第４部会－資料４

2020 年 10 月 20 日

東京大 江崎 浩

杉並区 への 提案

(1) デジタルシステムを前提に

デジタル化を元に戻さない。国もデジタル庁を創るなど「完全デジタル化」を推進しようとしています。 さらに、Society5.0 を打ち出した 第 5 次総合科学技術・イノベーション戦略の次の期の第 6 次戦略では、「政府がアーリーアダプタになるとともに、自ら行動変容を起こす」と明記する方向にあり、「Society5.0 の社会実装に関する司令塔を明確化する」ことで、以下を実現するとの目標設定をします。

① デジタルガバメント
② スマートシティー
③ 政府事業等のデジタルイノベーション
④ 中小企業変革

これまでの、物理的なモノ(例えば紙)を前提にした社会経済システムではなく、デジタルシステムでの設計・構築・運用を前提にして、物理的なモノは、例外的なシステムとして考える方向です。これまでの、IT/ICT 施策は、利用の促進や新しい価値の創造 でしたが、次の段階を目指そうというものです。 例えば、ビッグデータや AI の存在を前提にして、これまでのシステムの存在を前提としないシステムの設計や運用を行おうという方向性です。

このような観点からは、以下の 3 つあたりが 大きな柱になっていると考えます。

(a) ペーパレス化

中東アラブ首長国連邦のドバイ市は、2021 年にブロックチェーンを用いて、市のシステムをすべてペーパレス化することを宣言しています。 ペーパレスは、さらに、金銭の出納に関わる書類の電子化を含みます。見積書・請求書・納品書や調達書なども、すべて、デジタルシステムでの運用を前提にします。あくまで、紙は、これを支援するコストのかかるものであり、かつ、**「事実の詐称・改竄の可能性を生むもの」ととらえ、不正の発生を防御するものである**と考えます。

すなわち、**『すべての区の業務において、紙を使わないことを 前提にシステムを見直す・再設計する』**という考え方です。その効果は、

(i) 業務の効率化
(ii) 業務における不正(改竄など)の防止
(iii) 環境対策と地球温暖化防止への貢献
(iv) 災害対策(紙の消失可能性への対応)

(b) 統合化（De-Siloing）　・・・ De-Siloing は 2017 年 3 月の CeBIT での造語

現在の縦割り型の区のシステムを、データセントリックな形態に移行する。それぞれのシステムのオープン化(統一技術仕様化)を、一気に実現するのは、費用と実運用の観点から非現実的であるので、共通のデータ保存システムを設置し、そこに、それぞれのサブシステムがデータの転送を行う形態にする。 区の各部署が、この共通のデータ保存システムに共通の技術仕様でアクセス可能にし、サービス展開を行う。もちろん、このデータは、区民に提供可能なものに関しては、公開しアクセス&利用可能にする。新設するシステムに関しては、既存の縦割り型システムの技術仕様ではなく、共通のオープン化技術仕様を利用するような調達条件・要件にする。

このようなシステム構成は、すでに、米国ニューヨーク市やミシガン州オークランド市などで、採用&実装されている。

この施策の実施にあたっては、

(i)　「調達のスマート化」を実施するための新体制の創設を行うべきだと小職は、考えます。

(ii)　上記の海外の自治体だけではなく、国内のいくつかの自治体との情報交換と連携を実現することが望まれます。

この考え方は、内閣府の Society 5.0 の全体のシステム構成とも整合性がとれたものになっています。

(c) 働き方改革

「職員の在宅勤務環境整備と区民サービスのローカル化」は、是非推進したい案件ではないでしょうか。これは、平成 29 年度の政策キーワードの一つであった「働き方改革」ともリンク・連携可能です。効用としては、以下が挙げられます。言わば、「杉並区行政 KOBAN」です。

(i)　無駄な時間の削減(効率化)

(ii)　区民サービスの向上(地域の情報収集)

(iii)　災害対策(情報収集と発災時の区職員の具体的活動)

(2) ガバナンス体制の確立と新設

以下の 3 つを方向性と挙げてはどうでしょうか？

(a) {サイバー}セキュリティー対策

(i)　仮想化とデータセンター利用

米国政府は、FedRAMP(Federal Risk Authorization Management Program)という政策を推進することになっています。オンサイトに設置されたコンピュータシステムのサイバーセキュリティー対策の実施に必要な経費と人件費・人材の確保は、事実上不可能になったので、基本的にオンサイトは Thin-Client 化し、サーバーはデータセンターに誘導する。これに必要な、調達条件を NIST が作成する。すでに、マイクロソフト社の

オフィス 365(クラウド型の Office)の米国政府版の開発は完了し、NIST および米国政府から認証を得ている。当然、仮想化とデータセンターへの移行は、サイバーセキュリティーの向上だけではなく、

・エネルギー削減
・財務体質の改善(必要な予算のでこぼこが消える＝予算の平滑化)
・在宅勤務の支援

の効果を生む。

オンサイトに設置されたコンピュータには、清掃職員やメインテナンス技術者など、容易にアクセス可能な状況になっていることも、認識されている。

(ii) SOC および CIRT の設置

日本政府として、SOC(Security Operation Center)および CIRT(Cyber Incident Response Team) の設置を推奨している。

