2. e-Societyを推進する暗号技術

2. 電子政府・自治体と暗号技術
―戦略的調達へ向けて―

大山 永昭
東京工業大学 フロンティア創造共同研究センター
yama@isl.titech.ac.jp

はじめに

我が国政府は，平成17年度をめどに電子政府を構築するために，「e-Japan戦略II[1)]」や電子政府構築計画などを策定・公表し，電子化の妨げとなる各種の法令等の改正などの制度的な対応に加えて，自ら各種の情報システムの開発・導入を積極的に行っている．電子政府・電子自治体を構築する目的は，すでに多くの人により指摘されているように，行政の効率化とスリム化，行政区域を越えたサービスの提供やサービスの質の向上，さらには電子化された行政情報のバックアップを遠隔地に保管することによる災害対策などである．

一方，社会全体のIT化を推進する目的は，ITがもたらす数々の便益を全国民が享受するとともに，我が国に富をもたらす新規産業の創出や既存産業の国際競争力の回復などである．この観点から電子政府・電子自治体の構築の現状を見ると，年間2兆円もの投資を行っているにもかかわらず，我が国のIT産業とりわけソフトウェア産業は，残念ながら輸出になっていない．さらに，電子政府・電子自治体により提供される各種の行政サービスを，安全かつ安心して利用可能にするために必須となる暗号技術なども，外国に依存している状況にある．

本稿では，これらの課題の解決を目的として行われているIT機器等の調達手法の改善について紹介する．そして，我が国の暗号技術の発展と電子政府・電子自治体の構築に資する戦略的な調達の考え方について解説する．

暗号技術の役割と課題

住民票や印鑑登録証などの各種証明書の自動発行サービスに代表されるように，行政機関の電子化は現実空間から開始された．その後，行政機関間を結ぶネットワークが整備され，さらに公的個人認証サービスなどの開始により，現在では，インターネットなどのネットワークを経由するオンライン化が推進されている．一方では，法的に紙を意味する書面要件などは，平成14年12月に成立した行政オンライン化法などにより，電子書類を紙に置き換える制度的な障害はほぼ取り除かれている．そして，平成16年秋の臨時国会では，民間等に書類の保存を義務付けているものや紙で作られた添付書類等の電子化を可能とするための，いわゆる「e-文書法案」の審議が行われる予定である．これらの作業が完了すると，我が国は電子政府を構築するための制度的な環境整備において，世界中で最も進んだ国の1つになる．

電子政府・電子自治体のサービス提供は，その利便性と効果の観点から必然的にインターネット経由になると予想される．行政サービスは基本的に国民・住民の権利に基づいて提供されていること，そしてその権利は，地方選挙権などを考えれば明らかなように，各人で異なっていることから，本人確認なしで提供することはできない．一方，よく知られているように，インターネットに代表されるオープンなネットワークで構成されるサイバー空間では，他人や架空の人物へのなりすましや情報の盗聴・改ざんがあり得ることから，これらの問題を解決する手段の導入が不可欠である．暗号技術の必要性はまさしくこの点であり，これらの手段が脆弱であれば，電子政府・電子自治体の構築は不可能であろう．

このように暗号技術は，電子政府・電子自治体を支えるきわめて重要な要素技術であるが，技術的にはさらなる発展が期待されることや，安全性のレベルが時間とともに低下することなどを考えると，以下の要件を満たすことが重要になる．すなわち，①暗号の強度が客観化されること，②システムに組み込まれた暗号手法の変更や更新が容易にできること，③複数の暗号が使える

ことである．①は，すでにCRYPTRECなどにより，②はCRYPT-APIなどにより，その解決が図られつつある．ところが，③については，秘匿を主目的とする対称鍵（共通鍵）暗号方式はまだ良いとしても，電子署名などに用いられる非対称鍵（公開鍵）暗号方式では，RSA方式がほぼ独占している．もちろん，クローズなシステムではECC（楕円暗号：Elliptic Curve Cryptosystem）が用いられる場合もあるが，少なくとも電子政府・電子自治体の応用分野ではRSA方式になっている．そしてその主たる原因は，研究レベルでは数々の有望な暗号方式が開発されていても，実用化や標準化が不十分なため，現実に利用することができないことである．この問題を解決するには，新たな暗号手法を必要とする市場の育成が重要であること，一方では電子政府・電子自治体の構築に複数暗号の利用環境が望まれることを考えると，これらを組み合わせる政策的な対応が必要であろう．

