デジタル社会推進標準ガイドライン DS-310

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

2022 年（令和４年）12 月 28 日
デジタル社会推進会議幹事会決定

〔ガイドライン〕
規範として順守するドキュメント

〔キーワード〕
クラウドサービス、クラウド・バイ・デフォルト、ガバメントクラウド、ISMAP

〔概要〕
政府情報システムのシステム方式について、クラウドサービスの採用をデフォルト（第一候補）としつつ、単にクラウドを利用するのではなく、クラウドを適切（スマート）に利用するための考え方等を示した標準ガイドライン附属文書。

改定履歴

改定年月日	改定箇所	改定内容
2022年9月30日	－	・初版決定（抜本改定）
2022年12月28日	別添	・「安全保障等の機微な情報等に係る政府情報システムの取扱い」の策定に伴う修正

目次

１　はじめに

１．１　背景と目的

2018 年６月に初版決定された「政府情報システムにおけるクラウドサービスの利用に係る基本方針」（以下「旧方針」という。）は、クラウド・バイ・デフォルト原則に基づき政府情報システムのオンプレミスからクラウドへの移行を促すものであった。旧方針に基づいて多くの政府情報システムがクラウドに移行されたが、一方でクラウドへの移行そのものが目的化されてしまい、必ずしもクラウドサービスの利用メリットを十分に享受できていないといった例も散見された。

こうした状況を踏まえ、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。

これまでの政府情報システムにおけるクラウドサービスの利用の多くは、オンプレミスのサーバ群を単に「雲の向こうにある仮想サーバ群」に置き換え、迅速な整備や柔軟なリソースの増減を図るものにとどまっていた。他方で、近年においては、クラウドサービスの急速な進化・発展により、多種多様なマネージドサービスが利用可能となっており、利用システムが自らサーバを構築しなくても、マネージドサービスを利用することによって、必要とする情報システムを構築することが可能となっている。

また、環境構築の自動化や運用の自動化も大きく進展し、いわゆるインフラ作業（構築・運用・保守）の在り方も以下のように根本的に変化している。

すなわち、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。あわせて、合理的な責任分界の下、コンピュ

ータの基本部分（サーバや OS）のセキュリティ対策を信頼性の高い CSP に委ねることで、利用者はサービス利用に集中することができ、高水準のセキュリティ対策を低コストで実現することが可能となる。

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。オンプレミスから旧世代のクラウドへの移行では、サーバ構築に伴うコストや手作業に係るコストが大きかったが、スマートなクラウド利用ではそれらのコストは大きく削減される。

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。

１．２　適用対象

本方針は、デジタル・ガバメント推進標準ガイドラインが適用されるサービス・業務改革並びにこれらに伴う政府情報システムの整備及び管理に関する事項に適用するものとする。ただし、特定秘密（特定秘密の保護に関する法律（平成 25 年法律第 108 号）第３条第１項に規定する特定秘密をいう。）及び行政文書の管理に関するガイドライン（内閣総理大臣決定。初版平成 23 年４月１日。）に掲げる秘密文書中極秘文書に該当する情報を扱う政府情報システムについては、本方針の全部を適用対象外とする。

また、安全保障、公共の安全・秩序の維持といった機微な情報及び当該情報になり得る情報を扱う政府情報システムについては、別添を除いて本方針の全部を適用対象外とする。

なお、外郭団体や自治体が本方針を参考にすることは自由とする。特にガバメントクラウドを利用する場合については、積極的に参考にされたい。

１．３　位置付け

本文書は、デジタル社会推進標準ガイドライン群の一つとして位置付けられる。

１．４　用語

本方針において使用する用語は、表１-1 及び本方針に別段の定めがある場合を除くほか、標準ガイドライン群用語集の例による。なお、参照しやすいよう用語集と同様の定義を記載する場合がある。その他専門的な用語については、

民間の用語定義を参照されたい。

表 1-1 用語の定義

用語	意味
クラウドサービス（クラウド）	事業者等によって定義されたインタフェースを用いた、拡張性、柔軟性を持つ物理的又は仮想的なリソースにネットワーク経由でアクセスするモデルを通じて提供され、利用者によって自由にリソースの設定・管理が可能なサービスであって、情報セキュリティに関する十分な条件設定の余地があるものをいう。また、本方針でのクラウドは原則として IaaS/PaaS を中心に記述し、SaaS については SaaS と明示して記述する。
CSP（Cloud Service Provider）	クラウドサービスを提供する事業者。
ISMAP（Information system Security Management and Assessment Program）	政府情報システムのためのセキュリティ評価制度のこと。政府が求めるセキュリティ要求を満たしているクラウドサービスをあらかじめ評価・登録することにより、政府のクラウドサービス調達におけるセキュリティ水準の確保を図り、クラウドサービスの円滑な導入に資することを目的としている。 なお、リスクの小さい情報システムが利用するクラウドサービスを対象とした、簡素な仕組みによる評価・登録も検討されている。
オンプレミス	従来型の構築手法で、アプリケーションごとに個別の動作環境（データセンタ、ハードウェア、サーバ等）を準備し、自らコントロールするもの。
IaaS（Infrastructure as a Service）	利用者に、CPU 機能、ストレージ、ネットワークその他の基礎的な情報システムの構築に係るリソースが提供されるもの。利用者は、そのリソース上に OS や任意機能（情報セキュリティ機能を含む。）を構築することが可能である。
PaaS（Platform as a Service）	IaaS のサービスに加えて、OS、基本的機能、開発環境や運用管理環境等もサービスとして提供されるもの。利用者は、基本機能等を組み合わせることにより情報システムを構築する。

