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

2026 年（令和８年）X 月 XX 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、クラウド第一原則、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第一原則（デフォルト）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
2026年X月XX日	1.1	・2026年XX月改定における背景の追加 ・時間経過に伴う表現の修正
	1.8	・「1.8 SeeS化によるメリット」を追加
	1.9	・「1.9 クラウド利用における生成AI活用によるメリット」を追加
	1.10	・「1.10 クラウド利用時の留意点」を追加
	2.1、他	・SaaSや生成AIに関する記述の追加
	3.1	・公共SaaSの追記
	3.2、他	・最新CRYPTREC「電子政府推奨暗号リスト」の反映
	3.4	・利用に問題のないマルチクラウドの明記
	3.5	・モダン化の説明の修正 ・利用中サービス終了時の対応の追記
	3.6	・「12 クラウド環境利用終了時のリソースの削除」を追加
	3.7	・海外CSP利用時の為替変動対策について追記
	3.9	・長期間に渡って改修を繰り返し、複雑化した現行システムへの対策を追記 ・画面や帳票の見直しについて追記
2025年５月27日	1.1	・2025年５月改定における背景の追加
	表1-1、他	・Rebuild、Replatformの説明の軽微な修正
	1.7	・「1.7 クラウド化による間接的なメリット」を追加
	3.2	・ガバメントクラウドとそれ以外の記述を統合
	3.5、他	・モダン化や定量的計測に関する文言の修正
	3.6	・セキュリティ対策に関する記述を最新化するために修正
	3.7	・「3.7 システム運用について」を追加
	3.9	・閉域網に関する記述の追加 ・開発規模のスリム化に関する記述の追加

		・「広域災害」を「リージョン全域にわたる大規模災害」に修正 ・「2 システム方式(全体アーキテクチャ)の考え方」を追加 ・「３ 刷新時のプロセス（システム計画工程）」を追加 ・「図3-1」、「図3-2」、「図3-3」、「図3-4」、「図3-5」を追加
2023年９月29日	表1-1、他	・ISMAP-LIUの追加
	3.8	・「3.8 システム刷新の進め方」を追加
	1章、３章	・「3.8 システム刷新の進め方」の追加に伴う文言の軽微な修正
	4.1	・「2) 監査フレームワーク」を廃止と置き換えに伴い修正
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
2022年９月30日	-	・初版決定（抜本改定）

目次

目次 i
1 はじめに 1
1．1 背景と目的 1
1．2 適用対象 1
1．3 位置付け 2
1．4 用語 2
1．5 クラウドサービスの当初からの利用メリット 5
1) 効率性の向上 5
2) セキュリティ水準の向上 5
3) 技術革新対応力の向上 5
4) 柔軟性の向上 6
5) 可用性の向上 6
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 6
1) マネージドサービスの活用によるコスト削減 6
2) サーバー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 7
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 7
1．7 クラウド化による間接的なメリット 8
1) クラウドで削減したコストでシステム化される領域の拡大へ 8
2) クラウドによる競争力の強化へ 8
1．8 SaaS 化によるメリット 8
1) SaaS 利用組織のメリット 8
2) SaaS 提供組織のメリット 9
3) 社会全体のメリット 9
1．9 クラウド利用における生成 AI 活用によるメリット 9
1．１０ クラウド利用時の留意点 9
1) ネットワーク環境 9
2) 旧来型の情報システムの維持が不可欠な場合 10
2 基本方針 11
2．1 クラウド第一原則（クラウド・バイ・デフォルト原則） 11
2．2 モダン技術の利用 11
3 具体方針 12
3．1 クラウドサービスの選択 12

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 13
３．３ ベンダーロックインについて 13
３．４ マルチクラウド等について 14
３．５ アプリケーションとシステム刷新について 14
1) 見積りの取得時の留意点 15
2) クラウド移行に向けた刷新 15
3) 小規模なシステムにおける刷新 17
4) 組織ごとに独立していたシステムの刷新 17
5) クラウド上で稼働するアプリケーションについて 17
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 .. 20
7) クラウド移行後のシステム刷新タイミング 20
３．６ セキュリティについて 21
1) 責任共有モデルによる対象の絞り込み 22
2) ベストプラクティスへの準拠 22
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） 22
4) 予防的統制と発見的統制の実施 23
5) サーバーを構築しないアーキテクチャの採用 23
6) 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構成管理 24
7) データ保護に関する暗号化技術の利用 25
8) 定量的計測とダッシュボードによる状況の可視化 25
9) 継続的なアップデートへの対応 25
10) インシデント対応と自動化 26
11) クラウドに最適化した自己点検・監査 26
12) クラウド環境利用終了時のリソースの削除 26
３．７ システム運用について 27
1) クラウド利用料を定期的に確認する 27
2) 稼働していないリソースへの課金を抑制する 27
3) ピーク時を想定した大きなリソースを通常時に使用しない 27
4) IaC によるインフラ作業の効率化..... 27
5) 運用作業の自動化を徹底する 28
6) 監視対象を見直す 28
7) 運用報告を見直す 28
8) 常駐運用からリモート運用へ 28

9）夜間バッチの必要性を見直す 29
10） マネージドサービスのアップデート時等における確認テストの最適化 29
11）運用作業を定期的に見直す 29
３．８ 公文書管理との関係への留意 29
３．９ システム刷新の進め方 31
1）システム刷新実施時の基本的な考え方 31
2）システム方式（全体アーキテクチャ）の考え方 37
3）刷新時のプロセス（システム計画工程） 38
4）刷新時のプロセス（要件定義工程） 40
5）刷新時のプロセス（設計開発・運用保守工程） 42
6）暫定対処時のプロセス（要件定義工程） 43
7）暫定対処時のプロセス（設計開発・運用保守工程） 44
４ 補足 45
４．１ ISMAP 以外のクラウドセキュリティ認証等 45
1）認証制度 45
2）監査フレームワーク 45
別紙　附則 46
１ 施行期日 46
１ 施行期日 46
１ 施行期日 46
１ 施行期日 46
別添 47

