デジタル庁に期待する

一般社団法人情報セキュリティ研究所
代表理事　中村宇利

新聞報道によれば、2020 年 9 月 14 日に組閣された菅新内閣は、「各省庁にある関連組織を一元化し強力な司令塔機能を持たせるデジタル庁を創設する」という。「各府省庁のシステムの一括調達を進めてデータ様式を統一していく。省庁間だけでなく地方の自治体や行政機関の間でもスムーズにデータをやりとりし、行政手続き全般を迅速にする」ことは、いまだ実現していないのが不思議なくらいで、今直ぐ取り組むべき課題である。「強い権限をもつ司令塔として機能させ、首相直轄組織にする新法制定も検討し、予算要求も一元化する」という方針は、欧米どころか近隣の中国や韓国に較べても数年、否、十年以上遅れる日本の官民のデジタル化を促進するためにも心強い。これを機に、世界が進むべき道を日本が示し、再び世界をリードする立場を確立することを期待する。

デジタル化の戦略を考えるうえでまず、日本の現在を正確に把握する必要がある。世界中でデジタル化が進む中日本はどうして後れを取ってしまったのだろうか。
コンピュータの歴史の中で、黎明期においては米国の後塵を拝したが、汎用機、パソコン、OS、マイコン、メモリ等の半導体など、日本人又は日本企業が多くの実績を残してきたことは知られている。現在の機械学習を中心とする AI やアニーリング式量子コンピュータも日本人によって生み出された技術である。また通信の分野においても、光ファイバーや高速無線技術など、世界の先端を歩み続けており、５G、６G につながる重要な役割を果たしてきた。ところが、バブルが全盛を迎え日本が各 ICT 技術分野において世界をリードすることで慢心し始めた頃、世界は、コンピュータや通信技術を総合的に捉え、これらが人類の未来にどのような影響を及ぼし、どのような世界を形成していくか深く考察していた。そして官民が協力して戦略を立て実践してきたのである。例えば、80 年代後半日本が半導体メモリ RAM で米国を凌ぎ、世界市場を独占する時代があったが、RAM では勝てないと判断した米国企業は、表向きにはより付加価値が高いとされる CPU、国家戦略としては半導体設計技術を進化させた。その中から数々の高度な設計技術や製品が生まれたが、その中の 1 つである FPGA（静的可変回路）は、それまで半導体回路の開発ではウエハーに焼き付けてみないと成否が判断できず巨額の開発資金を要していた時代を、いつでも回路の書き換えができる時代に一変させた。日本でも一矢報いようと DRLP（動的可変回路）が開発されたが、その重要性は無視されたまま現在に至っている。今や米国特許を使用せずして半導体開発を行うことは不可能である。また、汎用機と PC という２つに棲み分けされていたコンピュータも、80 年代に商用利用できるようになった米国発の技術であるインターネットと融合し、クラウドコンピューティングに進化した。90 年代前半にこの動きを察知し警鐘を鳴らす者がいたが、当時の通信は狭帯域で、セキュリティも無かったので、日本ではほとんどの企業に嘲笑されるのみで忘れ去られた。今では米国のマイクロソフト、アマゾン、そしてグーグルが世界を席巻しており、日本企業のみならず官公庁でもこれらに依存する事態となっている。これに対して中国はこれらの地殻変動にいち早く感付き、米国の覇権が国内に及ばないよう、国家を上げて様々な対策をとってきた。象徴的なものを紹介すると、マイクロソフトの中国代表を個人的な問題で糾弾し、返す刀でオフィス系ソフトウエアを国産化し、同時にグーグルやアップルに対抗する企業を育て上げた。また米国理系大学への中国人留学生の急増や米国先端企業への就職など、その後の米中冷戦につながる動きも存在する。韓国は逆に、経済危機後多くの金融機関や財閥企業が米国資本を受け入れたこともあり、徹底的に米国追随の戦略をとってきた。こうして日本

の二つの隣人は独自のデジタル化を成し遂げた。
一方バブル崩壊後、日本に戦略と呼べるようなものは存在しなかった。80 年代後半に至る経済成長で米国の虎の尾を踏んだ日本は委縮し、先端技術の種をたくさん産み出しながら、遂にこれらを育てる官庁も企業も現れなかった。むしろ積極的に無視してきたと言っていい。その結果各官庁、各企業が何の戦略もないまま野放図に、手探りでデジタル化を進めた結果が日本の現在である。
現在の行政手続きをデジタル化し迅速化することに反論する人はいないと思うが、デジタル化はすべての産業、国民生活にかかわる問題である。総務省管轄の放送/通信は言うに及ばず、経済産業省管轄のコンピュータや半導体、自動運転、厚生労働省管轄の医療のクラウド利用、金融庁や財務省が関係するフィンテックなどあげればきりがない。これらを一官庁がすべて統括するのには無理がある。むしろどの省庁もほとんど取り組んでいない重要課題を基礎に据え、デジタル化を進めていくのが肝要であろう。その上で、デジタル庁創設を機に、日本の 10 年後、100 年後、500 年後の姿を見据えた戦略を策定し、国をあげて実践すべきと考える。

