④ 動き始める行政情報通信基盤

■山口健太郎

1―はじめに

村井純がその著書「インターネットⅡ」で「この環境がすべての人のために公平に、自由に提供されなければならない」と書いて3年、インターネットは本当に急速なスピードで成長している。（参考：横浜市民意識調査）

横浜市が、平成7年1月にインターネットへの接続を行ったときの回線容量は256Kbps（注1）だ。それが現在、一般の家庭からの接続容量が10Mbpsを越えようとしている。大容量、いわゆる「ブロードバンド（注2）」の時代に突入したのだ。

このような通信インフラの充実は、インターネットを経済の基盤として定着させるとともに、ネットワーク上に地域コミュニティを形成する事も容易になってきていることを意味している。それに併せて、関連する法規などの整備も進んでいる。

行政も当然にその対応を求められる。市民にとってもはや特殊でない環境となったネットワークにおいて、これまで窓口で提供してきたサービスなどの実現を求められているといえる。

市民の要求に対する一つの答えが「電子自治体」の実現である。

電子自治体の実現には、各局区の役割、施策を明確にすることとともに、それを実現する情報通信基盤の整備が重要である。

ここでは、総務局が進めている行政情報通信基盤（いわゆる庁内LAN）と今後のサービス提供に不可欠な認証・セキュリティなどについて述べることとしたい。

2―横浜市の行政情報ネットワーク

「とにかくインターネットへの接続をから…」

横浜市がインターネットで情報の受発信を始めてまもなく、その理解を広げていくことを目的として「インターネット実験線」が敷設された。これは、市庁舎に整備された10BASE-5（注3）の幹線などによるネットワーク基盤であった。市庁舎だけでも1000台以上のコンピュータが接続されているこのネットワークは、当初の目的を充分に果たしたといってよいだろう。

メールアドレスの発行は8000を超え、ほとんど全ての局・区が独立したホームページを持ち、提供情報数も7万画面程度になっている。また、インターネットの情報へのアクセス数も、平成13年8月で約400万件／月ページビューを超えているという状態だ。

しかしながら、当初の目的が、インターネットの普及促進に重きを置いていたため、業務用ネットワークとしては確実性や安全性などの面で不充分だった。そこで現在構築を進めている「行政情報通信基盤＝庁内LAN」の整備が進められることになった。

3―行政情報通信基盤

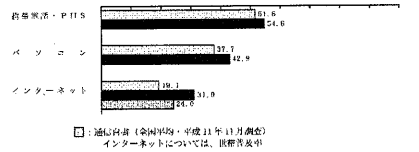
行政情報通信基盤はネットワーク、運用管理の規約整備と利用者教育が一体となって本来の能力を発揮するものであるが、基盤となるネットワークがなければはじまらない。また、その基盤に求められるものは「安全性・確実性」であり、今後様々なアプリケーションの基盤となりうる「応用力」である。もちろん、インターネットを最大限に活用できることも必要だ。

そういうロバスト（注4）で応用力のあるネットワーク実現のポイントとして以下の点に配慮している。

❶―24時間ノンストップ稼働

ネットワークは一定の時間でサービスを停止するというものではなく、いつでも利用で

（参考）平成12年度横浜市民意識調査から携帯電話、パソコン、インターネットの利用状況（平成12年通信白書との比較）



（注1）bps（ビーピーエス）（bits per second）データの転送速度を表す単位の略称。1秒あたりにどれだけのビット数のデータを送信することができるかを示す。モデムの転送速度や、インターネットの専用線の容量を表すのに用いられる。「256Kbps」は「1秒間に256000ビット」のデータを送信できる。「ビット」は、ハードディスクなどの容量で使われる単位「バイト」（byte）とは異なる。8ビットが1バイト。

（注2）ブロードバンド
ADSLなどの技術によって一般家庭でも実現してきた大容量の接続環境を指し、放送や通信に利用できるバンド幅の広いもの言う。従来の56kbps,ISDNの64Kbps以上の通信を一般的にブロードバンドという。

（注3）10BASE-5
コンピュータ同士をネットワーク接続する規格。太さ約10㎜の同軸ケーブル（黄色いことからイエローケーブルなどと呼ばれた）を使ったEthernetの接続方式のこと。「テンベース・ファイブ」と読む。