用語	意味
SaaS（Software as a Service）	利用者に、特定の業務系のアプリケーション、コミュニケーション等の機能、運用管理系の機能、開発系の機能、セキュリティ系の機能等がサービスとして提供されるもの。
マネージドサービス	利用者が機器やソフトウェア等を購入しなくても必要な機能をサービスとして利用できるもの。 本方針では、CSP によって提供される、利用者に運用負担が生じないサービスを指す。
IaC（Infrastructure as Code）	サーバやネットワーク等のインフラ構成をコードで記述することにより、環境の構築や管理を自動化すること。
マイクロサービスアーキテクチャ	アプリケーションを、モノリシックと呼ばれる一枚岩ではなく、独立性の高いサービスの組合せによって構成する考え方。
ガバメントクラウド	「デジタル社会の実現に向けた重点計画」等の政府方針に基づき、デジタル庁が提供する複数のクラウドサービス（IaaS、PaaS、SaaS）の安全かつ合理的な利用環境。
利用者データ	クラウドサービスの利用者（各府省）が直接的に作成・管理するデータ。システムが自動生成する管理情報等は含まない。
モダン技術	新しい技術のこと。ただし、研究室レベルの最先端技術は含まず、市場に一定レベルで普及しているもの。
モダンアプリケーション	モダン技術によって構築されているアプリケーション。令和 4 年現在であれば、マイクロサービスアーキテクチャ、API、クラウドネイティブ、マネージドサービスのみによる構成等が特徴。
定量的計測	モニタリング（監視）、オブザーバビリティ（可観測性）、ビジュアライゼーション（可視化）の３つの要素から従来のシステム運用（監視業務）をサービス運用（提供サービスの改善）に高度化させるための考え方。

１.５　クラウドサービスの当初からの利用メリット

旧方針策定時において、クラウドサービスを利用する主たるメリットとして、以下を挙げていた。これらのメリットは今日においても有効である。

1)　効率性の向上

クラウドサービスでは、多くの利用者が使用するリソースを共有するため、一利用者当たりの費用負担は軽減される。また、クラウドサービスは、多くの場合、多様な基本機能があらかじめ提供されているため、導入時間を短縮することが可能となる。

2)　セキュリティ水準の向上

多くのクラウドサービスは、一定水準の情報セキュリティ機能を基本機能として提供しつつ、より高度な情報セキュリティ機能の追加も可能となっている。また、世界的に認知されたクラウドセキュリティ認証等を有するクラウドサービスについては、強固な情報セキュリティ機能を基本機能として提供している。多くの情報システムにおいては、オンプレミス環境で情報セキュリティ機能を個々に構築するよりも、クラウドサービスを利用する方が、その激しい競争環境下での新しい技術の積極的な採用と規模の経済から、効率的に情報セキュリティレベルを向上させることが期待される。

3)　技術革新対応力の向上

クラウドサービスにおいては、技術革新による新しい機能（例えば、ソーシャルメディア、モバイルデバイス、分析ツール等への対応）が随時追加される。そのため、クラウドサービスを利用することで、最新技術を活用し、試行することが容易となる。

4)　柔軟性の向上

クラウドサービスは、リソースの追加、変更等が容易となっており、数ヶ月の試行運用といった短期間のサービス利用にも適している。また、一般に汎用サービス化した機能の組み合わせを変更する等の対応によって、新たな機能の追加のみならず、業務の見直し等の対応が比較的簡易に可能となるほか、従量制に基づく価格設定や価格体系が公表されていることも一般的である。

5)　可用性の向上

クラウドサービスにおいては、仮想化等の技術利活用により、複数の物理

／仮想サーバ等のリソースを統合されたリソースとして利用でき、さらに、個別のシステムに必要なリソースは、統合されたリソースの中で柔軟に構成を変更することができる。その結果、24 時間 365 日の稼働を目的とした場合でも過剰な投資を行うことなく、個々の物理的なリソースの障害等がもたらす情報システム全体への悪影響を極小化しつつ、大規模災害の発生時にも継続運用が可能となるなど、情報システム全体の可用性を向上させることができる。

