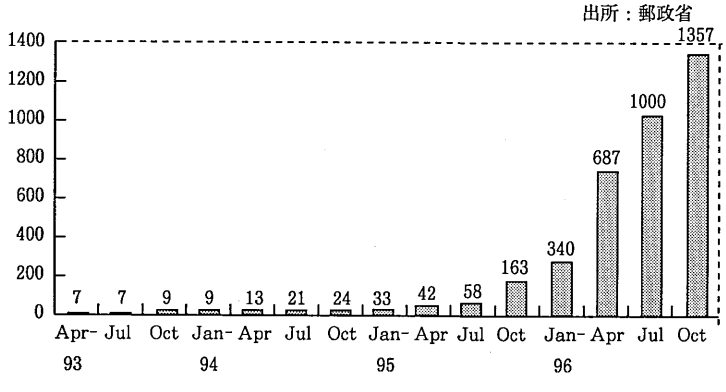


査」によると九六年三月末時点で一七・三％と着実に普及していることがわかる。さらに、日本電子工業振興協会(電子協)の調査によるとパソコンの国内出荷台数は、九四年度の三百三十四万九千台から九五年度の五百七十万四千台へと大幅に増加し、九六年度は七百五十万台を越えることが予想され、先の普及率を勘案すると個人需要が本格化してきたものとみられる。また、違う調査のため単純比較はできないが、ワープロの普及率は九四年の「全国消費実態調査」では四三・七％で、九六年三月の「消費動向調査」では四〇・九％と、普及率が約三％下がっており、情報機器の主流はワープロからパソコンへのシフトが始まったと考えられる。

❷―インターネット・サービス・プロバイダの推移

家庭や企業でインターネットに接続する場合には、電気通信事業法に定められている電気通信事業者であるインターネット・サービス・プロバイダを介する必要がある。特に、プロバイダの大部分を占める一般第二種電気通信事業者は、参入障壁などの規制がほとんどなく初期投資も低額で開業できることから新規参入が相次いだ。この参入ラッシュは、会員から接続手数料を得ることや広告収入によって会社経営を存続させているプロバイダは、当然のようにプロバイダ間で激しい競争が始まり、高値安定していた接続料金が価格破壊を起こし、一部のプロバイダでは接続料金無料というサービスまで行い、会員数の獲得競争がさらなるインターネットのブームを煽った。プロバイダ数の推移グラフからも明らかであるようにプロバイダ数は、九三年四月から九五年七月までは微増傾向であったが、九五年十月から九六年一月まで急増、さらに九六年四月からは激増傾向を示している。この現象は、インターネットの利用者が確実に増加していることを示すものであり、一般家庭にインタラクティブな環境が整いつつあることを示すものである。

図―2　インターネット・サービス・プロバイダ数推移数

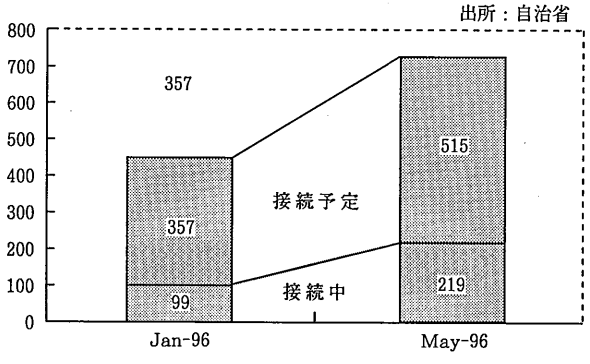


❸―インターネットに接続中及び接続予定の地方自治体数

このように一般家庭にまで普及しつつあるインターネットであるが、地方自治体での普及状況ついては、次のグラフのとおりである。九六年一月と五月に自治省が行った「地方公共団体におけるインターネットの利用に関する調査」では、一月の調査時点で九十九団体しかインターネットと接続しWWWサーバにホームページを開設していなかったが、五月の時点では二百十九団体と倍増以上している。また、接続予定団体も三百五十七団体から五百十五団体へ約一・五倍に増えており、インターネットを利用した情報提供に地方自治体が高い関心があることが示されている。特に、都道府県及び政令指定都市については、九六年度中に全団体が接続する予定となっており、大規模自治体ほど積極的に活用していることが伺われる。