＜残されたデジタルの重要課題＞
最近ドコモ口座の不正出金事件が報道されたが、2020 年東京オリンピックに向けて万全のセキュリティ対策を施してきた企業の事件だけに大きな注目を集めている。しかし毎日のように報道される様々な情報漏洩事件は、国民の個人情報や産業界の機密情報にとどまらず、防衛や外交などの国家機密情報も例外ではない。
最近は日本でも、特にサイバーセキュリティの重要性が認識され始めており、国家レベルのサイバーセキュリティ体制が強化され、また警察庁でもサイバー対策を重視し、各都道府県警ではサイバー対策課を設けて対策にあたるなどサイバー犯罪への対策を強めている。その結果サイバー犯罪を脅威と考える企業は徐々に減ってきている。しかしながら、サイバー犯罪とは、主にコンピュータネットワーク上で行われる犯罪の総称であり、ネットワーク上の不法取引やデータの大量配布による著作権侵害、法律に違反するデータの公開などがあげられるが、情報セキュリティ上の脅威の一つに過ぎない。ドコモ事件はサイバー攻撃だけによるものではなく、情報セキュリティ対策の欠如に問題がある。また、昨年末には警察庁がフィッシングによるものとみられるインターネットバンキングに係る不正送金被害の急増について、全銀協等と連携して注意喚起を行っているが、これも情報セキュリティ対策の欠如が原因である。
情報セキュリティ上の脅威・攻撃は、①情報の盗難、②情報の改竄、③認証情報の不正使用によるなりすまし、④コンピュータ及びネットワークの破壊・かく乱の４つである。ネットワーク上の攻撃であるサイバー攻撃は、これらのうちの 4 番目に過ぎず、情報セキュリティを考える場合には、4 つすべてに対して適切な対策を講じなければならないが、現在の日本は驚くほど無策である。こうして情報漏洩は起こるべくして起こる。官庁も企業もサイバーセキュリティ対策についてはすでに対策ができると考えるところが多くなっているが、情報セキュリティ全般となるとどうしてよいか分からない。故にできることなら国で対策のガイドラインを示してほしいと要望している。
実は、前世紀中は暗号技術が未完成だったこともあり、十分な対策を講じることができなかった。これは日本だけではない。デジタル化で先行する米国も同様である。これこそが残されたデジタルの重要課題である。
しかし今世紀に入って、従来の計算量的安全性ではなく情報理論的安全性が担保された暗号技術が完成し、超並列計算が可能な量子コンピュータが現実のものとなっても適切な対策が可能となった。世界中がこの新たな技術を応用し、新たなデジタル時代の姿を描き出すべく動き始めている。情報通信分野では、AI、量子コンピュータ、通信、IoT、クラウドコンピューティング、フィンテック、VR/AR の 7 つの分野が有望視されているが、この新たな技術で先行するものが通信、IoT、クラウドコンピューティング、フィンテック、

VR/AR の 5 つの分野で覇権を握ると考えられている。日本も一日も早く 1 つの分野だけでも先行してほしい。
デジタル庁には、行政手続きのデジタル化から始めて、この情報セキュリティを基礎に据えたデジタル化の設計図及び設計ガイドラインを策定することを提案したい。情報セキュリティという世界でもまだ十分とは言えない課題から近未来のデジタル化を考えることで、世界から見ても先進的な状態に持っていくことが可能となろう。以下、具体策を提案する。