１.６　クラウドサービスのスマートな利用によるメリット

クラウドサービスのスマートな利用においては、これまでの利用メリットに加えて、以下のメリットも享受が可能となる。

1)　マネージドサービスの活用によるコスト削減

旧世代のクラウド利用では様々な機能の実現のために、仮想サーバを構築し、ソフトウェアをインストールし、サーバの運用管理を行うことが一般的であった。すなわち、仮想サーバのクラウド利用料、ソフトウェアのライセンス・保守費用、運用管理の人件費が発生していた。今日のスマートなクラウド利用においては、CSP が提供するマネージドサービスの機能を利用するだけなので、その費用はマネージドサービスのクラウド利用料のみとなり、その金額は多くの場合、旧世代の数分の１といわれている。

自らがサーバ構築をしないため、サーバ構築にかかる固定費が不要になることに加え、インフラ環境が完成されたサービスとして提供されるため、インフラ環境のテストや評価等の作業も大きく削減されるからである。

利用数、利用時間などの従量課金体系である場合、処理量が少ない時から多い時まで、クラウド利用料が処理量にリニアに対応するため、処理量が少ない場合のコスト効率が特に向上し、例えば、処理量の少ない週末や利用時間が限定的な検証環境では処理量が少ない分コストも明確に下がる。

2)　サーバを構築しないシステムにおけるセキュリティ向上とセキュリティ対策コストの削減

自らがサーバを構築し運用すると、そこへのセキュリティ対策として、サーバへの侵入監視・防止、ソフトウェア脆弱性への対応、OS 等のセキュリティ設定管理等を自らの責任で行う必要がある。今日のスマートなクラウド利用においては、マネージドサービスが提供する機能を利用するだけなので、自ら業務影響を避けるなどの理由からアップデートタイミングを定める場合はあるものの、それらの責任と対策が基本的に不要となる。本方針で想定す

るマネージドサービスはISMAPへの登録等で信頼性の高いCSPによって提供されており、利用システム側はサービス利用に集中できるので、高水準のセキュリティ対策が低コストで実現可能となる。

また、マネージドサービスでの管理レベルが高くなり、利用システム側が単にサービスを使うだけとなる度合いが高くなるにつれ、利用システム側のセキュリティ対策の負荷が、より軽減されることになる。

3) IaC (Infrastructure as Code)とテンプレートによる環境構築の自動化によるコスト削減

旧世代のクラウド利用ではインフラ環境の構築を手作業（画面操作）で実施していたが、今日のスマートなクラウド利用においては、CSP 等により準備されたテンプレートをベースに若干の修正を行ったコードを実行することでインフラ環境を構築する。

これは単に手作業からコードの実行によって環境構築コスト（人件費）を削減するだけにとどまらない。第一にインフラ環境が短時間で正確に再構築できるようになる。環境構築時の検証コスト（人件費）を削減し、テスト等での一時的な環境利用も可能にすることで、不使用時等、不必要なクラウド利用料の削減にも貢献する。第二に、インフラ環境がコード化されることによって、コードに対する自動テストやレビューが可能となり、信頼性を向上させる。第三に、コード化されることによって 環境のバージョン管理が可能となる。これはアプリケーション開発と同様の管理方法が適用可能となることを意味し、ガバナンスを効かせつつ継続的な開発・改善を行うといった形でインフラ管理の更なる自動化につながる。

２　基本方針

２．１　クラウド・バイ・デフォルト原則

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。

２．２　モダン技術の利用

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、「３．５　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　具体方針

３．１　クラウドサービスの選択

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。なお、ISMAP 関連の詳細については、「政府情報システムのためのセキュリティ評価制度（ISMAP）の利用について」（令和２年６月 30 日 サイバーセキュリティ対策推進会議・各府省情報化統括責任者（CIO）連絡会議決定）に従うこと。

また、サプライチェーン・リスクについて注意を要する場合は、「IT 調達に係る国等の物品又は役務の調達方針及び調達手続きに関する申合せ」（平成 30 年 12 月 10 日関係省庁申合せ、令和３年９月１日一部改正）に従い事前確認を行うこと。オープンソース等、外部で開発されたソフトウェアを用いるクラウドサービスを利用する場合には、内部にバックドア等の潜在的リスクがないことが事前に確認されていることが望ましい。

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、ISMAP に未登録である場合は、「政府情報システムのためのセキュリティ評価制度（ISMAP）の暫定措置の見直しについて」（令和３年７月６日サイバーセキュリティ対策推進会議・各府省情報化統括責任者（CIO）連絡会議決定）に係る暫定措置に従い利用すること。また、本暫定措置による対応も困難な場合は、当該調達を行う政府機関等における最高情報セキュリティ責任者の責任において、本制度の要求事項や管理基準を満たしていることをそれぞれの政府機関等で確認を行い、加えて、「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についても検討すること。