(iii) CISO (Chief Information Security Officer)の 設置

CIO(Chief Information Officer)に対応する監査機能を実現する CISO(Chief Information Security Officer) の設置・任命が 望まれる。CISO の重要な職務の一つに、スマートで健全な調達の実施、データの改竄防止などが挙げられる。“業務”監査機能であり、財務監査と並んで組織における監査ガバナンスの実現に重要な職務である。

(iv) 避難所の環境整備

避難所の環境整備として、WiFi 環境の整備 が挙げられる。
より、具体的な施策として、以下の 2 つを提案する。

(a) 現在の低品質の公衆 WiFi の環境の抜本的な見直し・改善

現在の公衆 WiFi 業者が運用する公衆 WiFI)の品質は、低品質であることが一般的である(接続されるが通信品質が非常に悪い)。 根本的な改善を行うべきと考える。 本件は、災害対策のみならず、常時の観光客(特に外国人)へのインターネットアクセスの品質向上に貢献する。

(b) 充電施設の充実

特に災害時は、携帯端末のバッテリー充電設備が重要となる。再生可能エネルギーと大容量の蓄電池の環境整備を行うべき。

(b) 調達体制(スマート調達)

調達手順・フローの抜本的な見直しと、調達基準の作成と確認作業を行う組織を創設すべき。サイバーセキュリティー対策を『梃子に』することは有効な方法である。同時に、長期的な財務体質の改善と持続可能な施設管理を実現することに貢献する。組織統治としての新しい施策と位置付けることができる。

(c) 財務 3 表 の作成

現在実施していると聞いている区の財務 3 表の作成 と、これを支援する財務管理システムの構築。上記(1)(a)「ペーパレス化」 と整合する。すべての 対外ならびに対内の取引をデジタル化する。

(3) 人材の登用と育成

(a) 「シニア」人材の区政への登用

スマート調達の実現には、現場の実状、業者のロジックを熟知した人材が必要となる。このような人材を、現役の区職員で確保あるいは育成するのは、時間と費用が膨大となってしまう。このような、知識と経験を有する人材として、企業等を退職(役職定年を含む)したシニア世代の人材が考えられる。

(b) 若手「エキスパート」人材の育成

総合職ではなく「専門性」を持ったエキスパート人材が、上記(2)(b)のスマート調達の実現には必要となる。このような、専門性を持ったエキスパート人材は、4 年生総合大学よりも、高専などの専門性の高い教育機関の卒業生が適している場合が少なくない。高専などの専門性の高い教育機関との連携によるインターンシップの実施、あるいは、ハッカソンのようなイベントの開催など、有機的で戦略的な人材の育成・確保を実現する体制を目指すべき。

(4) パブリックデータ化の促進による シェアリング・エコノミーの推進支援

区民を含む、自治体に存在する「資源」(Resource) の登録と取り引きを可能とするプラットフォームを、上記、(1)-(b) の「共通のデータ保存システム」を用いて実現することができるであろう。すなわち、民へのデータの提供によるシェアリングエコノミーの実現に際しては、

- 規制
- 税制

が、大きく関係することを認識すべきであろう。

これには、「Dig Once」施策の実現は、その一つの例として、WEF(World Economic Forum)によって提唱されている。

(5) 区民データのデジタル化とオンライン化の支援

ブロードバンドインターネット環境の提供を基本的人権として位置付ける。

(ア) 特に、児童・生徒・学生(含 グローバルな交流の機会)

(イ) 医療・福祉

(ウ) 在宅勤務・・・住宅の物理的環境の重要性

(6) 情報システムに安全性(サイバーセキュリティー対策)

「ファイアウォールによる保護」は、逆に危険な状態を生みます。 特に、ほとんどの業者は、閉じたシステムということを理由に、サイバーセキュリティー対策を実施していないシステムを納品することが非常に多い状況です。そのために、「ファイアウォールを導入しているが故に」サイバーインシデントを経験する確率が大きくなってしまうことが、認識されています。

また、「閉じたシステムなので」、SOC 機能は不要であり実装しないという場合が少なくありません。

この状況を抜本的に解決するために、以下の施策を実施すべきなのです。

(a) スマート調達において、Security-by-Design に基づいた技術基準・要件で、調達手順を実施する。

(b) SOC(Security Operation Center)機能の実現。SOC 自体を創設するということだけではなく、各個別システムにおいて、セキュリティーインシデントの監視機能の導入を推進する。具体的な実現方法は、スマート調達の実現と SOC および CIRT の設置になります。

(7) 人材のオープン化・グローバル化

Incoming と Outgoing の両方において、人材の流動性を向上させ、オープン化を進めるべきであると考えます。

(ア) オンライン環境の提供は、その入口作りになる。

(イ) 何故、米国が強いのか？何故、中国が追い付きつつあるのか？

以上