＜デジタルの意味するところ＞
その前に、デジタル化を進めるにあたって、デジタルの意味を正確に知る必要がある。
世間では、リアルの世界をすべてデジタル化し、一対一対応させるとか、すべてをビッグデータとして扱い、より良いサービスや製品の提供に活かしていくなどの意見があるが、デジタルの本質を知らない者の暴論といわざるを得ない。デジタル化できるのはリアルのほんの一部に過ぎない。デジタル化されたデータはリアルを切り取ったものであり、矮小化ともいえる。決してリアルのすべてを表現することなどできないことを肝に銘じなければ、デジタルデータをリアルより重視するという愚を犯すことになる。実際中国では国民の個人データだけでなく、すべての行動、思想をも記録しようとしている。そしてその記録をもとに管理する。記録がすべてで、記録を訂正する自由は個人にはない。正しいのは記録で、リアルの個人ではない。中国には大勢の戸籍を持たない子供がいるという。リアルに存在するのに、国家としては存在しない子供達である。
以上のように、改めてリアルが重要であること、記録された（デジタル化された）ものはリアルの一部を表すに過ぎない、単なる偽情報の場合もあると考えることを、人類共通の認識としなければならないだろう。そうすれば、人はデジタルの世界で複数の人格を持ってもよいし、匿名でも生きられる。但し法が必要とする場合には、どの人格であっても個人を特定できるようにして国民としての責任と義務を果たせるようにする。一方で自身の発する情報が偽情報と思われたくないのであれば、自身が特定されるサイン入りで情報を発信すればよい。

＜具体的提案＞
1. 情報セキュリティを基礎に据えたデジタル化の設計図及び設計ガイドラインを策定する
   行政手続き全般をデジタル化するのに、今ではデータ様式を無理に統一化する必要はない。むしろインターネット技術として世界中で使われているプロトコルやフォーマットを積極的に取り入れることで、省庁間だけでなく地方の自治体や行政機関の間でもスムーズにデータをやりとりできるようになる。

   デジタル化の基礎に据える情報セキュリティ対策は、基本を正しく理解し実施することが肝要である。まず、情報セキュリティを考える準備として、どの組織でも、不必要な情報まで集め保管していないか自ら問い、必要な情報だけを、必要な人だけが使用できるようにする。大規模なデータベースを構築している場合にも、本当に統合する必要があるか精査し、分割できる場合には分割する。バックアップについても必ず留意する。
   その上で、A.情報セキュリティ上の防御と、B.情報セキュリティ上の認証の 2 つの基本を押さえて、デジタル化のガイドラインを策定する。
   A. 情報セキュリティ上の防御の基本
      前述の通り、情報セキュリティ上の脅威・攻撃は、①情報の盗難、②情報の改竄、③認証情報の不正使用によるなりすまし、④コンピュータ及びネットワークの破壊・かく乱の 4 つであり、④サイ

バーセキュリティについてはすでに確立された技術で対応し、より本質的な脅威とされる①②③については最新の暗号技術で対応する。

B. 情報セキュリティ上の認証の基本

認証は、複数要素認証と複数経路認証、そして複数の認証者の３つを適切に組み合わせて行う。

複数要素認証は固定型よりも可変型を優先する。認証の問題に対してよく語られる 2 段階認証もパスワードを 2 回同じ経路で送ったのでは、長いパスワードを使ったのと同じであり 2 要素認証とは言えないので注意が必要である。この基本を考慮すれば、キャッシュレス決済で多用される ID とパスワードのみの認証は論外であることが容易に理解されるであろう。現在使用されている「マイナンバーカード」は複数要素認証の 1 つで、サービス提供の経路とは異なる経路を使用するよう推奨しており安全性は低くはないが、固定の認証情報を使用する点で、インターネットバンキングで多用される「ワンタイムパスワード」に劣る。近い将来、可変型の「ダイナミックマイナンバー」に改良されることを期待したい。

情報セキュリティを正しく理解し、国家においても、民間においても、個人においても、ハードについてもソフトについても、正しいデジタル化の設計方法を確立し、設計ガイドラインを策定、提供すべきである。

2. 情報セキュリティを基礎に据えた「Nippon デジタルプラットフォーム」を開発する

上記の設計ガイドラインに則った以下の 4 つのデジタルプラットフォームを開発し､すべての官公庁(国&地方）で使用する。外国製品ではなく中身が透明で、情報セキュリティ対策を施した、独自のプラットフォームを使用する。その結果毎年発生するソフトウエアライセンス料などのシステム費用を最小化できる副次効果も期待できる。

a. パソコン単体レベルのプラットフォーム（OS、オフィスソフトなど）
b. ネットワークレベルのプラットフォーム（ネットワークシステム、ブラウザ、メールシステムなど）
c. クラウドプラットフォーム
d. 次世代製造プラットフォーム

上記のうち a.と b.は、下位互換をもたせるとともに、日本国が存在する限り未来永劫オープンソースで提供し続けていくことを日本政府として世界に宣言する。その結果、日本のみならず世界中がデジタルデバイドの苦悩から解放される。日本の中古ハードを発展途上国に無償提供し、その上で a.と b.のソフトウエアを自由に改造しながら使用してもらうことが可能となり、日本の味方（シンパ）を増やすことができるであろう。