３．２　クラウド利用者のデータが所在する地域と適用される法令等について

クラウドの利用にあたっては、国内法以外の法令及び規制が適用されるリスクを評価し、情報が取扱われる及び契約に定める場所と準拠法・国際裁判管轄に留意する必要がある。このため、こうしたリスクを低減する観点から、利用するサービスや、データセンタの設置場所等を選択する必要がある。

1)　ガバメントクラウドに選定されているクラウドサービス

ガバメントクラウドのポリシーで許可されている範囲（リージョン、サービス）での利用とすることで、国内に閉じた利用となる。

2)　その他のクラウドサービス

当該クラウドで利用するデータセンタの設置場所に関しては、国内であることを基本とする。

ただし、システムの可用性、データの保存性、災害対策等から冗長化やバックアップ用のデータセンタが海外にあることが望ましい場合、準拠法や国際裁判管轄を確認し、かつ具体的な争訟リスクが低い場合又は別途、契約等において利用者データの保護が担保される場合はこの限りではない。

なお、利用者データ（利用者が作成・管理するデータ）を国外に設置されるクラウドに保管する場合は以下の対策を行うこと。

・利用者データの保護

公開情報ではなく、漏えいした場合のリスクが明らかな利用者データを保管する場合は、最新の「CRYPTREC暗号リスト（電子政府推奨暗号)」に掲載されている暗号又は同等の暗号を用いて利用者データの暗号化を行うこと。また、利用者データの機密性によっては利用者自身の暗号鍵によるデータの保護と鍵管理（BYOK）を行い、クラウド（CSP）や監督権限を持った政府等が利用者データを判読不能とする措置を行うこと。

・利用者データ可用性の確保

利用者データに可用性が要求され、外国の法令に基づいてデータの域内保存義務が課されること等により可用性におけるリスクが予見される場合には、当該法令の効力の及ばない場所（国）にバックアップ等を保持すること等により当該リスクを回避又は低減すること。

３.３　ベンダーロックインについて

データの移行性が担保され、合理的な価格体系が公開された上で、その導入プロセスも含めて透明性が担保されている等の条件を満たすクラウドサービスを選択することにより、CSPによるベンダーロックインを回避すること。

３．４　マルチクラウド等について

個々の政府情報システムにおいて、主たる環境として利用する IaaS/PaaS の CSP を複数とするマルチクラウドはコストが増大することが多いため、真に必要性がある場合を除いては避けること。SaaS 等を中心に特定機能に特化して他のクラウドを併用することは問題ない。

CSP によるベンダーロックインを懸念して、複数の IaaS/PaaS の CSP を積極的に使用する考え方もあるが、「３．３　ベンダーロックインについて」のようにデータの移行性が担保され、合理的な価格体系が公開された上で、その導入プロセスも含めて透明性が担保されていればベンダーロックインには該当しない。

いずれにせよ、技術的な合理性と経済的な合理性を持たないマルチクラウドは厳に避ける必要がある。

クラウドとオンプレミスを組み合わせてデータを処理・保存する利用形態については、オンプレミスからクラウドへの移行期、データの多重バックアップ、ネットワーク遅延が許容できない場合を除いては、システムの複雑化と高コスト化の要因となるため、その適用を避けること。

３．５　アプリケーションとシステム刷新について

クラウドへの移行時における刷新の考え方を以下に示す。新規システムの場合については、ここで記述されている刷新後のシステムを当初から開発する前提で読み替えられたい。また、全体的な事項についてはデジタル・ガバメント推進標準ガイドラインに準拠し、クラウドに関する部分については、本指針を優先されたい。

1)　見積りの取得時の留意点

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。

この際、刷新時のアプリケーション開発コスト（整備経費）の増加分と刷新後のランニングコスト（運用経費）の減少分を総合的に評価する必要があるが、その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。

モダン技術に明るくない事業者による見積りは、従来方式を墨守するためのものが多く、正しい意思決定を阻害するため、技術的な妥当性に加え、比較対象が適切か否か、特定の意図を持った恣意的な見積りとなっていないか等、特に留意が必要となる。

納品物についても、必要性の低いドキュメントを納品物と定義して、利用されない大量ドキュメントに工数（費用）と作業期間を割くのではなく、クラウドの場合は、まず、実機環境で開発構築してみて、試行錯誤や評価の後に、確定した内容のみを真に必要なドキュメントとして納品物とすることが重要である。