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、クラウド第一原則（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となってしまい、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たわけではなかった。

こうした状況を踏まえ、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、スマートにクラウドを利用（クラウドを賢く適切に利用）することで、政府情報システムのコスト削減とセキュリティレベルの向上に資するため、2022 年に旧方針の抜本的な改定を実施した。ここでの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)」の適用が、その中心となる。

2022 年の改定後もクラウドを取り巻く環境は更なる変遷を遂げている。本方針においても、モダン化の説明を詳細化し、運用のモダン化やモダン化のためのシステム刷新の方法について追記した。また、クラウドは、その黎明期においては単なる「新しいインフラ環境」にすぎなかったが、それが「インフラやソフトウェアを所有しない IT の形態」へと進化し、今日では「スピーディかつ合理的に業務を進めるための手段」と、より包括的に捉えるべき存在に変遷している。例えば、「個別交渉を要した取引価格から定価と定率割引で交渉不要に」、「長い時間を要したインフラ環境の納期がオンデマンドで即時に」、「当初からピーク時を想定するシステム構成からオートスケールで綿密な当初見積りが不要で無駄のない構成へ」、「自らが開発するのではなくマネージドサービスや SaaS を活用する」等、IT に関する業務のプロセス自体も合理化できる可能性が顕在化しており、これらも本方針に取り込んでいる。

2025 年度にはガバメントクラウドにおいて公共 SaaS が開始された。生成 AI も研究段階から実用段階に到達している。2026 年の改定においては、クラウド利用における生成 AI や SaaS の更なる活用を本方針に取り込んでいる。

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。

地方公共団体や独立行政法人等において、ガバメントクラウドの利用を検討する場合には、本方針も参考にされたい。

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のこと。
ISMAP	政府情報システムのためのセキュリティ評価制度の

用語	意味
(Information system Security Management and Assessment Program)	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。 登録が決定されたクラウドサービスについては、「ISMAP クラウドサービスリスト」に登録され、ISMAP ポータルサイトにおいて公開される。
ISMAP-LIU（ISMAP for Low-Impact Use)	ISMAP のうち、リスクの小さな業務・情報の処理に用いる SaaS サービスを対象とした仕組みのこと。 なお、本仕組みは、ISMAP とはクラウドサービスの評価・登録の仕組みが異なるため、「ISMAP-LIU クラウドサービスリスト」に登録され、ISMAP ポータルサイトにおいて公開される。
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、サーバー等）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。
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	サーバーやネットワーク等のインフラ構成をコード

用語	意味
（Infrastructure as Code）	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のこと。
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のこと。
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・管理するデータのこと。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	比較的新しい技術のこと。ただし、研究段階の技術ではなく、すでに広く使われている技術を指す。例えば、令和 6 年現在では、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による構成などが挙げられる。
モダンアプリケーション	モダン技術を活用して構築されたアプリケーションのこと。柔軟性、拡張性、保守性、セキュリティなどに優れている。
モダン化	既存のシステムを最新の技術や考え方を取り入れて、より良いシステムにすること。具体的には、以下のような作業が挙げられる。古いハードウェアやソフトウェアを新しいものにする。アプリケーションを作り直す。開発や運用の方法を新しいものにする。クラウドサービスのメリットを最大限に活かせるようにシステムを改良する。
API（Application Programming Interface）	異なるシステム間で情報をやり取りするための共通の仕組み。システム連携を容易にし、開発効率を高めることができる。
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のこと。

用語	意味
Rebuild（全面的な刷新）	クラウドへの移行方法の一つで、システムを作り直し、全面的にモダン化して移行すること。本方針では刷新を指す。
Replatform（基盤の変更）	クラウドへの移行方法の一つで、システムを部分的にクラウド上のマネージドサービス等に置き換えてモダン化し移行すること。本方針では Rebuild での移行前の暫定対処を指す。

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、資源を占有しないアーキテクチャを採用したならば、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、こうした機能を効果的に活用した場合には、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、組織内 SNS、モバイルデバイスや IoT、分析ツール、AI による不正検知・認識・予測等の自動化）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、改修確認に係る試験環境の構築や、災害発生時の利用、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／仮想サーバー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 日の稼働を要件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、仮想サーバーを構築し、ソフトウェアをインストールし、サーバーの運用管理を行うことが一般的であった。すなわち、仮想サーバーのクラウド利用料、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組み合わせることで多くの機能が実現可能であり、かつ保守・運用管理は CSP 側で行われることから、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。

自らがサーバー構築をしないため、サーバー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比例するため、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) サーバー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

自らがサーバーを構築し運用すると、そこへのセキュリティ対策として、サーバーへの侵入監視・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、自らの責任でそれらのセキュリティ対策を行うこと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 への登録等で安全性が評価されたクラウドサービスとして提供されており、利用システム側はサービス利用に集中でき、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側が自動で設定・最適化する度合いが高くなり、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。

この IaC には以下のコスト削減効果がある。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、管理チームによる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。

１．７　クラウド化による間接的なメリット

クラウドはその利用における直接的なメリットだけでなく、以下の間接的なメリットが存在する。

1)　クラウドで削減したコストでシステム化される領域の拡大へ

クラウドによってシステムの運用・保守費用が削減されると、これまで費用面で難しかった領域のシステム化が可能になる。今まで人手に頼っていた業務や、紙を介して行っていた業務も、デジタル化を通じて効率化することができる。