先端科学技術の開発と実用化

インターネット，GPS，燃料電池などは，我々の社会にとってきわめて重要な先端科学技術であるが，よく知られているように，これらの技術は米軍とNASAにより開発・実用化されている．もちろん，実際の技術開発は発注を受けた米国の民間企業により行われているが，その研究・開発の成果は実用化の初期段階に達し，現実に発注者により開発された製品の調達が行われている．その後，これらの技術は民間に開放され，たとえば電子メールやカーナビ，さらには電気自動車などを実用化している．これらの先端科学技術の開発・実用化は多額の資金を必要とするため，米軍やNASAなどのいわゆる官からの発注なしでの民間企業による独自開発はきわめて困難であったと考えられるが，ここで重要なことは，これらの先端科学技術に関する基本的な知財は米国により取得されていることである．そして，これらの科学技術の開発を国民が支持していることも，これまでの米国の成功を支えている．我が国の将来として，IT立国や知的財産立国，さらには科学技術立国などを目指すのであれば，このような事実をしっかりと見据えるべきであろう．

上記のことを踏まえて我が国の状況を考えてみると，現状では，高額の費用を投入し，政府自らが最初の利用者となり，さらに国民の支持が得られる最も有望な対象は，まさしく電子政府・電子自治体の構築ではないかと思われる．このことからも電子政府・電子自治体の構築にかかる情報システムの調達は，戦略的に行うべきであるといえる．

政府調達と連携した技術開発の具体的なテーマは，今後より深い検討を通して明らかにすべきであるが，前述した暗号技術の実用化も有望なテーマの1つである．また，すでに成功した実例としては，住基カードの開発があげられる．すなわち，住基カード[2)]は平成11年8月に成立した改正住基法によりその発行が決定されたが，カードに対する機能と安全性に関する要求を満たすスマートカードは，当時，どこにも存在していなかった．そのためまったく新規の開発に着手したが，当時の我が国のスマートカード技術は，技術先進国である欧州の後追いであった．ところが，現在は住基カードの実用化に成功したことから，世界の最先端技術を有することができている．このように世界で最も進んだスマートカードとそのシステム技術を獲得できたのは，4年以上前に要求定義を明確にし，官が自ら調達することを明らかにするとともに，現在の経済産業省が開発支援を行ったことが大きな要因である．これはまさしく，政府調達に絡めた先端技術開発の成功例である．

戦略的な調達への試み

調達を戦略的に行う必要性は，地域や国レベルでのIT産業の育成の観点からも明らかである．すなわち国や地域のIT化は，すでに述べたように国民や地域住民の生活を豊かにするための手段であることを思い返すと，IT産業の中でもソフトウェア関連産業の育成はきわめて重要なことであるといえる．ところが，現状は電子政府や電子政府に多額の費用を投入しているにもかかわらず，これらに関連する産業界のソフトウェアは，海外への輸出になっていない．もちろん，諸外国の行政制度は我が国と異なっているため，日本製のソフトをそのまま輸出できるとは思わないが，少なくともカスタマイズを含めたソフトウェアの受注ができるよう産業界を支援すべきと思われる．

一般的に競争的な市場においては，消費者などのニーズに合わせるために，販売者は取り扱う商品の質を高めるとともにその価格を減じる努力を行うことが重要とされている．このことは，マーケットオリエンテッドな戦略がビジネスの成功の前提条件として多くの人により指摘されていることであり，現状では我が国の自動車産業などがその成功例としてしばしば取り上げられている．このことを念頭において，電子政府・電子自治体に製品を供給する情報システム産業を見ると，発注者側が購入する情報システムに関する知識を十分に有していないため，必然的にベンダへの丸投げに近い体質が残っていることが大きな原因であるといわざるを得ない．これらのことから，本来の目的を達成するためには，発注者側が賢く商品を選べるようにすることがきわめて重要であるといえる．