地方自治体がインターネットを利用する目的としては、情報提供によってその地方自治体をアピールし、企業誘致や観光客誘致などの促進を図ることなどがあげられる。しかし、

図―3　地方自治体インターネット接続状況



多くの地方自治体のホームページを見ると内容が通り一遍であったり、情報の更新頻度が低いため陳腐化して役に立たない情報が平然と残っているものもある。また、集合サイトを利用しているホームページでは、どの地方自治体も似たり寄ったりの構成・内容で、自治体のやる気すら感じられない。これらの地方自治体では、インターネットとの接続が目的となってしまって、情報の提供といった真の目的が果たされていないと言わざるを得ない。地方自治体は、積極的にインターネットを利用しているように見えるが、インターネットを活用している自治体は少ないのが現状である。

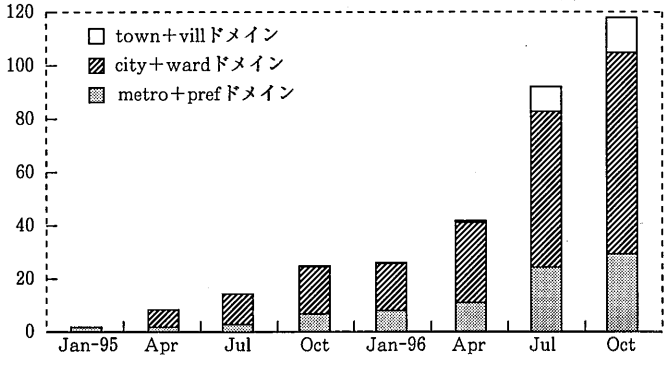
❹－地方自治体の地域型ドメイン割当数の推移

コンピュータネットワークでTCP／IPプロトコル群を使用する場合には、IPアドレスとドメイン名が必要となり、また、外部とのネットワークと接続するためには、共にユニークでないと通信することはできない。我が国では、IPアドレス、ドメイン名の割り当てを日本ネットワークインフォメーションセンタ（JPNIC）が行っている。この組織では、ドメイン名などを割り当てるほか、ドメイン名の命名規約なども定めている。ドメイン名には、属性型ドメインと地域型ドメインがあり、属性型ドメインは、ドメイン名を取得する組織の持つ法的・外形的な位置付けをもとに割り当てられるものである。地域型ドメインは、その地域に住んでいる個人やその地域を中心に活動する法人など地域に密着しているものに割り当てられるドメインである。

特に、地方自治体には、特別のドメイン名として東京都には"metro"、道府県には"pref"、市及び特別区には"city"、町には"town"、村には"vill"が割り当てることになっており、このドメインの取得状況を見ることにより地方自治体の外部ネットワーク接続の関心度を図ることができる。九六年十月現在で都道府県は三十五団体、政令指定市は八団体が割り当てを受けており、規模が大きい団体ほど取得割合が高い。また、九六年五月頃から地域型ドメインを取得する地方自治体が増えてきている。これは、地域型ドメインの割り当て手数料が九六年六月から必要になったための駆け込み申請があったことも要因のひとつであると考えられるが、その後の割り当ての推移を見ると着実に増加しており、地方自治体が外部ネットワークとの接続を積極的な取り組みをしていることのが主因と考えられる。

図－4　地方自治体地域型ドメイン割り当て累計表

出所：JPNIC



3　行政サービスに対する市民ニーズ

九五年八月に市民局が実施した『横浜市区役所窓口事務改善基礎調査』によると区役所窓口の抱える課題・問題点として「取扱時間」、「取扱曜日」、「サービスポイント」、「案内・表示」、「所要時間」、「職員の応対」、「窓口のわかりやすさ」、「機械化」、「庁舎」、「その他」の十項目をあげている。この課題・問題点から市民ニーズは、二十四時間サービスを行う「ノンストップ・サービス」、窓口が市民の身近にある「マルチ・サービスポイント」、手続きが一ヵ所で済む「ワンストップ・サービス」の三つに絞られ、市民は区役所窓口のコンビニエンス化を望んでいると推察できる。