2)　クラウドによる競争力の強化へ

従来型のシステム運用・保守から事業者を解放し、クラウドを活用したモダン技術によるシステム刷新や構築を促進することで、事業者の競争力強化を支援していく。また、モダンなシステムの普及と拡大は、社会全体の IT による競争力向上に繋がる可能性がある。今日のクラウドは、単なるデータセンタやハードウェアビジネスではなく、最先端ソフトウェアを駆使したサービスとして進化を続けており、モダンなアプリケーション開発においては、アジャイル開発のような迅速かつ効率的な手法が注目されている。このような環境下では、開発者が自身の能力を最大限に発揮し、創造性を活かしたサービスを迅速に提供できるようになることが期待される。

１．８　SaaS 化によるメリット

従来のパッケージシステムは、SaaS などのクラウドサービスへと移行する流れが加速している。共通的な機能については、個別に開発したりパッケージ製品を導入するよりも、既存の SaaS を利用するか、SaaS や共通サービスとして開発して提供する選択肢を検討することが重要となるだろう。このように、SaaS や共通サービスの利用を積極的に検討することで、開発者と利用者の双方にとってより効率的なシステム構築が可能になると考えられる。

1)　SaaS 利用組織のメリット

SaaS 利用組織においては、SaaS を利用するのみとなれば、自らがシステムを開発・運用する負担から解放される。特定機能における部分的な利用であっても、開発量が削減されることへの期待値は小さくない。制度改正等に伴うシステムの改修も、従来システムであれば改修作業の調達行為が必要であったが、SaaS であれば調達行為を伴わずとも改正内容が継続的なアップデートの一環として、しかるべき手順を前提にシステムに反映されることが期待

される。

2)　SaaS 提供組織のメリット

SaaS を民間企業が公共市場において主体的に提供することは、それまでのリアクティブな受託ビジネスからプロアクティブな自主ビジネスへの転換の契機となりうる。技術においても、調達仕様を満たすだけの観点から、より良いサービスを自ら提供する観点への転換が促され、レベルアップが期待される。

3)　社会全体のメリット

利用組織毎に稼働環境を個別に構築せず共通化することで効率化によるコスト削減効果が期待できる。集約化にともなう標準化の推進、自主ビジネス化による技術レベルの向上、サービスの高度化等もコスト削減に加えて社会の進化に寄与することが期待される。

１．９　クラウド利用における生成 AI 活用によるメリット

生成 AI の活用領域は、これまでシステム化されていなかった領域だけではない。既にシステム化されている領域においても、生成 AI による代替が可能であれば、刷新コストの大幅な削減が期待される。書式や手順等のワークフローを予め定義する必要がなく、目的を達成することが可能である。また、生成 AI では代替が困難であり、システム開発が必要な領域においても、開発作業に生成 AI を用いることで大幅なコスト削減が可能となる。高コストが阻害要因となって刷新が困難だったシステムも、生成 AI による代替やシステム開発への生成 AI 活用を行うことで刷新が可能となる可能性が拡大される。

１．１０　クラウド利用時の留意点

クラウド利用においては、以下の点で留意が必要となる。また、これらの要素がクリティカルな場合においては、クラウドを避けることが現実的である。

1)　ネットワーク環境

クラウド利用にはネットワーク接続が必要である。ネットワークが利用できない環境や、システムの可用性要求をネットワーク環境がネックとなって満たせない場合はクラウドが不適となる。また、ネットワークによる遅延がエッジコンピューティング等の技術を用いても性能的に許容されないシステムも不適となる。

2)　旧来型の情報システムの維持が不可欠な場合

やむを得ない事情によって旧来型の情報システムの刷新ができず、旧来型の情報システムの維持が不可欠な場合。

２　基本方針

２．１　クラウド第一原則（クラウド・バイ・デフォルト原則）

政府情報システムは、クラウド第一原則、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、SaaS や生成 AI の活用でシステム開発を効率化した上で、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（公共 SaaS を含む）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 クラウドサービスリスト又は ISMAP-LIU クラウドサービスリスト（以下、「ISMAP 等クラウドサービスリスト」という。）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）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。SaaS 利用のみで全ての要件が満たせる場合だけでなく、開発する場合においても特定機能を SaaS に依存する形態が想定される。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。特に、アカウント数に対して課金される SaaS や高額な SaaS においては、利用アカウント数の増大で運用等経費が増大するため、利用アカウントの推移を想定する際、十分注意すること。

その際、ISMAP 等クラウドサービスリスト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）に基づき、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等」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、情報が取扱われる場所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。

政府情報システムが利用する場合、クラウドの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を海外に設置することが望ましい場合もある。その際は、準拠法や国際裁判管轄を確認し、具体的な争訟リスクが低いことを確認する必要がある。加えて、契約等において利用者データの保護が適切に担保されるようにする。

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、もしくは保管される可能性があ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 CRYPTREC「電子政府推奨暗号リスト」および「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」に基づいて暗号アルゴリズム・鍵長を選択し、システムのライフサイクルに応じたセキュリティ強度を確保すること。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（クラウドの鍵管理サービス提供の利用者が主体的に管理する鍵の利用や BYOK 等）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

一つの情報システムを複数のクラウドサービス（IaaS/PaaS）上で構成する「マルチクラウド」は、構成を複雑にして費用が増大する傾向にあることから合理的な理由がない限り避けるべきである。技術的にも経済的にも合理的なマルチクラウドは問題ない。また、組織として個々の情報システムが各々に異なるクラウドサービス（IaaS/PaaS）を利用することで、複数のクラウドサービス（IaaS/PaaS）を併用することも問題ない。

前述のように、個々の政府情報システムが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合理的な理由がない限り避けるべきだが、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。SaaS や生成 AI の活用でシステム開発を効率化することを前提とすること。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、自らサーバー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ー環境）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（サーバー更改）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ー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「5）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。

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、スケジュールの見直しを行い、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、事業者の体制、自己学習、トレーニング受講、資格取得等の状況を確認したうえで、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、サーバー構築のためのインスタンス（仮想サーバー）を利用する際には、その稼働を必要最小限とし、サーバー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)　小規模な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地方公共団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（モダン化）