2) クラウド移行に向けた刷新

これまでの情報システムにおいては、調達や構築・刷新において、アプリケーションとインフラを分離して考えることが一般的であった。しかし、特にオンプレミスで一般的であった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。なお、本節でのインフラはクラウド環境（オンプレミスではサーバ環境）を指しており、ネットワークや端末等を指すものではない。事業者や調達についてはSIerによる開発等の役務のみを指しており、物品やその付帯作業等を指すものではない。

システムの刷新においても、オンプレミスでは、ハードウェアの老朽化により、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刷新（サーバ更改）する方式が多かったが、これはクラウドへの移行では好ましくない。アプリケーションの改修を前提としない刷新では、マネージドサービスの利用も自らサーバを構築しない構成も非常に困難になってしまう。

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。なお、ここでのアプリケーション刷新は、後述の「4）クラウド上で稼働するアプリケーションについて」への対応であり、BPR やビジネスロジックの刷新を要求しているものではないが、BPR やビジネスロジックの刷新についても、システム本来の在り方から、可能な限り同時に実施されたい。

予算の制約でインフラとアプリケーションの同時刷新が困難と考えられる場合は、刷新時のアプリケーション開発コスト（整備経費）の増加分と刷新後のランニングコスト（運用経費）の減少分を総合的に評価する必要があるが、事

業者から取得した見積りが適切なものか否かを事業者の姿勢や能力から再確認し、必要であれば「1）見積り取得時の留意点」の対応を実施すること。

アプリケーションの刷新に時間を要し、同時刷新がスケジュール的に困難な場合は、刷新スケジュールの見直しが必要となる。

事業者の対応能力で同時刷新が困難な場合は、事業者へ体制強化、自己学習、トレーニング受講、資格取得等を促したうえで、より一層の競争環境醸成を行う必要がある。

システム規模が大きいために競争環境の十分な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。

上記の対応を行った上で、それでも同時刷新が困難で、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、コスト削減の観点から、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とき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） 小規模システムにおける刷新

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。

4） 組織ごとに独立していたシステムの刷新

同じ根拠法によるにもかかわらず、オンプレミスでは府省や自治体など組織ごとに独立したシステムとして運用されていたシステムについては、クラウド利用により物理的な統合が容易になることから、システム更改などの機会に効

率化の手段として１システムへの統合を検討するべきである。長年の個別運用によって組織ごとに相違が生じている可能性が高いが、データ構造、アプリケーション、運用についても積極的に統合・一元化を図り、システムの統合を積極的に検討する必要がある。

5)　クラウド上で稼働するアプリケーションについて

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ため、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

マネージドサービスの組合せだけでシステムを構成する、自らサーバを構築せずシステムを構成するなど、クラウドならではの考え方とする。マイクロサービスアーキテクチャの採用や継続的な改善（開発）もモダンアプリケーションでは一般的である。

・オンプレミス時代の旧来技術・運用を単純に踏襲しない

以下に例示するような旧来技術・運用は、今日のクラウドでは高コスト化の要因となるため、原則として踏襲せず、モダンな技術・運用で再設計を行うべきである。特にセキュリティへの要求水準が高い場合は必ずモダンな技術・運用とすること。旧来技術・運用を継続使用する場合は、それが技術的負債となることに留意されたい。

旧来技術・運用の例：クライアントサーバ方式、専用端末のシンクライアント（VDI）、踏み台サーバ、閉域ネットワークのみに依存したセキュリティ対策、ビジネス要求やシステム価値につながらない監視ツール、メンテナンスを目的とした定期的なシステム（サービス）の停止、夜間に実施する必要のない夜間バッチ、オンプレミス用ミドルウェア等

・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

インフラ環境構築の自動化（IaC）とCI/CDパイプライン化、インフラテストの自動化、システム監視や運用の自動化、セキュリティ監視の自動化をクラウドの機能を活用して行う。

・単なるシステム監視ではなく定量的計測を行う

これまでは、ビジネス価値（政策や業務レベルでの価値）に直結しないイ

ンフラリソース監視やログ監視が一般的だったが、クラウドの機能を用いて定量的計測を行い、業務レベルでのサービス改善につながる監視や運用を行う。

・セキュリティ対策もクラウドに最適化させる

オンプレミスとクラウドでは、セキュリティ対策も大きく異なるため、クラウドに最適化したセキュリティ対策とする必要がある。詳細は「３．６セキュリティについて」を参照のこと。

・開発プロセスをクラウドに最適化させる

オンプレミス時代には、インフラ環境をすぐに使用できない、一時的な使用がコストも含めて困難等の制約があったため、アプリケーションの開発プロセスについても、これらの制約に依存したものとなっていた。クラウドでは、インフラ環境を安価にすぐ使えるため、机上で工数をかけて検討するよりも実機で検証する方が低コストとなることが多い。設計についてもドキュメント作成よりも実機でのプロトタイピングや検証を優先しドキュメント化は後段とする方が合理的であり、ウォーターフォールを採用する場合でも、アジャイル的な手法を重視すべきである。また、クラウドの機能で自動生成可能なドキュメントは積極的に自動生成を行うべきである。