3. 情報セキュリティを基礎に据えた製品/サービスの開発

情報通信の先端暗号技術を用いた５つの重要分野の開発を行い、再び世界の最先端事業をリードする。

応用分野	完全暗号モジュール	具体例
通信	Crypto Comm 秘匿通信用ソフト・ハード	• 秘匿通信 • RSP/TCP/IP
IoT	Ubiquitous MK CryptoSyncKeyを用いるスマートキー	• スマートキー （鍵デバイス） • 自動運転 • スマートグリッド
Cloud Computing	CryptoChain/Cast Smart Contractプラットフォーム	• スマートコントラクト • データ信託
VR/AR	Crypto Print 暗号紋＆遠隔認証	• 暗号紋（著作権保護/管理） • デジタル印鑑 • 証明写真 ･ダイナミックマイナンバー
Fintech	Crypto Cash FinTech関係の応用ソフトウエア	• CBDC • 暗号資産 • 暗号証券／暗号債権 • 暗号保険

① IoT

様々なモノがインターネットに接続され、情報を交換しまた相互に制御する仕組みを IoT と呼ぶ。通信技術に加えて、「遠隔認証」と「秘匿通信」が必須とされ、センサーネットワークやビッグデータ、そして、自動車分野の将来図である自動運転や、エネルギーを相互供給するスマートグリッドに不可欠の技術である。独国のインダストリー4.0 や我が国の Connected Industries においても中心的役割を果たし近未来の工場／製造設備（ロボット等）の要となる。IoT をリードするものが世界の生産をリードする。

② クラウドコンピューティング

アプリケーションとデータをインターネット上に配し、計算もデータ保存／転送もすべてインターネット上で行う技術である。個人情報や産業情報を扱うので、通信技術に加えて、「遠隔認証」と「秘匿通信」「秘匿保管」が必須とされる。現在、マイクロソフトとアマゾンのクラウドサービスが群を抜いており、日本企業は大きく後れを取っているが、医療やネットワークカー（自動運転）などの特定目的クラウドではまだまだ挽回の可能性がある。

③ 次世代通信

現在無線通信の分野では、5G など高速大容量通信において米中がしのぎを削る。しかし通信にとって重要なのは、高速大容量だけではなく、クオリティを含むセキュリティであり中でも「秘匿通信」は不可欠である。無線有線を問わず情報の搬送方法（搬送経路）がどのように変化しようとも、今後インターネットの強大化、高密化に拍車がかかり、より重要なインフラとなることは間違いない。将来インターネットは、現在特定用途向け通信インフラで提供されている特別な通信網や専用線を取り込み、シンプルで安価で安全な最重要ネットワークに進化する。次世代の通信インフラが生まれつつある。

④ VR/AR

専用機を中心に日本が世界を席巻してきたゲームの分野においても、VR/AR を使って新しい 3D コンテンツを利用する時代になった。VR/AR 専用機の分野では米国企業の後塵を拝しているがまだまだ今後の応用分野では日本企業がリードできる分野である。3D コンテンツは 2D に比べてコストがかかるので、ゲームでも映像でも繰り返し利用が必要で著作権管理も重要である。 かつて音楽や映画の著作権管理はレコード/CD 単位での管理を行っていたが、デジタルコンテンツに変わった現在ファイル単位の管理に暗号技術が用いられている。3D コンテンツについても「暗号紋」を使えば、盗難や改ざんを防ぐだけでなく確実な著作権管理ができる。新たな著作権管理団体が組成されることも考えられている。

⑤ フィンテック

各国で自国の法定通貨をデジタル化する試みが始まった。これを可能にするのが「完全暗号」を利用する「クリプトキャッシュ」である。クリプトキャッシュはもともと従来の紙幣の偽造、不正使用を防止する目的で開発されてきた技術であり、21 世紀に入ってようやく完成した。クリプトキャッシュは法定通貨だけでなく、証券や債券、保険証券までをデジタル化することができる。一方で、ブロックチェーンという未熟な技術で始められた暗号資産という新しい通貨型資産は、交換価値があることを認められ新たな産業に育ちつつある。ブロックチェーンを使ううちは偽造、不正使用が絶えないため、これもクリプトキャッシュで作り直せば、安全な暗号資産を作ることができる。その結果、金融分野の産業は劇的な変化を求められるであろう。