「政府情報システムにおける クラウドサービスの適切な利用に係る基本方針」 の改定について

Digital Agency

2022年5月24日

ガバメントクラウドチーム

改定の概要

- 旧方針（2018年6月に初版）は、クラウドファースト（先ずはクラウドの利用を検討する）だったが、本方針では**クラウドスマート**（クラウドを賢く適切に利用する）を目的とする。

- タイトルに「適切な」を追加。
「技術政府情報システムにおけるクラウドサービスの**適切な**利用に係る基本方針」

- スマートとは**モダン技術**の利用であり「**マネージドサービス**」と「**IaC** (Infrastructure as Code)」が中心。

「1.1　背景と目的」より抜粋

- 本方針では、政府情報システムが単にクラウドに移行するだけではなく、クラウドの利用メリットを十分に得られるようにするため、政府情報システムがスマートにクラウドを利用するための考え方を示す。

- 従来のクラウドでは、オンプレミスと同様の発想でサーバ構築を中心としたインフラ作業を手作業で実施することが多かったが、今日のクラウドにおいては、**サーバは構築せずにマネージドサービスを利用**することや、**インフラ環境をコードにより自動生成**することが可能である。これにより、従来要していたサーバ構築に伴うコストや、手作業に係る工数を**大きく削減**することが可能となる。

- セキュリティ対策についても、従来のクラウド利用においては、オンプレミスと同様の発想で、ネットワークを中心に自らが構築したサーバを守ることが重要なテーマであったが、今日のクラウド利用においては、マネージドサービス等の利用により、必ずしも**自らサーバを構築する必要がなくなる**ため、データの暗号化や認証など、クラウド利用における様々な**設定を適切に行うことがセキュリティ対策の中心**となる。

「1.1　背景と目的」より抜粋（続き）

- 本方針が旧世代のクラウド利用ではなく、今日のスマートなクラウド利用を促進する目的は、システム開発の短期間化や継続的な開発・改善の実現等の要素もあるが、主として**コスト削減とセキュリティの向上**にある。

- 本方針は、このような大きな技術環境の変化に対応し、政府情報システムが今日においてクラウド利用をスマートに行うための考え方を示すため、旧方針の改訂ではなく、抜本的な改正を行うものである。

「２　基本方針」

- 政府情報システムは、クラウド・バイ・デフォルト原則、すなわち、クラウドサービスの利用を第一候補として、その検討を行うものとする。その際、「３　具体方針」に基づき、単にクラウドを利用するのではなく、**クラウドをスマートに利用**するよう検討するものとする。

- クラウドをスマートに利用するためには、アプリケーションのモダン化が必要となる。新規システムについては当初から、移行システムについてはアプリケーションのライフサイクルにおける刷新タイミングにおいて、「３．４　アプリケーションとシステム刷新について」に基づき、**アプリケーションのモダン化**を検討するものとする。

「3.1　クラウドサービスの選択」より抜粋

- クラウドサービスの利用については**ガバメントクラウドを原則とする**が、ガバメントクラウドを利用しない場合については、セキュリティの観点より、ISMAPに登録されたものを原則として選定する。

- **SaaSについては、開発量削減の観点から幅広く優先的に、その利用を検討する**こと。ただし、ニーズにマッチしているか、開発量削減に貢献するか、セキュリティ対策は十分か、費用対効果は十分に得られるか等を慎重に考慮すること。
  その際には、**ISMAPに未登録でも、ISMAPに登録予定のもの、「4.1 ISMAP以外のクラウドセキュリティ認証」で示される認証を取得しているもの、又は、ISMAPに登録されたIaaS/PaaS上で提供され将来の登録が想定されるサービスについても検討する**こと。

「3.4　アプリケーションとシステム刷新」より抜粋

- 従来型の業務システムを、多種多様なマネージドサービスを利用し、自らサーバを構築しない業務システムとするには、**アプリケーションのモダン化、刷新が必要**となる。