（注4）ロバスト（robust）
頑強な、障害などに強く停止しないという意味で利用

きるものでなければならない。また、業務のノンストップ化などに対応したものとするためには、24時間止まらずに動くことが必要である。

❷―二重化による確実性の確保

ネットワーク構築において、NOC（注5）などの拠点、回線、ネットワーク機器、主なサーバなどを二重化。故障、メンテナンスなどに対応している。

❸―各種の安全対策

セキュリティ対策は非常に重要な要素である。今回構築するネットワークでは、その構成を整理すると共にファイアウオール（注6）の二重化やネットワークの監視、コンピュータウイルスの対策も行うなど、必要な機能を導入し、安全性を高めたものになっている。

❹―利用者空間と責任範囲の明確化

ネットワークを利用する上で、利用できるドメイン（注7）を明確に定義し、その単位でのコントロールを行うことにより、利用・責任とその範囲を関連づけている。

今回は、横浜市の行政情報通信基盤としてのドメインの中に、局、区、全体というドメインを設けるとともに、それらを包含する横浜市というドメインを定義して、利用やセキュリティのコントロールを行うように考えている。

❺―各局、区が主体となったネットワーク利用・サービス提供が可能

各局、区が各々の組織内でサービスを提供する場合や、ある部署が市内部全体へサービスを提供することを可能とした。各部署がASP（注8）として機能するように配慮し、その環境を提供する。

以上のような点に配慮し、構築されるネットワーク「行政情報通信基盤」は、これまでの「インターネット実験線」と異なり、今後、業務をネットワークを利用して行うための充分な能力と機能を有したものとなる。

ネットワークは、各局区を結ぶ10Mbps程度の回線を中心に、回線の分割利用を可能とするため、幹線部分はATM（注9）により構築される。各回線や、ネットワーク構成は、組織の変更や利用の増加などに対応できるスケーラブルなものであり、その時点で最も経済的な回線などを選択することが可能となる。今後のアプリケーションはこの基盤の上で展開されることになる。

4―PKI（公開鍵認証基盤）

ネットワーク利用の拡大につれ、耳にすることが多くなった言葉にPKI（注10）がある。

❶―なぜPKI

インターネットの研修などの際によく私は電子メールのことを「『ハガキ』のようなものです」といい言い方をする。私設の業者が仲立ちしているハガキだ。その中では、内容を見ようと思えば見ることができるし、何かを書き加えたり、差出人を偽ることさえ可能となる。

国や他の都市と電子メールなどでデータのやりとりをする場合、そのデータは、外のインターネットを経由して相手に届くことになる。通信やデータが暗号化されてなければ、第三者が簡単に内容を見ることも可能だ。

出すものだけでなく受け取る電子メールについても同様、差出人の詐称なども不可能ではない。

インターネットを利用して業務を行ったり、市民サービスを提供する際にはそういったことのないように、

㋐送受するものが、詐称されたり改ざんされたりしない完全性の提供

㋑差出人や受取人を電子的に確認する方法。認証、公証

㋒必要な両者の間でしかデータが解読できないようにする秘匿性の確保

を実現する仕組みが必要となる。それを実現するのがPKIとそれを利用したディジタル署名などの仕組みである。

❷―PKIとは

PKIは非対称鍵暗号を利用した基盤で、特に事前に関係のない両者間でセキュア（注11）な情報の交換を実現するのに適したものである。我々が行う業務の多くは不特定の市民などを対象として行われるため、それに適したものであるともいえる。

例えば、対象鍵暗号に属するID、パスワードを利用したセキュリティでは、事前に相互がその情報を知っている必要があるとともに、ネットワークを利用してパスワードを行

（注5）NOC（Network Operation Center）ネットワーク管理する施設、拠点。サーバやネットワーク機器などを集中して設置する。

（注6）ファイアウオール（Firewall）不正アクセスを防ぐための装置（ハードウエア、ソフトウエア）。定められたポリシー以外の通信を制限する機能を持つ。通常インターネットとの接続部分に設置され外部から内部のネットワークへの不正アクセスなどを制限する。

（注7）ドメイン（domein）ネットワーク上の空間単位、ドメイン名といった場合は、インターネットで利用されるネットワーク名称を指す場合が多い（横浜の地域ドメイン名はcity.yokohama.jp）

（注8）ASP（Application Service Provider）データセンターなどでアプリケーションを動かし、インターネットなどのネットワークを利用してその機能を配信する事業者やその仕組み。ネットワークを通じてソフトウエアを提供することに始まり、様々なサービスを提供する意味も持つ。

（注9）ATM（Asynchronous Transfer Mode）非同期転送モード、データをセルと呼ばれる固定長のフレームで転送する通信方式。ATMはデータ、音声、動画などのさまざまな情報を効率よく伝送可能な方式であるとともに、一つの物理的なネットワークを容易に複数の論理的なネットワークに構築可能。