中央政府は、『行政情報化推進基本計画』（平成六年十二月二十五日閣議決定）において、「行政をめぐる内外諸情勢の変化に的確に対応し、行政の総合性の確保、簡素化・効率化の一層の推進、国民ニーズへの対応等を図っていくことが要請されているが、近年急速な進歩を遂げつつある情報通信技術の成果を活用し、これらの要請に一層的確に対処する」ため、国民等からの申請・届出・報告・相談等の電子化を事務内容に即して推進することとし、特に、各種申請・届出等手続について、電子化に対応したものとするための見直し指針を策定することが明記された。さらに、高度情報通信社会推進本部は、申告・申

請手続の電子化・ペーパーレス化を積極的に推進する旨の決定を行った。申請・届出は窓口事務の主要な事務であるから、中央政府はこの決定によって窓口事務の電子化を推進したものであると言える。高度情報通信社会推進本部では、この電子化には、「オフラインによる電子化」と「オンラインによる電子化」があり、「オンラインによる電子化」は、窓口に行かずに、端末機等からダイレクトに申請などができるため、端末機等が存在するところが窓口となるものである。すなわち、この「オンラインによる電子化」は、市民ニーズの一つである「マルチ・サービスポイント」を意味するところである。また、申請や届出などは、職員の審査が必要となるものがあるが、単純な論理チェックだけであればコンピュータによる受付も可能となり、「ノンストップ・サービス」のうち二十四時間受付が実現することになる。この場合では受付以降の行政行為はできないため、「オンラインによる電子化」だけでは、完全な「ノンストップ・サービス」を実現することは困難であることは言うまでもない。

4 ―高度情報通信社会における事務

行政情報システム各省庁連絡会議では、「国民等からの申請・届出等手続について電子化に対応したものとするための見直しを行うことにより電子化を原則として実施することとし、関係法令の改正等所要の措置を講ずる。」としており、特許庁や法務省では、オンラインによる各種申請の導入を予定している。

しかし、インターネットなどオープンなネットワークを利用する場合には、「情報の漏洩防止」（注1）、「発信者の認証と否認防止」（注2）、「情報の改ざん防止」（注3）及び「受信者の認証と否認防止」（注4）の四つの対策を講じなければ、安心して「電子取引」や「オンラインによる電子化」を行うことはできない。これら四つの対策には、暗号化の機能である「情報暗号化」、「ディジタル署名」、「認証機関（CA）」などを利用することが必要となる。

❶―情報暗号化

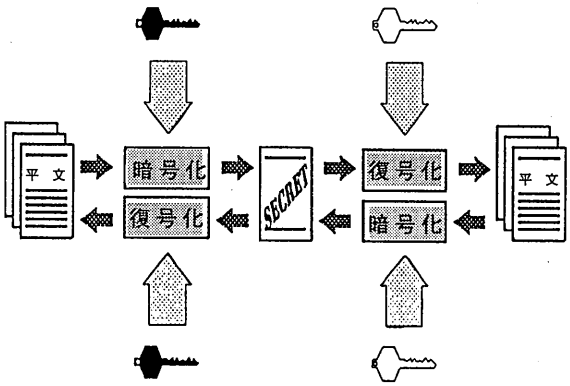
暗号化技術の分類には暗号鍵の公開性に着目した場合には、暗号化と復号化に同じ鍵を用いる共通鍵暗号方式（対称鍵暗号方式、慣用暗号方式、秘密鍵暗号方式とも呼ばれる。）と暗号化と復号化に別の鍵もしくは関数を用いる公開鍵暗号方式（非対称鍵暗号方式とも呼ばれる。）の二種類が存在する。共通鍵暗号方式の特徴としては、必要な鍵の長さが比較的短く、暗号化・復号化が高速なことがあげられる。共通鍵暗号方式の最大の問題は、いかにして発信者と受信者とで鍵を配送するかということである。暗号通信開始前に暗号化されていない状態で鍵を送ることはできない。かといって、鍵を送らなければ暗号通信をできなというジレンマに陥ることになる。公開鍵暗号方式は、暗号化と復号化とでは対になっているそれぞれ別の鍵を使い、どちらかの鍵で暗号化したメッセージはもう一方の鍵で復号化する仕組みになっている。すなわち、どちらか一方の鍵を一般に公開し、もう一方の鍵を自分自身で大切に管理すれば、誰とでも安全に暗号通信ができることになる。