・稼働日で完成ではなく日々の運用で改善していく

オンプレミス時代はシステムを本番稼働させたタイミングで開発が一旦、終了し、その後は運用フェーズと位置付けてシステムを稼働させるだけだったが、クラウド時代では後からのリソース追加やサービス追加などに柔軟な対応が可能なため、本番稼働した後もサービス改善を続け、より利用者に便利なサービスとなるように改善していくべきである。そのため、アプリケーション開発は本番稼働後の運用フェーズも含めて日々改善していくことを前提に予算、体制、スケジュール等を計画しておく必要がある。

マネージドサービス等、クラウドから提供されるサービスのアップデートへの対応についても、義務的な改修負担としてイベント的に捉えるのではなく、通常のアップデートと捉えて日常的に対応していく必要がある。

6) アプリケーションが利用するクラウド機能（サービス）について

市場シェアの大きいクラウドでは、サービス開始当初からの古い機能（サービス）も継続して提供されているため、クラウドが提供する全てのサービスが

必ずしもモダンなものではない。また、クラウドが提供する全てのサービスをそのまま使ったとしても必ずしもモダンなアーキテクチャになるわけではない。

サーバ構築を前提とするものなど、使用を避けるべきサービスもあるため、適切なクラウドサービス上でのシステム構築であっても、事業者からの提案が本方針に沿ったものであるか否かについて留意する必要がある。

7) クラウド移行後のシステム刷新タイミング

オンプレミス時代には、ハードウェアの寿命が業務システムのライフサイクルを大きく支配しており、ハードウェアの更改時にシステムを刷新する方法が一般的であった。しかしながら、クラウドにおいては、ハードウェアの寿命を利用システムが意識する必要がなくなったため、システム刷新タイミングの考え方も見直す必要がある。

マネージドサービスだけを組み合わせて構成するモダンなアプリケーションでは、アジャイル的なアプローチで継続的な改善（開発）が行われるため、アプリケーション自体も陳腐化しにくい。

よって、クラウドに移行後のシステム刷新は、以下のタイミングで行われることが好ましい。

・環境の変化（根拠法の大規模な改正を含む。）に伴い業務システムを在り方レベルで大きく見直す必要が生じたタイミング

・構築時から大きな技術変化（利用可能サービスの革新的な変化）があり、継続的な改善（開発）ではなく抜本的な刷新が必要となったタイミング。旧世代のクラウド利用から今日のスマートなクラウド利用への切替えも含む。

・競争性の確保のため、競争的な調達によって事業者の見直しを行うタイミング

システムを継続使用する間の運用保守事業者については、継続的な改善（開発）を行うシステムについては国庫債務負担行為（複数年契約）での調達が合理的である。単年度での契約を繰り返す場合は、事業者変更時の対応、メリット・デメリットを十分に評価しておく必要がある。

３．６　セキュリティについて

「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、「政府機関等のサイバーセキュリティ対策のための統一基準群」や個人情報の保護に関する法律等の個人情報等の適正な取扱いに関する関係法令等への準拠が求められる[1]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）では、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。

1)　責任共有モデルによる対象の絞り込み

オンプレミス時代のアプリケーションでは、システムを構成するハードウェア、OS、ミドルウェア、業務アプリケーションから、設備・運用も含め、全てのセキュリティ対策を考慮する必要があったが、クラウドにおいては、責任共有モデルにより、クラウドが提供するものは CSP が責任を負い、利用システムはその利用についてのみ責任を負う。

利用システムの責任は、業務アプリケーション、利用者端末、運用、クラウド利用における設定（利用者データの保護に係るものを含む。）、アカウント等に限定される。OSS も含めて業務アプリケーションや利用者データに係るセキュリティ対策はシステム構築側の最終的な責任となるため、システム構築者が自らその対策を行う必要がある。

ISMAP に登録されたクラウドサービスについては、クラウドが提供する部分のセキュリティレベルを利用システムが特に検証を行う必要はないが、ISMAP に登録されていない場合は、「４．１　ISMAP 以外のクラウドセキュリティ認証等」の対応が必要となる。

2)　リファレンスアーキテクチャへの準拠

ガバメントクラウドに選定されているクラウドや一部のクラウドにおいては、CSP によって、そのクラウド利用に最適な考え方や方式がリファレンスアーキ

---

[1] なお、個人情報の保護に関する法律上、行政機関等は保有する個人情報について、CSP が保有個人情報を取扱うこととなる場合も含め、個人情報の漏えい等が生じた場合に本人が被る権利利益の侵害の大きさを考慮し、事務又は業務の規模及び性質、保有個人情報の取扱状況、保有個人情報を記録した媒体の性質等に起因するリスクに応じて安全管理のために必要かつ適切な措置を講じなければならない（同法第 66 条第１項）。