- 費用見積りについては、モダン技術に明るい事業者（担当者）に依頼することが不可欠となる。仮に見積り可能な事業者が現行事業者しか存在せず、現行事業者がモダン技術に明るくない場合には、**現行事業者が体制強化、自己学習、トレーニング受講、資格取得等を実施する時間を想定しておく必要がある**。

- アプリケーションとインフラを分離した調達は、アプリケーションのモダン化とスマートなクラウド利用を阻害する要因となるため、クラウドでは見直しが必要となる。（中略）クラウド移行に向けた刷新においては、**インフラとアプリケーションを同時に刷新する**ことが合理的である。また、事業者や調達についても**インフラとアプリケーションを原則として分離するべきではない**。

「3.4　アプリケーションとシステム刷新」（続き）

- システム規模が大きいために競争環境の醸成が困難な場合には、**マイクロサービスアーキテクチャを採用**し、疎に連携するサービスを基本として調達単位を分割することも有効である。

- （やむを得ない理由で）アプリケーションの改修を最小限にとどめてインフラのみをクラウド化する刷新を選択しなければいけない場合については、これを第一段階と考え、第二段階でアプリケーションも含めた刷新を行うことを**当初から計画しておく**ものとする。
  また、第一段階においても、コスト削減の観点より、**データベースと運用管理系の機能については、マネージドサービスの利用を優先的に検討**するものとする。やむを得ず、サーバ構築のためのインスタンス（仮想サーバ）を利用する際には、その稼働を必要最小限とし、**サーバが実稼働していない時の利用料発生を抑制**すること。インスタンスの容量・能力については、事前評価に加え運用開始後においても、**実際の運用状況から継続的に評価と見直しを行う**こと。インスタンスの長期使用契約を選択する場合は、前述を踏まえた上で、慎重な検討を行うこと。

「3.4　アプリケーションとシステム刷新」（続き）

- 小規模なシステムにおいては、単独での刷新（クラウド移行）よりも他システムへの**統合や廃止を検討**するべきである。近々に統廃合される予定のシステムについては、刷新せずに現行システムを統廃合まで維持した方が合理的である可能性が高い。
  単独での継続が必要なシステムについては、SaaSの採用を優先されたい。

- オンプレミスにおけるアプリケーションとクラウド上のアプリケーションでは、以下の点で大きく異なるので、新規開発時やアプリケーション刷新時には特に留意されたい。
  - **モダンアプリケーションとする**
  - **オンプレミス時代の旧来技術・運用を単純に踏襲しない**
  - **オンプレミス時代の人海戦術的な方式を踏襲せず自動化する**
  - **単なるシステム監視ではなく定量的計測を行う**
  - **セキュリティ対策もクラウドに最適化させる**
  - **開発プロセスをクラウドに最適化させる**
  - **稼働日で完成ではなく日々の運用で改善していく**

（各項目の説明は本文を参照されたい）

「3.5　セキュリティについて」より抜粋

- 「セキュリティと利便性とコストでバランスをとる」、「扱う情報の機密性等に応じたセキュリティ対策をとる」等の基本的な方針は普遍であり、統一基準や「個人情報の保護に関する法律についての事務対応ガイド（行政機関等向け）」への準拠が求められることはオンプレミスと変わらないが、セキュリティ対策についても、オンプレミスとクラウド（特に今日のクラウド）については、考え方や方針レベルで大きく異なる点がある。クラウドを利用する政府情報システムについては、以下を踏まえたセキュリティ対策を行うことを原則とする。

  - **責任共有モデルによる対象の絞り込み**
  - **リファレンスアーキテクチャへの準拠**
  - **境界型セキュリティのみに依存しないセキュリティ対策を行う（ゼロトラスト）**
  - **予防的統制と発見的統制の実施**
  - **セキュリティ対策の自動化**
  - **サーバを構築しないアーキテクチャの採用**
  - **IaCとテンプレート適用による主要セキュリティ対策のデフォルト化と適切なセキュリティ管理**
  - **定量的計測とダッシュボードによる状況の可視化**
  - **継続的なアップデートへの対応**
  - **クラウドに最適化した監査**