2026年７月１１日発行

特集　インフラの維持と未来

行政デジタルインフラとAI
～NY9.11と東北大震災3.11と向き合ったマイナンバー開発者がAI時代を迎えデジタルインフラの活用と課題を考える～

前　地方公共団体情報システム機構（JLIS）理事長
元　みずほ銀行 常務
技術経営士の会　DX支援グループ幹事　吉本 和彦

1．まえがき

AIという新しい産業革命にデジタル世界が直面している安全性問題、日本のデジタル行政の要であるマイナンバーシステムは大丈夫であろうか。
デジタル技術の遅れが問題となっている日本であるが実は世界で最も高い安全性を有していることは余り知られていない。そこには徳川家康が築いた江戸城の知恵が隠されている。
難攻不落であった江戸城の安全性コンセプトが日本のデジタル行政のインフラに活かされている。この堅牢なトラストアンカーを拠り所にしてこそ正しい社会データをAIが学習できる。

日本の要となるインフラ産業にもソブリンクラウドなる名城を築き、新産業革命後も安全・安心な日本社会を創りましょう。

2．日本の行政デジタルの安全性（現在）

税と社会保障の一体改革から始まったマイナンバー制度は、医療も含めて日本の行政

デジタルの根幹としてシステム開発され真に日本のトラストアンカーとなっている。
自治体１７４１を含む３６１１機関を情報連携し、日本の銀行サービスと同じように自治体の窓口だけでなくマイナポータルやコンビニからも利用できる。
システムへのアクセスは、トラストアンカーであるマイナンバーカード(JPKI)を用いて本人確認証明を行っている。

アーキテクチャーは、行政ネットワークの3層分離による情報セキュリティー管理を行っており、江戸城の内堀と外堀のように大手門、坂下門のような門と赤坂見附、四谷見附によって出入りを監視管理している。
このようなゾーンディフェンスを活かして、情報の特性に応じたAIツールの使い分け（ガバナンス）ができ、公開前提の情報ではオープン環境でのChatGPT、行政機密性情報ではLGWAN（総合行政ネットワーク）での自治体AI ZEVOが活用されている。

セキュリティー技術としては、マイナンバーカードのJPKIのほかDBの暗号化かつ分散管理する仕組みとなっている。また自治体CSIRT協議会により、セキュリティー情報の共有・対応を行いNICTのＤＡＥＤＡＬＵＳ(ダイダロス)で不審な通信を２４時間、観測・管理している。

データセンターの安全性についてはどうであろうか。
各国は可能な限りリスクが最小限になるよう堅牢性、バックアップを備えている。
デジタル行政の先進国エストニアは、ロシアの脅威に晒されているので、データセンターのバックアップをNATO本部があるベルギーに置いているのは周知の事実である。
これによって、万が一国土が占領されてもバーチャル国家としてエストニアは生き残る。
日本においても、マイナンバーシステムの構築を機にメガバンクよりも更に安全性が高いデータセンターを構築・配備している。たとえ富士山が噴火して火山灰が降り注いでも大丈夫である。
なお、その場所や内容については、公務員の「秘匿義務」として退職後も一生涯継続されている。

3. 本格的なAI時代を迎えて

生成AIの活用が広がる中で、AIにどこまで任せて良いのかが問われている。
AIは極めて短時間に数万冊の本を読破するスーパー読書家でもあり、本の内容（特にデータ）によって分析結果も異なってくる。

読ませる本の内容によって、即ちデータの真正性の確保やより機密データを扱うことで結果も変わってくる。
AIを外部サービスに委ねて良いのだろうか。
誰もがデータの主権を持つことにより『人がAIを制御していく』鍵となる。
また、EBPM（エビデンスに基づく政策立案）には、説明責任と透明性が問われる。
扱っている顧客データも個人情報保護としてしっかり守っていく義務も課されているのではないか。

最近BAAS*の動きが盛んである　＊Banking as a Serviceの略
JR東日本、高島屋などの一流企業がBAASを使った銀行業務を組込み始めている。
銀行は、マイナンバー(JPKI)により、顧客の本人確認を行っており、架空口座がないよう金融庁までもが厳しく検査している。
自社の経済圏を作るだけでなく、間接的にではあるが、狙いは実質的にマイナンバーによる本人確認が可能となり、なりすまし会員ではなく、真正な顧客データを集めることができる。
BAASを始めた企業は銀行と同様の守秘義務が課されるデジタルインフラ準備が必要だ。