特に、冗長化やバックアップ用のデータセンタが海外にある場合や、ISMAP 等に登録されたクラウドサービス等の民間事業者が提供するクラウドサービスを利用する場合で、当該民間事業者が外国にある事業者の場合や当該民間事業者が国内にある事業者であっても外国に所在するサーバに保有個人情報が保存される場合においては、「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）」（令和４年２月個人情報保護委員会事務局））等も参照しつつ、外的環境の把握等の対応が必要となる点に留意が必要である。

テクチャとして用意されている。過去のオンプレミス時代のセキュリティ対策の踏襲を基本とするのではなく、利用するクラウドのリファレンスアーキテクチャに準拠した最新の対策を行う必要がある。

3) 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）

オンプレミスでは境界型セキュリティの考え方に基づいてネットワークセキュリティを重視して、危険な外部と安全な内部を遮断するといった対策方法が主流であったため、内部についてのセキュリティ対策が十分でない場合があった。クラウド利用時においては、ゼロトラストの考え方に基づいて全てのレイヤーでセキュリティ対策を検討し、エンド・ツー・エンドで、データの秘匿・保護を行い、動的に監視や認証等を実施することが推奨される。

4) 予防的統制と発見的統制の実施

誤った設定による意図しない情報の外部公開を避け、システムをセキュアに保つため、クラウドでは様々な設定を正しく行い、維持することが重要となる。

予防的統制とは不正な操作を事前に防止することであり、発見的統制とはリソースが不正な状況になっていないかを継続的に監視し修正する機能である。

予防的統制では、組織で定めたポリシー（国外サービスの利用禁止、必要なログの取得、高権限アカウントの管理等）を設定し、発見的統制では、前述のポリシーの準拠状況、暗号化や監視の実施状況、外部公開設定等を定期的に監視し必要に応じて修正する。

5) セキュリティ対策の自動化

オンプレミス時代はセキュリティ対策を人海戦術的に実施したり、全量検査ができないためサンプリングによる検査を実施したりしていたが、クラウドにおいては、前述の予防的統制、発見的統制、セキュリティ対策のデフォルト化に必要となる、全量ログ保管とその分析を自動化したセキュリティ対策がサービスとして利用可能である。これにより人為的なミスによる見落とし、検知の遅れや抜け等が大きく是正されるとともに、セキュリティ運用の低コスト化も期待できる。

また、セキュリティ対策の自動化には、インシデント対応の自動化も含まれることが望ましい。調査作業等においても自動化が可能となる領域が拡大しており、自動化によるインシデント対策のスピードアップ、高度化を図ることも望ましい。

6) サーバを構築しないアーキテクチャの採用

自らサーバを構築し運用すると、そのサーバにおけるセキュリティに関する監視や運用を自らの責任で行う必要がある。システムで求められるセキュリティ監視、運用機能を具備したクラウドが提供するマネージドサービスを利用することで、サーバ構築が不要となると、サーバのセキュリティ対策もサービス（サーバ）を運用する CSP が実施することになり利用システムでは不要となる。

サーバを構築しないこと自体がセキュリティ対策であり、大きなリスク軽減となる。ただし、アプリケーションやデータなどに関するセキュリティ対策は利用システム側の責任において実施する必要があるため、「1）責任共有モデルによる対象の絞り込み」等を参考に利用システムで検討すること。

また、自らがサーバを構築すると、その部分については前述の予防的統制と発見的統制、セキュリティ対策のデフォルト化、自動化についても阻害される場合があるので特に留意が必要となる。

7) 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

前述の予防的統制と発見的統制を容易かつ確実に行うために、これらの設定を組み込んだテンプレートを用いた IaC（インフラ環境の自動構築）が望ましい。

また、IaC コードでインフラを構築するため、インフラ構成が IaC コード通りとなっていることが保証され、IaC コードの内容で構成を適切に管理でき、セキュリティの維持にも役立つ。

8) 定量的計測とダッシュボードによる状況の可視化

セキュリティ対策の自動化を実施しても、管理者や関係者が速やかに状況を把握する必要性は変わらない。大規模システムや影響の大きいシステムについては、定量的計測とダッシュボードにより、可視化された情報が自動で提示されることが望ましい。

9) 継続的なアップデートへの対応

前述のセキュリティ対策の多くはクラウドが提供する機能に依存し、その機能は絶えずアップデートされている。利用システムにおいては、アップデート対応を義務的な改修負担としてイベント的に捉えるのではなく、通常のアップデートと捉えて日常的に対応を行い、適宜、設計の見直しも実施する必要がある。意図しない範囲まで情報が公開されるなど、特に機密性の低下を招かないよう注意する必要がある。