2025 年現在のモダン化の定義としては以下の項目が主要な要素となる。

「API ベースのシステム構成」：システム間を疎結合して API ベースでデータ連携を行う（マイクロサービス化）。非同期処理とすること、API 定義の公開、API で扱うデータの管理責任の明確化、データ定義の明示、フロントエンド・バックエンドアーキテクチャ、バッチ処理のイベントドリブン化を含む

「ステートレスなアーキテクチャ」：ステートレスとは状態（ステート）を保持しない（レス）ことである。ステートレスにしないとコンテナやオートスケール等、クラウドにおける中核技術の十分な活用ができない。

「マネージドサービスの活用」：開発量の削減、運用負荷の軽減、セキュリティ対策の観点からマネージドサービスを適用する。対象としては監視機能、ログ管理機能、バックアップ機能、セキュリティ機能、データベース等が中心となる。データベースは RDB 以外のものも積極的に検討する。共有ストレージやファイルサーバもオブジェクトストレージ（マネージド

サービス）に置き換える。利用サービスは負荷に応じて自動的にサイズ変更ができるものや、その時点で適切なサイズを選択して負荷変化時にサイズの変更を行う。

「運用のコード化、自動化」：インフラ管理をコード化（IaC）し、定型的な作業を自動化する。コード化や自動化を前提に本番環境への作業者のアクセスを不要化（Zero Touch Production）し、手作業によるミスの発生を防ぐ。アップデート時においてもコード化や自動化を前提にリスクや業務影響の最小化を図るリリース方針を策定する。障害対応においても、自動化とリモート対応に取り組む。

「サービスレベルの定義、計測」：モダン化された環境では変更が容易なため、積極的に改善を継続することが好ましい。定義した KPI やサービスレベルについて内容を計測し継続的に振り返り、改善することが重要となる。

これらの項目を杓子定規に捉えるのではなく、生成 AI の活用等、より前向きな代替策があれば、積極的に検討されるべきである。

既存のアプリケーションを改修してモダン化するには大規模な改修が必要となる場合が多く、改修によるイニシャルコストを削減されるランニングコストで回収するには、一定の投資回収期間を要するが、回収後にはランニングコストの削減効果が顕在化する。特に新規開発や適切に実施される刷新時であれば、イニシャルコストとランニングコストの双方が削減される。

・オンプレミス環境の旧来技術・運用を単純に踏襲しない

クラウド環境では、オンプレミス環境で一般的であった技術や運用方法をそのまま踏襲すると、コスト増加やセキュリティリスクなどの問題が発生する可能性がある。旧来の技術や運用方法は、クラウド環境では適さない場合が多いため、クラウドの特徴を活かした新しい技術や運用方法のベストプラクティスに沿って見直し、システムを設計・開発する必要がある。例えば、クライアントサーバー方式などは、今日のクラウドへの移行を想定するべきではない。処理やデータをサーバー側に集中させ、クライアント側を軽量化するなど、クラウドの特徴を活かしたアーキテクチャを採用することが重要である。特に、セキュリティの要求水準が高いシステムでは、最新の技術や運用方法を採用することが重要である。旧来の技術や運用方法を継続して使用する場合には、それが将来的にシステム改修や運用を困難にする「技術的負債」となる可能性があることに留意する必要がある。

見直すべき技術・運用の例:

クライアントサーバー方式、シンクライアント専用端末（VDI 等)、踏み台サーバー、境界型セキュリティのみに依存したセキュリティ対策、非効率な監視ツール、定期保守のための予定断、不必要な夜間バッチ、SaaS やマネージドサービスで代替できるミドルウェア等

・人海戦術的な人手に頼った方式を踏襲せず自動化する

オンプレミス環境で一般的であった、人手に頼った作業方法は、クラウド環境では自動化する。インフラ環境の構築 （IaC)、CI/CD パイプライン、インフラのテスト、システム監視、運用、セキュリティ監視などを、クラウドの機能を活用して自動化する。

・システムの価値に直結する定量的計測を行う

従来のシステム監視では、サーバーやネットワークなどのインフラが停止しないことや、処理能力を超過させないことを主な目的として、インフラリソースの監視やログの監視が行われてきた。しかし、クラウド環境では、インフラの障害発生時に自動的に復旧する機能や、必要な処理能力を柔軟に調整できる機能が提供されているため、インフラを監視することの必要性は低くなる。クラウドサービスでは、システムの様々な状態を監視できる機能が標準で提供されており、これらの機能を組み合わせることで、従来のシステム監視よりも高度な監視を実現することができる。具体的には、システムが提供する業務レベルでの価値を明確に定義し、その価値を実現するために必要なシステムの状態を指標として設定する。そして、業務レベルでのサービス改善につながる運用につなげていく。

・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。

・開発プロセスはクラウド環境に合わせて最適化する

従来のオンプレミス環境では、インフラ環境をすぐに利用することができなかったり、一時的に利用する場合でもコストがかかったりするため、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。

クラウド環境では、インフラ環境を低コストで利用できるため、机上で

検討を重ねるよりも、実際にシステムを構築して検証を行う方が効率的な場合が多くある。設計についても、あらかじめ詳細な文書を作成するよりも、実際に動作するシステムを作成して検証を行う「プロトタイピング」を優先し、詳細設計の文書化は後回しにする方が効率的な場合が少なくない。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

従前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、クラウド環境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。

サーバー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。

利用中のサービスが終了する場合、事前に終了時期や代替機能と合わせて通知されるので、システムの継続的なアップデート・改善の一環として、早期に代替機能への変更を計画・実施することが望ましい。

7) クラウド移行後のシステム刷新タイミング

オンプレミス環境では、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、オンプレミスとクラウド（特に今日