公開鍵暗号方式は、暗号化・復号化に使う鍵を事前に発信者と受信者との間で交換しなくてもよい便利な暗号方法であるが、べき乗などの複雑な計算を行うため暗号化・復号化処理に時間がかかる欠点がある。鍵の長さにもよるが、共通鍵暗号方式と比べると三～四桁処理時間が多くかかることが知られている。そのため、公開鍵暗号方式は、比較的小さいデータの暗号化に適している。しかし、鍵の交換は必要としない性質から不特定多数が利用するネットワークでは、情報の漏洩防止対策としては最も効果的な手段である。

❷―ディジタル署名

我が国では、本人の同一性の確認と意思の確認を印鑑登録証明書で行っているが、ネットワーク上では、現状のような、確認資料を添付する方式では同一性と意思の確認はでき

図―5　公開鍵暗号方式



注1　情報の漏洩防止
「情報の漏洩防止」とは、情報をやりとりする当事者以外の第三者に、その情報が洩れないようにすることである。インターネットが採用しているTCP/IPプロトコルは、オープンなネットワークで用いるプロトコルのデファクトスタンダードとなっている。しかし、このプロトコルではいったんネットワーク上に流れたパケットは、発信者の意思とは関係なしに、ルータのテーブルやトラフィックの状態によって様々なルータを経由して受信者に届くことになる。したがって、データ内容が平文のまま、やりとりが行われていると、経路途中のルータでは、全てのデータが丸見えとなってしまう。このため、情報の漏洩を防ぐには、情報が漏洩する危険なネットワークを利用しないことであるが、もしそのようなネットワークを利用せざるを得ない状況下では、例え第三者に情報が漏洩したとしても、その内容が当事者以外の者には理解できないようにしなければならない。つまり、発信者は情報を暗号化し、受信者が復号化することで情報の漏洩を防がなければならない。

注2　発信者の認証と否認防止
「発信者の認証と否認防止」とは、発信者本人以外のものが発信者になりすましができないよう正当な発信者の証明をし、さらに発信者本人が発信したにもかかわらず発信した事実がないと主張できないよう発信事実の否定を防ぐことにある。

注3　情報の改ざん防止
「情報の改ざん防止」とは、データ内容を伝送途中で変えてしまい発信者、受信者の双方を混乱に貶めようとするものである。オープンなネットワークでは、経路途中のルータで、次のルータへデータを転送するときに、受信したデータをそのまま転送するだけでなく、内容を書き換えることも可能となっている。また、電子化された情報は容易に改変することができ、その上、改変の痕跡さえ残らない。

注4　受信者の認証と否認防止
「受信者の認証と否認防止」とは、発信者が指定した受信人本人に情報が届き、正当な受信者が情報を受信したにも関わらず受信していないと主張することができないようにする対策である。