4. 人間がAIを持続的に管理していくには（ソブリンAI）

（１）デジタルインフラをソブリンクラウド化しよう

AIを単に使うのではなく、顧客データを守り、自社の機密データや判断を主体的にコントロールできる形で持つことがこれからの課題である。
ソブリン（主権）AIのためには、そのデジタルインフラとなるシステムが主体的に管理体制がとれるソブリンクラウドである。
日本のクラウド技術は残念ながら大幅に遅れている。純国産のさくらインターネットも頑張っている。ただ果たして純国産に拘わる必要があろうか。
純国産技術に拘らずに米国先進クラウド技術を部品として使って、ソブリンクラウドを達成・運用することは可能である。
例えば、日鉄ソリューション等大手日本のSIヤーがオラクルアロイという部品を用いて、ソブリンクラウドの開発・運用が始まっている。（2022年11月ソブリンクラウド宣言）
米国クラウド法による情報主権が脅かされることもなく、しかも運用コストも安い。円安が進む中、デジタル赤字の増大に歯止めをかけることも大事である。

（2）公開鍵基盤（PKI*）を使って、ドローン、AIエージェントの本人確認をする

＊PKI（Public Key Infrastructure）

インターネット上における人・組織・データの真正性を確保するには、トラストサービスとしてのPKI技術を社会的に広く拡大していくことも必要だ。患者のマイナンバー(JPKI)だけでなく、医者、薬剤師の電子資格確認(HPKI)の確立により、リモート診療も進む。
人だけでなく、ドローン、AIエージェントの本人確認も喫緊の課題であり、PKIの考え方が適用できるのではないか。
もちろんふるさと納税の原産地証明だけではなく、電子文書や、撮影画像の証拠証明にも使えるだろう。

（3）EBPM*1個人データの匿名化について

顧客データをAIにかけることも多くなってくるだろう。
行政データの活用として、自治体フロントヤード改革では、つくば市、浜松市がJLIS*2に匿名加工依頼して、分析を行って、地域政策の一助としている。
企業も個人データを匿名加工する保証・信頼があってこそ、真正なデータが集まってくることに留意すべきである。個人情報保護はAI革命の最も大切な要件である。

＊1 EBPM　エビデンスに基づく政策立案（Evidence-Based Policy Making）
＊2 JLIS　マイナンバーを所管している地方公共団体情報システム機構

本評論は、ソブリンAIを説くことから、私自身一切AIを使用せずに記述した。
文才に乏しい理科系技術者で稚拙な表現や誤字がありましたら、お許し下さい。

＜閑話休題＞

昨年秋、ゴルフ大好き人間の私は所属ゴルフクラブの公式競技で、その日はラッキーが重なり、76のスコアとなりエージシュートを達成した。
会員となっている某ゴルフメーカーからエージシュートのお祝い品が頂けるということになったが、いざゴルフコースの記録証明書を提出したところ、年齢が干支もひとまわり違うと言われてしまった。
私は、趣味や通販などのサイトから生年月日登録を押し付けられる筋合いはないとの主義で、どうしても生年月日を登録しないと会員になれない場合には、仮の生年月日にしていたのに気がつき、そのメーカーさんには、真の生年月日を登録し直すことで笑い話で済みました。
今後も12才若い年齢相応のゴルフ仕様を提案して頂けるようです。
JR東日本さんのSuicaには大人の休日倶楽部を愛用しており、当然正しい年齢を登録しております。

＜自己紹介＞

①富士銀行（現みずほ銀行）のCIOとして、2001年N.Y 9.11同時多発テロの復旧に尽力
②郵政民営化をCIOとして指導し、日本で初めて本格的にクラウドを導入
③フイデアHD（荘内銀行＆北都銀行）のシステム統合と東北大震災の危機管理
④地方公共団体情報システム機構理事長（2期2017年～2023年）として、マイナンバー制度のシステム開発、コンビニでの各種証明書発行を全国に拡大