[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）。

のクラウド）では、セキュリティ対策の具体的な考え方や技術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

従前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 等クラウドサービスリスト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 等クラウドサービスリスト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)　ベストプラクティスへの準拠

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ベストプラクティスとして用意されている。従前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ベストプラクティスに準拠した最新の対策を行う必要がある。また、ガバメントクラウドが用意するリファレンスアーキテクチャを活用することで、より具体的な実装も可能となる。

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

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 等クラウドサービスリスト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ー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。

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

予防的統制とは、潜在的なリスクを事前に予測し、不適切な設定や操作を未然に防ぐための対策を指す。例えば、担当する業務に必要な最小限の権限のみをユーザーに与え、必要以上の情報へのアクセスや誤操作を防ぐことは、予防的統制の一つである（最小権限の原則）。ただし、クラウドではサーバーやストレージなどの IT リソースの細かな操作をプログラムから API を介して呼び出せるように、権限もその操作の単位で割り当て可能なことが多く、サーバーの構築・運用だけで数百の操作や権限が定義されている場合もある。

クラウド環境では、システムの開発段階、運用環境の種類、業務の内容などに応じて、権限設定の厳密さを調整することが重要である。例えば、本番環境でシステムの障害の切り分けを行う際には、様々な操作を制限されたユーザーでは業務を遂行することが困難になる場合がある。このような場合は、業務効率を優先し、一時的に広範囲な権限をユーザーに与えることも考えられる。このような予防的統制への補完として求められるのが発見的統制である。

発見的統制とは、組織で定めたポリシーの準拠状況（暗号化やログ取得の実施状況、外部公開設定など）やリスクの発現につながる操作等を監視して検知し、必要に応じて修正する統制を指す。クラウドではポリシーへの準拠状況等を点検し、ログの監視が可能なマネージドサービスが提供されており、それを活用することが望ましい。前述の幅広な権限の割り当て時は、発見的統制の一環でログの点検で不要なサービスや操作へのアクセスの有無を検知することが望まれる。

5)　サーバーを構築しないアーキテクチャの採用

自らサーバーを構築し運用すると、そのサーバー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、サーバー構築が不要となると、サーバーのセキュリテ

ィ対策もサービス（サーバー）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。

サーバーを構築しないこと自体が利用システムの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、自らがサーバーを構築すると、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。

6） 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構成管理

セキュリティ対策を効率的かつ確実に実施するために、予防的統制と発見的統制の設定を組み込んだテンプレートと IaC（インフラストラクチャ・アズ・コード）の活用が重要となる。IaC とは、サーバーやネットワークなどのインフラ環境の構築を、コードを用いて自動化するという手法である。あらかじめセキュリティ対策の設定を組み込んだテンプレートを利用することで、人為的なミスを減らし、セキュリティレベルを向上させることができる。

IaC を活用することで、検証環境や本番環境など、用途に応じた複数のクラウド環境を容易に構築・管理できる。また、IaC によってインフラ環境の構築プロセスを自動化することで、人為的なミスを減らし、効率的かつ低コストでインフラ環境を構築・運用することが可能になる。例えば、従来のオンプレミス環境では、ログの取得状況を一つずつ確認し、場合によっては、担当者が手作業でログを取得する設定を行ったり、人手では全てのログを検査できないため、一部のログを抽出して検査したりしていた。しかし、クラウド環境では、提供されている機能を利用することで、全てのログを保管し、設定したルールに基づいて自動的に分析することが可能になる。これにより、人為的なミスによるログの見落としや分析の遅れなどを防ぎ、セキュリティ運用コストの削減も期待できる。

また、IaC ではコードによってインフラ環境を構築するため、構築されたインフラ環境がコードの内容と一致していることが保証される。そのため、コードの内容を適切に管理することで、インフラ環境のセキュリティを維持することができる。

7)　データ保護に関する暗号化技術の利用

クラウド環境では、データを暗号化する機能を提供するサービスが充実しており、オンプレミス環境よりも容易かつ安全に暗号化技術を利用することができる。データの機密性や想定される脅威に応じて、通信中のデータや保管されているデータを暗号化することを検討する必要がある。暗号化を行う際には、最新の CRYPTREC「電子政府推奨暗号リスト」および「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」に基づいて暗号アルゴリズム・鍵長を選択し、システムのライフサイクルに応じたセキュリティ強度を確保するとともに、適切な方法で暗号鍵を管理する必要がある。なお、「電子政府推奨暗号リスト」 に掲載されている暗号の利用に関しては、 一定のセキュリティ強度の暗号について、 2030 年までに、よりセキュリティ強度の高い暗号又は鍵長への移行の完遂が前提とされていることに留意すること。具体例として 112 ビットセキュリティ強度を持つ暗号アルゴリズムである 2048 ビットの RSA 暗号や 224 ビットの楕円曲線暗号が該当する。クラウドでは暗号鍵管理をクラウドの利用者が自ら実施できることを考慮し、取り扱うデータに求められるセキュリティ要件に基づいて運用方式と実装を検討する。例えば、クラウドの暗号鍵管理サービスの提供する利用者が主体的に管理可能な暗号鍵では、アクセス権の設定を含む鍵のライフサイクルを管理する。「BYOK(Bring Your Own Key)」と呼ばれる方式では、利用者自身が作成した暗号鍵をクラウド環境に持ち込み、クラウドサービス事業者が提供する鍵管理サービスを利用して、その暗号鍵を管理し暗号化処理を行う。また、HYOK(Hold Your Own Key)と呼ばれる方式では、利用者が保有する鍵管理システム上で保管・管理されている暗号鍵をクラウドサービス事業者のサービスから利用して暗号化処理を行う。いずれの場合も、利用者自身がクラウド以外で暗号鍵を作成・保管・管理する場合は、サービスに組み込まれた標準的な方法を利用する場合と比べて運用負荷や処理の複雑さが大幅に増すため、導入前に十分な検討が必要となる。