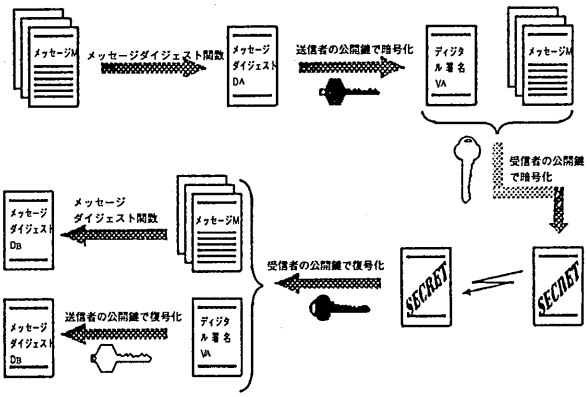
ない。そこで、ネットワーク上でも同一性と意思の確認ができるディジタル署名というものが考えられた。このディジタル署名は、同一性と意思の確認を保証するため、「第三者に偽造されない」、「受信者に偽造されない」、「署名を行った本人が後で否認できない」、「誰にでもディジタル署名の有効性を確認することができる」の四つの要件が満たされなければならない。そのため、ディジタル署名は、毎回同じ署名データが使われるのではなく、送信メッセージの内容に応じて、毎回異なる署名データを生成し、この署名データと送信されたメッセージとの整合性によって、同一性と意思の確認を行うものである。発信者は、メッセージとメッセージを暗号化した暗号文を送信し、受信側では、暗号文を復号化し、その復号化したものと送信されたメッセージが一致すれば、同一性と意思の確認ができたと受信側で判断するものである。

ここで、共通鍵暗号方式では、送信者、受信者双方が同じ鍵を利用するため、受信者が受信した送信されたメッセージを改ざんし、その改ざんしたメッセージを暗号化されるおそれがあるため、暗号文の作成に共通鍵暗号方式を使うことは、「受信者に偽造されない」という要件を単純にはクリアできない。そのため、暗号化する鍵と復号化する鍵が異なる公開鍵暗号方式が、ディジタル署名で使われることになる。

❸ディジタル署名の問題点

ディジタル署名を用いることによって、情報の改ざん防止をすることはできたとしても、本当に発信者Aが自身であるか疑わしい。それは、発信者Aが自身であるかを確認しているのは、Aの秘密鍵を用いて暗号化したものをAの公開鍵で復号化できたことによってである。ここで、Xなる人物がAになりすまし、Aの知らぬ間にAの秘密鍵と公開鍵を作り、それとは知らずに公開鍵がBの手に渡ったとすれば、BはXからのメッセージをAからのものだと信じてしまうであろう。それ故、公開鍵が紛れもなく本人のものであることが証明されなければ、面識のないものとのメッセージの交換を行うことは、非常に危険なこととなる。ネットワークを安全に利用できるようするためには、Aの公開鍵は間違いなくA自身のものであることの証明をしなければならない。また、受信者が、その情報を取得したにもかかわらず、その事実を否定されたとしても反証できない。さらに、内容証明郵便や公正証書のようなメッセージの内容を証明することも必要となる。そのためには、信頼のおける中立的な機関いわゆる認証機関が必要となる。

図－6　ディジタル署名



❹－認証機関

認証機関が提供するサービスとしては、「公開鍵登録申請者の本人確認」、「公開鍵の登録・管理・破棄」、「公開鍵証明書の発行」、「公開鍵の配信・案内」、「送信証明、受信証明」、「内容証明」などがあげられる。これらのサービスは、現在、市町村や法務局で行っている印鑑登録事務、公証人役場で行っている公証人事務及び郵便局で行っている特殊取扱郵便に類似しており、公の機関が実施、関与している。しかし、認証機関については、どのセクターが担うかまだ結論がついていない。郵政省では郵便局が、法務省では法務局等が認証機関として相応しいと考えている。また、通商産業省では、私企業が認証機関として相応しいと考えているようである。それでは、どこが担えば安心できる認証機関となるであろうか。認証機関は、「本人確認の厳密性の確保」（注5）、「全国共通かつ公平のサービス」（注6）、「セキュリティの確保」（注7）、「財務基盤の確立」（注8）、「権威・信頼」（注9）、「個人・法人の基礎的情報の保有」（注10）の六つの要件が満たされなければ認証機関としての責務を果たすことはできない。