10)　クラウドに最適化した監査

単にオンプレミスの監査方法を踏襲するのではなく、1)～9)を前提とし、IaC、テンプレート、予防的統制・発見的統制等を活用し、サーバを構築しないアーキテクチャを前提としたクラウドならではの監査を行うことが可能となる。

３．７　公文書管理との関係への留意

クラウドで管理されている文書についても、公文書等の管理に関する法律（平成 21 年法律第 66 号）第２条第４項の要件を満たせば行政文書となり得る。クラウドの特性を踏まえ、遺漏なく法令等に基づいて公文書管理が行われるよう、システムの開発や運用に際しては、公文書管理に関する法令のほか「業務システムと公文書管理のルールについて」（令和４年２月 16 日内閣府大臣官房公文書管理課長通知）等に留意する必要がある。

4　補足

4.1　ISMAP 以外のクラウドセキュリティ認証等

クラウドサービスが ISMAP に登録されていない場合、暫定措置も含め各府省においてその対応を検討する必要がある。その際、クラウドサービスの情報セキュリティ機能の実態を利用者が個別に詳細に調査することは困難である。そのため、ISMAP 管理基準に基づくセキュリティ対策状況の確認に加え、第三者による認証や各クラウドサービスの提供している監査報告書を利用することが重要である。以下のいずれかの認証制度の認証を取得し、又は監査フレームワークに対応していることが推奨される。

1)　認証制度

(1) ISO/IEC 27017 による認証取得
https://isms.jp/isms-cls/lst/ind/index.html

(2) JASA クラウドセキュリティ推進協議会 CS ゴールドマーク
https://jcispa.jasa.jp/cs_mark_co/cs_mark_co/

(3) 米国　FedRAMP
https://marketplace.fedramp.gov/#/products?status=Compliant

2)　監査フレームワーク

AICPA SOC2（日本公認会計士協会 IT7 号）
AICPA SOC3（SysTrust/WebTrusts）（日本公認会計士協会 IT2 号）

別紙　附則

附則（令和4年9月 30 日デジタル社会推進会議幹事会決定）

1　施行期日

本方針は、決定の日から施行する。

附則（令和4年 12 月 XX 日デジタル社会推進会議幹事会改定）

1　施行期日

本方針は、改定の日から施行する。

別添

安全保障、公共の安全・秩序の維持といった機微な情報及び当該情報になり得る情報[2]をクラウドで扱う上での基準については、経済財政運営と改革の基本方針及びデジタル社会の実現に向けた重点計画（令和４年６月決定）で明記された方針[3]に沿って、セキュリティの観点から個別の措置を講ずる必要があること等を踏まえ、基本的かつ共通的な内容を「安全保障等の機微な情報等に係る政府情報システムの取扱い」として定めたため、当該文書を参照されたい。

---

[2] 行政文書の管理に関するガイドライン（内閣総理大臣決定。初版平成 23 年４月１日。）に掲げる秘密文書中秘文書に該当する情報及びそれに準ずる情報のこと。例えば以下の情報などが考えられるが、これらには経済安全保障に関連する重大な企業情報や先端的技術情報等も含み得るなど、我が国を取り巻く内外の情勢変化を十分に踏まえて解釈するものとする。
一　アクセスを認められた者以外の者が当該情報にアクセスすることにより、国の安全に損害を与えるおそれがある情報となり得るもの
二　アクセスを認められた者以外の者が当該情報にアクセスすることにより、他国若しくは国際機関との信頼関係が損なわれるおそれ又は他国若しくは国際機関との交渉上不利益を被るおそれがあると認められる情報のうち、特に慎重な取扱いが求められるもの
三　アクセスを認められた者以外の者が当該情報にアクセスすることにより、犯罪の予防、鎮圧又は捜査、公訴の維持、刑の執行その他の公共の安全と秩序の維持に支障を及ぼすおそれがあると認められる情報

[3] 「政府が扱う情報の機密性等に応じたクラウドの利用方針を年内に定め、必要なクラウドの技術開発等を支援し、クラウド等に係る政府調達に反映する。」（令和４年６月７日閣議決定経済財政運営と改革の基本方針 2022（抄））
「政府が取り扱う情報の機密性等に応じてパブリッククラウドとプライベートクラウドを組み合わせて利用する、いわゆるハイブリッドクラウドの利用を促進する。このため、特に厳格な取扱いが必要となる情報をクラウドサービスで扱う上での基準について、令和４年（2022 年）中に政府方針を定める。また、政府として、クラウドサービスや関連する暗号化等の技術開発や実証を支援しつつ、その成果を政府調達に反映していくなど、政府情報システムにおけるクラウド利用を、地方公共団体等のユーザーの理解と協力を得て、セキュリティを確保しつつ進める。」（令和４年６月７日閣議決定デジタル社会の実現に向けた重点計画（抄））