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。大規模な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)　インシデント対応と自動化

インシデント対応のプロセスを定義し、適切な訓練を実施することは、オンプレミス環境だけでなく、クラウド環境においても重要である。クラウド環境では、どのような種類のインシデントが発生する可能性があり、その影響範囲はどの程度なのか、誰がどのような対応を行うべきなのかを、事前に明確に定義しておく必要がある。発生が予想されるインシデントについては、具体的な対応手順をまとめた「プレイブック」を作成し、訓練を実施することで、迅速かつ適切な対応が可能になる。また、クラウド環境では、インシデント発生時の調査に必要な環境を自動的に構築する機能が提供されている場合があり、このような機能を活用することで、インシデント対応の迅速化・効率化を図ることができる。

11)クラウドに最適化した自己点検・監査

クラウド環境において利用システムが自己点検を行う、または監査を受ける場合、前述の「責任共有モデル」を考慮した対応が考えられる。利用システム自身が構築している範囲は従来通りの自己点検や監査対応が必要だが、クラウドサービス事業者が提供するマネージドサービスなどを利用している範囲はCSPが受けている独立した第三者の監査法人による監査内容の確認を自己点検とすることや確認結果等を監査者に示すことで対応の効率化を検討できる。なお、利用システム自身の構築範囲においては、クラウドサービス事業者が提供するセキュリティ監視機能などを活用することで、セキュリティ設定の適用状況を迅速に把握することが可能な場合もある。

12)クラウド環境利用終了時のリソースの削除

クラウド環境の利用を終える際はクラウド環境上に保管したすべてのデータを適切に削除する。データを暗号化し、削除と同様の実質的な効果を得られる手法として、暗号鍵の破棄を行うことで復元不能な状態とする（暗号化消去と呼ばれる）。なお、取り扱うデータに係る法令または規制の要件に応じ、データの保全が必要な場合にはバックアップまたは他システムへの移行を行う。これらの操作については証跡を適切に保管し、必要に応じて監査可能な

状態にすること。
　また、予期せぬデータアクセスを防ぐため、クラウド環境へアクセスするユーザーを削除するとともに、クラウド事業者が提供する各サービスの利用を停止するほか、サーバーやデータベースなどのリソースを削除する。なお、クラウドサービスを一定期間の契約のもと利用している場合は、利用終了後の料金発生の有無を確認するとともに、解約等の必要な対応を行うこと。

３．７　システム運用について

　システムをモダン化して刷新しても、システム運用が従前のままではコスト削減効果は十分に発現しない。クラウドを利用する政府情報システムについては、以下を踏まえたシステム運用を行い、運用に係る費用の削減を行うことを原則とする。

1)　クラウド利用料を定期的に確認する

　クラウドサービスの利用料金は、実際に利用した分だけ課金される仕組みになっている。無駄なコストが発生していないか、利用料金を定期的に確認するようにする必要がある。

2)　稼働していないリソースへの課金を抑制する

　クラウドサービスでは、サーバーなどのリソースが稼働している間は、常に料金が発生する。そのため、休日や夜間など、システムを利用しない時間帯には、サーバーを停止するなどして、稼働していないリソースへの課金を抑制する必要がある。クラウドサービス事業者が提供する自動起動・停止機能などを活用することで、効率的に課金を抑制することができる。

3)　ピーク時を想定した大きなリソースを通常時に使用しない

　クラウドサービスでは、アクセスが集中するピーク時に備えて、あらかじめ大きなリソースを確保しておく必要はない。アクセス状況に応じて自動的にリソースを調整する「オートスケール」機能を活用することで、必要な時に必要な量のリソースだけを利用することができる。オートスケール機能を利用できない場合は、運用コストが過大とならない範囲で、手動でリソースの調整を行う必要がある。

4)　IaC によるインフラ作業の効率化

　IaC を活用することで、インフラ環境の変更や、類似した環境の構築を、コ

ードの修正と実行だけで行うことができるため、従来のように手作業で設定を行う必要がなくなる。また、人為的なミスを減らし、検証作業にかかる時間も短縮できるため、開発期間の短縮やコスト削減に繋がる。さらに、検証用の環境を容易に構築できるため、テストを効率的に実施することも可能になる。

5)　運用作業の自動化を徹底する

クラウドサービスでは、バックアップ、システムの状態監視、アラート発生時の初期対応など多くの運用作業を、CSP が提供するマネージドサービスや自動化ツールなどを活用することで自動化することができる。人手に頼っていた運用作業を自動化し、運用コストの削減とヒューマンエラーの防止を図る必要があるため、自動で実行可能な単純作業を事業者が人件費を用いて実施しないよう、特に留意が必要となる。

6)　監視対象を見直す

従来のオンプレミス環境では、サーバーやネットワークなどのインフラの状態を監視することが重要視されていたが、クラウド環境では、インフラの監視よりも、アプリケーションやサービスが正常に動作しているかを監視することが重要になる。CSP が提供する監視ツールなどを活用して、システムの稼働状況やパフォーマンスなどを監視し、サービスの品質維持や業務レベルでの価値向上に努める必要がある。

7)　運用報告を見直す

従来のオンプレミス環境では、月次で運用報告書を作成し、前月のリソース使用状況や運用作業の内容などを報告することが一般的であった。しかし、クラウド環境では、システムの稼働状況やパフォーマンスなどをリアルタイムに確認できるダッシュボードが提供されているため、月次報告書を作成する必要性は低くなる。ダッシュボードで確認した内容を基に、迅速に問題点の解決やサービス改善に取り組む必要がある。また、運用に関する記録の保管は必要最小限のコストで対応し、システムの価値に直結する定量的計測の結果と評価についても併せて実施すること。