上記の問題意識の下に，現在，中央政府は全府省等にCIO（Chief Information Officer：情報担当の最高責任者）を平成15年に設置した．そして，ITに関する専門知識を強化するために，CIO補佐官を登用した．さらに情報システムの最適化を実現する具体的な手法としてEA（Enterprise Architecture：業務・システム最適化と訳されている）の導入を図っている．これらの動きは，政府をあげて調達側の責任体制を整え，ITに関する知識を強化し，システムのあるべき姿を共有することで，電子政府で用いる情報システムの質の向上と費用の削減，さらにはIT産業の競争力の強化などを図るためのものであり，今後の成果が期待される．今後は同じような動きが都道府県から市区町村へと広がることが必要であろう．

調達の手順と制度の見直し

情報システムの調達は，①発注者からの要求定義の提示，②システムの設計，③システムの開発，④システムの検収の4段階に分けることができる．この手順を，家を建てる場合にたとえて説明すると，①は一般的に家族会議などを経て決める建物の大きさ，部屋数，部屋の配置，予算などを施主が示すものであり，情報システムの政府調達の場合にはRFP（Request For Proposal）として公表される．そして，RFPに記述される要求の実現可能性等をあらかじめ調査する必要がある場合には，RFPの前にRFI（Request For Information）を出し，情報提供を求めることもある．②は，上流工程と呼ばれるもので，発注者が示した要求を満たす情報システムの具体的な設計を行う工程である．この設計工程の成果は，建物の場合と同じような設計図になるため，当然のことながら発注者の同意を得て次のステップに進むことになる．③は，②で得られた設計図に従って，実際にシステム構築を行う工程（下流工程と呼ばれている）で，建物の場合には工務店などの施工者を決定し工事を行うことに対応している．④は，完成した建物と同じように，構築されたシステムが発注者の要求を満たしているかを含めて，設計通りにできているかを検収する工程である．

構築される情報システムの機能や安全性などはシステム設計に大きく依存しており，決して設計時に想定した以上のことは実現されることはない．そのため，前述のRFPを作成するのに必須となる企画立案はきわめて重要な工程であり，一般的に広く指摘されている業務プロセスの見直しなどを含めると，1年以上の歳月を要することもしばしばである．これらのことを念頭に置いてこれまでに開発・導入されてきた電子政府・電子自治体用の情報システムを見ると，次の更新のためにもできるだけ早期に次期システムの企画立案に着手すること，および調達のプロセスを適正化するための発注者側の意識改革が必要と考えられる．

平成13年には，過度な安値による情報システムの落札を防止し，より効果的な調達を実現するために，経済産業省により調達制度の見直しが開始された．ここで検討された項目は，①外部人材の活用，②複数年契約の実施，③競争入札参加資格の見直し，④総合評価落札方式の見直し，⑤分割調達の実施，⑥契約後のマネジメントの実施，⑦事後評価の実施などである．そしてこれらの課題は，その後の政府内部の検討などにより，①はCIO補佐官の登用として，④は従来の技術点を入札価格で割る方式に加えて，両者の重みつき加算方式の導入などとして，解決されつつある．

おわりに

本稿は「電子政府・自治体と暗号技術–戦略的調達へ向けて–」と題し，はじめに電子政府・電子自治体の構築における暗号手法の役割と複数暗号が使える環境整備の重要性を説明した．次に，電子政府・電子自治体の構築に投入している多額の資金をより有効に使うためには，IT機器調達を戦略的に行うことが必要であり，そのための政府の取り組みを紹介した．さらに，先端科学技術の研究・開発と実用化には大きなギャップがあり，このギャップを埋めるのに政府自らがユーザになることの有効性を，実例をあげて明らかにした．

電子政府・電子自治体の本格的な実運用は，順調に進展すれば数年以内に開始されると予想される．そして一度この実運用が開始されれば，我々住民・国民の多くは，電子的な行政サービスがもたらす数々の便益を享受することになり，その安定したサービスの提供は欠かすことのできないものになると考えられる．暗号技術が電子政府・電子自治体の実運用に不可欠な要素技術であること，暗号の安全性が時間とともに低下することなどを考えると，システム全体の安全性と安定した運用を確保する観点から，電子署名や本人認証などに用いる非対称鍵暗号方式と秘匿通信などに用いる対称鍵暗号方式を早急に複数化することが肝要である．

参考文献
1）e-Japan戦略Ⅱについて，官邸のWebサイト：http//www.kantei.go.jp参照．
2）大山永昭：次世代ICカードシステムの開発と暗号技術，電子情報通信学会誌，Vol.83, No.2, pp.91-95（Feb. 2000）．

（平成16年9月30日受付）