（注10）PKI（Public Key Infrastructure）公開鍵暗号技術と電子署名を使って、インターネット上で安全な通信を可能とする基盤。「公開鍵基盤」。公開鍵暗号技術では、誰でも利用できる公開鍵でデータを暗号化、自分だけが持つ秘密鍵で復号化するが、その公開鍵を電子署名とともに認証する機関「認証局」（CA：Certification Authority）などを設けてそれを行う。PKIの活用によりデータの盗聴や改ざん、なりすましを防止できる。

（注11）セキュア（secure）安全な

使する場合、その情報自体が、ネットワーク上に流れてしまうという大きな欠点がある。また、交換する情報の相手分ＩＤ、パスワードのペアを作らなくてはならない方法は、不特定多数にサービスを行う行政サービスには向いているとは言えない。

ＰＫＩは非対称鍵暗号を利用した基盤で、ＩＤ、パスワードなどを利用した時の欠点のをなくしたものである。認証局などの仕組みと、公開鍵、秘密（私有）鍵という鍵ペアや公開鍵の証明書などを用いて安全にデータの交換を可能にする。そのような普遍的な基盤を総称してＰＫＩと呼んでいる。

ＰＫＩそのものについては、各種の参考書を見てほしい。ピアソン・エデュケーションから発行されている「ＰＫＩ　公開鍵インフラストラクチャの概念、標準、展開」などが参考になる。

ただ、ここでは今後のネットワーク利用において起こるであろういくつかの事象をあげておこうと思う。

㋐組織間の文書交換などにおいては、現在整備が進められているＬＧＰＫＩ（注12）を利用することになる。また、組織内でも、同様に相互の間で認証を行うための基盤が求められることになる。

㋑市民へのサービス提供についてもＬＧＰＫＩを利用して組織の証明を行うとともに、発行した文書等の確認が可能な環境を作る。また、市民についても何らかの認証基盤が提供される。

今後行う業務については、自治体であることの証明があらゆる場面で必要になることが考えられるため、その準備と実現は非常に重要なポイントである。また、組織としての認証は、幸い自ら構築しなくても、ＬＧＷＡＮ（注13）によって提供されるＬＧＰＫＩを利用することが予定されている。さらに、自組織内の認証を検討し実現することも効率的に業務を行うための鍵となる。

そのＬＧＷＡＮは現在本格運用に向けて準備が進められている。組織認証などの基盤に加えて、データの流通する経路についてもセキュアなものとなっている。国・地方公共団体に閉じた接続となり、その経路に行政に関わりのないデータが流れることがない。このような基盤を利用することで、今後の行政サービスをより一層安全に行うことができる。

5―今後の動向

行政情報通信基盤は平成13年度に局・区、平成14年度以降には主な事務所・事業所について拡張される予定である。部分的な利用は平成13年度から行われるが、全体が整備されて始めて、行政内部のインフラが整ったといえるだろう。

併せて、現在策定を進めているのが、ネットワークを利用するためのルールの策定である。併せて利用者を指導する運用管理責任者などの養成についても検討を進めているところだ。

これまで、ネットワークを利用する上でのルールとしては、横浜市インターネット利用ガイドラインがあった。それが、情報の受発信とインターネット活用を主体としたルールであったのに対し、今回策定するものは業務基盤としてどのように利用するかという視点からのものになる。いかに堅牢な仕組みや技術を持ったネットワークであっても、それを運用する職員が責任を持って利用しなければ無駄になってしまうということだ。

そういったルールの策定と、責任的立場にある職員へのスキル・マインドの習得を目的とした研修を行うことで、行政情報通信基盤は一層強固なものになる。

それらを着実に行っていくことで、本当の電子自治体が実現するはずである。

〈総務局事務管理部情報化推進課〉

（注12）ＬＧＰＫＩ（Local Government PKI）総合行政ネットワーク。現在総務省などによって構築が進められている地方自治体公開鍵基盤、総合行政ネットワーク（LGWAN）を利用し地方自治体の組織認証を行うとともに、インターネットからの公証機能を備える。

（注13）ＬＧＷＡＮ（Local Government WAN）都道府県などを中心とするLGWAN運営協議会によって整備が進められている地方公共団体や国を接続するネットワーク。地方公共団体などに「閉じた」ネットワークで、団体間のデータ通信を安全、確実に行うための仕組みを備える。国などが提供する各種のサービスや組織認証基盤、接続団体間の通信などがこのネットワークを通じて行われる。