8)　常駐運用からリモート運用へ

クラウドでは、発注者拠点での常駐運用にオンプレミス時のような必要性はない。システムの運用管理を遠隔地から行うリモート運用を原則とすべきである。常駐体制よりもリモートでの速やかな対応や報告等を優先させるべ

きである。

9)　夜間バッチの必要性を見直す

クラウド環境では、リソースを柔軟に増減できるため、従来のように夜間バッチ処理を行う必然性は低くなる。特に、業務時間外に処理を実行する必要がない場合は、ピーク時の負荷軽減やシステムメンテナンスとの連携を考慮する必要もなく、業務によるデータ更新が発生しない時間帯に逐次処理を行うことで、より効率的な運用が可能となる。処理の要件として直列性が要求される場合、法令に基づいて基準日の決められている事務や、大量のデータを一括処理する必要がある場合においても、可能な限り日中の処理を計画し、夜間オペレータや夜間の自動処理に必要な複雑なジョブネットの最小化を図るべきである。

10)　マネージドサービスのアップデート時等における確認テストの最適化

CSP が提供するマネージドサービスは、定期的にアップデートが行われる。アップデートによってシステムに何らかの影響が出ないかを確認するテストは、影響が出る可能性が高い場合には必要だが、可能性が低い場合には事前に大規模なテストを行うよりも、アップデート後に問題が発生した場合に迅速に対応できる体制を整えておくことが有効である。いずれにしても、テストの自動化、テストコードの整備を開発時に行っておくことが望まれる。また、アップデートによって問題が発生しやすい特殊な実装は、当初から避けることが望ましい。

11)　運用作業を定期的に見直す

システムの運用作業は、定期的に見直し、効率化を図ることが重要である。運用作業にかかっている時間や労力を分析して自動化すべき部分がないか検討し、手作業を継続的に削減していく必要がある。

なお、海外の CSP を利用する場合には支払いにおいて為替変動の影響を受けるが、ガバメントクラウドに選定されているクラウドにおいては、一部の CSP によって、為替変動の影響を受けない費用請求モデル（為替固定プログラム）の選択が可能となっている。社会情勢や為替変動の動向を踏まえ、有利な費用請求モデルの選択を検討すること。

３．８　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。

３．９　システム刷新の進め方

クラウドへの移行時におけるシステム刷新の進め方を以下に示す。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)　システム刷新実施時の基本的な考え方

モダン化の実現には意識変革が必要である。旧来技術の温存はモダン化を大きく阻害する。SaaS や生成 AI の活用でシステム開発を効率化することを前提に、以下の考え方に留意すること。

・モダン化では技術の最新化と変化を追求すること

モダン化においては、最新の技術を積極的に取り入れ変化を意図的に促すことが基本となる。まず、職員がこの意識を持つことが重要となるが、事業者についてもモダン技術に明るく変化に積極的な事業者を選定することが重要である。

・インターネットへのセキュアな接続を前提とすること

従来のオンプレミス環境では、システムを外部ネットワークから隔離した閉域網で運用することが一般的であった。これは、管理されていないコンピュータがシステムに接続された場合に、セキュリティ上のリスクが高まることを防ぐためである。適切にクラウドを利用するシステムでは、システムやデータをセキュアなクラウド環境内に配置するため、データのコンピュータからコンピュータへのリレーが発生しない。クラウド内やクラウド間の通信は全て暗号化が基本であり、API 連携も認証と暗号化が前提となる。クラウドと利用端末間も認証と暗号化が行われる。クラウド自身については CSP の責任で不正アクセス等から守られている。よって、クラウドに処理を集約させること自体が安全対策となる。

また、セキュリティ対策の考え方も、従来の「境界型セキュリティ」から「ゼロトラスト」へと変化している。境界型セキュリティは、外部からの攻撃を防ぐことに重点を置いていたが、内部からの攻撃には脆弱であった。一方、ゼロトラストは「すべてのアクセスを信頼せず、常に検証を行う」という考え方であり、より強固なセキュリティ対策を実現できる。さらに、最新のセキュリティ対策を実施するためには、インターネット接続が不可欠になっている。

よって、クラウド利用については、インターネットへのセキュアな接続を前提とすること。旧来型の業務システムではアプリケーションや各機器で十分なセキュリティ対策をとっていなかったので境界型セキュリティによる防御（閉域網に閉じた運用）を必要としたが、今日の業務システムにおいては、適切なセキュリティ対策がとられていない業務システムのみがセキュリティ対策として閉域網に閉じた運用を必要としていると考えるべきである。

閉域網に閉じた運用は、システムの外部連携や SaaS 利用を大きく阻害し、外字に対応した閉域網内では文字化けが顕在化しないことから外字を多用するシステムや高コストな旧来型システムの温存を助長する。インターネットへのセキュアな接続を前提とすることはコスト削減の観点でも重要となる。

・二段階移行は可能な限り避けること

システム刷新（クラウドへの移行）については、１回での移行（刷新：Rebuild)、全面的なモダン化を原則とすること。対象システムのシステムライフサイクルを前提に、様々な環境を踏まえ、適切な時期での刷新を検討すること。

二段階移行については、２回の移行作業によってトータルコストが増大するおそれがあることから、刷新については、システムの規模や移行の難易度等を踏まえ、各システムのライフサイクルの適切なタイミングで実施することを前提としつつ、可能な限り１回での刷新を目指すこと。

また、本方針で記載するシステム刷新は原則として１回での刷新を指す。二段階移行における第一段階（暫定対処：Replatform）の場合は二段階目の移行を計画した上で「3.5 アプリケーションとシステム刷新について」を踏まえ可能な範囲での対応、部分的なモダン化とし、計画に従って二段階目（刷新）を実施すること。