この六つの要件を満たすセクターは、個人に関しては市町村、法人に関しては法務局等しかない。認証機関は、高度情報通信社会において市民生活を営む上でも非常に重要な機関

注5　本人確認の厳密性の確保
認証機関のサービスは、認証機関利用者の権利義務の発生、変更等を伴う行為に広く利用されることから本人確認事務の審査が甘ければ第三者のなりすましを見抜くことができずに、認証機関の信用・信頼を失いかねない。そのため、サービスを受けるための第一歩である公開鍵登録申請者の本人確認は厳正かつ慎重に行わなければならない。この厳正かつ慎重に本人確認が行える組織でないと認証機関を担うことはできない。一方、本人確認が厳しすぎて、登録申請者の手数がかかり不便を生じるのも問題であり、そのバランスをとりながら本人確認を行う必要がある。

注6　全国共通かつ公平のサービス
認証機関で提供するサービスは、特定地域だけに限定されるものではなく日本全国で提供されるべき性質のものである。ネットワークを利用することにより公開鍵の配信や公開鍵証明書の発行は、全国共通かつ公平のサービスを提供することは比較的容易にできる。しかし、認証機関で提供するサービスは、これだけではない。前述したとおり、公開鍵登録申請者の本人確認は、認証機関の提供するサービスのなかで最も基本的なサービスである。しかも、この本人確認をネットワーク上だけで行うのは、厳密さを充たしているとは言えない。やはり、本人確認は、対面で行うべきであると考える。印鑑登録の登録申請と同程度のサービス範囲で公開鍵登録申請者の本人確認のサービスを提供できなければならない。

注7　セキュリティの確保
認証機関には、公開鍵登録申請の本人確認や公開鍵を配信請において知り得た情報や利用者の権利義務の発生、変更等に重大な影響を与える情報などプライバシーに関する情報が保管されていることから、これらの情報が第三者に情報が漏洩しない仕組みを構築しなければならない。特に、認証機関は、このような情報を保有し、高度なセキュリティを擁していることから、格好の攻撃対象にされるおそれが十分すぎるほど確保されていなければならない。また、コンピュータに関係した犯罪の多くは、内部犯行であり、内部管理を徹底していなければならない。内部犯罪は、システムそのものを知っている者が引き起こす犯罪であるため、システムのセキュリティが高くてもこのセキュリティは役に立たない。さらに、犯行が発覚しないようカモフラージュするため、長年にわたって犯行が繰り返されやすい傾向がある。認証機関の職員、特にシステムやネットワークに直接携わるものなどの倫理教育も重要な要件となる。

注8　財務基盤の確立
万が一、クラッカーの侵入等によって利用者が被害を受けた場合に、認証機関は、被害を受けた利用者から損害賠償を請求されるおそれもある。その請求に耐えられる「財務基盤」が確立されていなければならない。

であるため、市町村は中央政府の動向を窺うだけでなく、認証機関のサービスを早急に検討し、提供すべきである。

5―市民ニーズの実現

中央政府では、自宅のパソコンを利用した特許出願システムや登記簿の閲覧制度など「オンライン申請」を着々と進めており、市民ニーズを充たす上でも地方自治体の事務も窓口の電子化を早急に進める必要がある。特に、パソコン等の通信機能は、相手が不在であっても伝達内容を正確に伝えることができ、「マルチサービス・ポイント」、「ノンストップ・サービス」に適している情報通信機器である。

図―7は、住民基本台帳事務を例としたオンライン申請のイメージである。ダイアルアップで自宅等から市町村に接続し、ディジタル署名付きの異動届出や証明書の交付申請を行い、郵送で証明書の交付する。手数料は、クレジットカードで支払うものである。この方法によって、「マルチサービス・ポイント」、「ノンストップ・サービス」を実現するものである。

また、住所異動に関しては、市町村の事務だけでなく、郵便局や都道府県公安委員会などの届出を事務の代行や事務委託（注11）を積極的に活用することによって「ワンストップ・サービス」を実現する。

6―市民ニーズの実現への課題

❶―現行法令の抵触

区役所に来庁する市民の約三分の一が利用する住民基本台帳事務を例にあげると、住基法及び住基令の規定では届出書には、「署名または押印」が必要とされている。署名または押印を必要とする理由は、申請者等の申請等の意志確認と悪意の第三者による偽りの申請等を未然に防ぐ犯罪抑止効果である。電子署名を用いたとしても、この「署名または押印」の規定を「署名（ディジタル署名を含む。以下同じ）または押印」等に改正あるいは、規定を廃止しない限りオンライン申請は、現行法令に抵触する。

自治法では、クレジットカードに関する規定はなく、地方自治体がクレジットカードで決済することはできない。しかし、クレジットカードによる決済は、実社会でキャッシュレス取引を実現している数少ないシステムの一つであり、ネットワークを利用した取引の決済手段としては最適なものである。オンライン申請を実現するためには地方自治体でクレジットカードが利用できるよう自治法の改正が必要となる。

❷―情報弱者の対策

「ノンストップ・サービス」、「マルチサービス・ポイント」の実現は、情報通信機器を用いて自宅等から市町村のコンピュータにアクセスして、申請等を行うものであるが、このシステムを利用するに当たっての前提条件は、当然のごとく自宅等に情報通信機器を保有していることのみならず、それを使いこなせなければならないのである。この提言以外にも、地方自治体は、情報通信技術・情報処理技術の成果を行政のあらゆる分野に活用し、市民のための効率的・効果的な行政サービスを提供することが予想され、今日以上に端末情報通信機器の利用が考えられる。このことは、行政サービスを高度化・高品質化するにしたがって、情報通信機器の操作になじめない市民、情報通信機器を保有していない市民は、そのサービスを受けることができずに、サービスを享受できる市民と格差が広がることになる。いわゆる情報弱者の問題が発生する。情報弱者が発生させないためには、情報通信機器を利用したサービスを提供しないことであるが、これでは問題の解決にはならない。しかし、根本的な情報弱者対策は今のところ存在しない。地方自治体は、情報弱者がいることを念頭に置きより多くの市民が利用できるように簡単な操作性を実現するため研究が必要である。

7―おわりに

このドキュメントは、本市の「長期国内留学研修制度」により、埼玉大学大学院政策科学研究科に派遣された二年間の研修成果を修士論文としまとめたものの概要である。そのため、文中の内容は、約半年前のものでありその後の、フォローアップを行っていないため、数値など古いデータとなっていることを御了承していただきたい。また、論文作成に当たっては、関係各課から貴重な資料を提供していただき改めてここでお礼を申し上げる。

〈下水道局経営企画課担当係長〉

注9　権威・信頼
ネットワークは国内と国外との境界がなくシームレスにつながれている。また、ネットワークの利用者は国内・国外と意識せずに利用する。そのため、認証機関は、国内だけでなく海外からも証明書の交付や照会など利用されることが予想されるため、国際的に信頼されなければならない。

注10　個人・法人の基礎的情報の保有
基礎的情報を保有しない組織が認証機関を行うとすれば、ディジタル署名の登録申請の際、個人や法人、団体が存在すること自体を証明するものとして住民票の写しや登記簿謄本などが必要となる。しかし、これらはその交付した時点の証明であり、翌日には存在していないかもしれない。これは、基礎的情報を有していないためである。だが、このことは、個人や法人、団体が存在しないディジタル署名登録できるということにつながり、ディジタル登録自体の信用性を失いかねない。

注11　「ワンストップ・サービス」
運転免許証の記載事項変更事務を都道府県公安員会から道交法の規定により市町村長へ委託し、住所異動届出の際、記載事項変更事務を行う。オンライン申請の場合には、運転免許証裏面に貼付する変更シールを郵送する。
郵便物の転居届
コンピュータに入力された住所異動のデータから、郵便物の転居届に必要なデータを抽出し、転居届のはがきを作成し郵便局に送付する。

図―7　オンライン申請のイメージ図