・大規模なシステム等、難易度の高いシステムについては一括刷新を避けること

システム刷新については、可能な限り一括での刷新を検討するべきだが、大規模なシステム等、難易度の高いシステムについては、リスクの分散化と予算の平準化を目的に、刷新する単位（サブシステム等）を分割し、優先度を十分に検討した上で、順次、刷新を行い、一括刷新を避けること。

なお、大規模なシステム等をサブシステム単位等に分割して順次、刷新する場合についても、各々の刷新は１回での実施とし、二段階移行は避け

ること。

・現行システムの機能や実装の単純継続を前提とせず、データ移行のある新規システムとして考えること

刷新においては、現行システムの機能や実装の単純継続を前提とした移行は行わない。そもそも現行システムを前提とすることは、後述の業務観点の見直しとシステム観点の見直しを行わないことになる。

現行システムからは、基本的に現行システムの仕様と現行データのみを抽出するだけとする。抽出された現行仕様については業務の見直しを行って新仕様を策定する際の参考情報にとどめ、単純な流用は行わない。現行データについても、必要なもののみに限定してデータ移行を行うものとする。現行システムのソースコード流用を前提とした移行は刷新の大きな妨げになるため厳に避けること。

特に現行システムが旧来のクライアントサーバー方式や Web 三層モデルを採用して多数の画面や、多くの帳票、大量のバッチ処理等によって大規模化（以下「肥大化」という。）している場合については、肥大化した現行システムの規模を前提に刷新の見積りを取得すると非常に高額な見積りとなり刷新計画自体が頓挫してしまう。

よって、肥大化した現行システムではなく業務観点の見直しとシステム観点の見直し後の新仕様を前提にデータ移行のある新規システムとして見積もりを取得すること。

業務観点の見直しとシステム観点の見直し（後述）を行った上で刷新を行うことができれば、現行システムと比較し刷新後のランニングコスト（運用等経費）の減少を見込むことができ、刷新に要したコスト（整備経費）の回収期間について適切な評価が可能になる。

また、この方法は長期間に渡って改修を繰り返し、複雑化した現行システムの刷新についても有効となる。過度に複雑化したシステムについては、現行システムをベースに大規模改修するのではなく、データ移行のある新規システムとして考えることが現実的である。

・開発規模のスリム化を徹底すること

現行システムは肥大化していることが多く、刷新時には現行システムの規模を決して前提とせず、スリム化されたシステムを新規開発することを前提に見積りを取得し、要件定義等を実施すること。スリム化の観点としては以下が想定される。

- 画面の削減（真に使いやすいGUIをフロントエンド・バックエンド分離

型 Web システムで実装）

- 帳票の削減（法定帳票以外の内部帳票は原則不要）
- バッチの削減
- 不要な例外処理の削減
- フルスクラッチ開発の削減（SaaS とマネージドサービスの活用）
- 特に非機能要件（大量処理、高信頼、セキュリティ）への対応はフルスクラッチ開発ではなくインフラ（マネージドサービス）で対応する

・業務観点の見直しとシステム観点の見直しの双方を実現すること

刷新においては、業務とシステムの双方の観点から見直しを行うこと。

「業務観点の見直し」

- サービスデザイン思考を採用し、法律等のルールを単純に実装するのではなく利用者視点でサービスを見直し、制度（法令、省令、内規、通知等）の変更も視野に入れて検討する
- 業務の高度化やサービス向上を合理的に実現する
- 業務処理から無駄や不合理を省く（システムの計算結果を電卓で確認する等の無用のチェック、過度の複数チェック、紙出力による確認や押印等）
- 外部システムと必要なデータを連携させ、デジタル第一原則（デジタルファースト）によって個々の手続・サービスが一貫してデジタルで完結させる
- 届出一度きり原則（ワンスオンリー）として、一度提出した情報は、二度提出することを不要とする

「システム観点の見直し」

- 旧来技術からの脱却（旧来型のセキュリティ対策、多階層の大規模な画面構成、クライアントサーバー方式、Web 三層モデル、シンクライアント（VDI 等）、法定帳票以外の多数の帳票、夜間バッチ、紙での月次運用報告等、人海戦術的な運用作業等の排除）
- システムやアプリケーションのモダン化
- アジャイルと CI/CD を原則とする開発・運用方式のモダン化

システム観点の見直しにおいては、先ず、旧来型の時代の技術と今日の技術の相違を意識されたい。当時のディスプレイは小さく、解像度も低く、高価であったため、画面は小さく、情報量も少なかった。よって、データ

の確認には帳票出力が現実解であり、データや観点毎に大量の帳票が設計された。しかし、今日ではディスプレイは大きく高解像度で安価である。また、情報を汎用的に画面出力可能な手段も確立されている。よって、画面での確認が現実解である。その環境下で旧来の帳票を単純に移行するのは合理的ではない。同様に当時の技術的制約下で設計された画面やバッチについても、今日の技術を前提に見直しを行わないと不合理となる。当時は他に選択肢がなくバッチが選択されてきた処理についても、今日ではより合理的な選択肢が用意されている。

次に、クライアントサーバー方式から脱却することが特に重要となる。クライアントサーバー方式の場合、画面生成に埋め込んでいた同じコードの繰り返しで規模が肥大化するだけでなく、クラウド技術にも馴染まないためモダン化の阻害要因になってしまう。更には、クライアント側に保管される業務データをセキュアに管理するため、シンクライアント（VDI 等）導入の要因にもなりやすい。

画面については「フロントエンド・バックエンド分離型 Web システム」の採用を検討されたい。分離型にすると以下のメリットが期待される。

- これまで画面生成に埋め込んでいた同じコードの繰り返し再利用による無駄（開発規模の肥大化）を解消でき、開発コストを削減できる
- 利用者体験（ユーザエクスペリエンス）を踏まえた全体アーキテクチャ検討の後に、UX 設計をワイヤーフレーム（画面レイアウト）まで具体化したフロントエンドを作成することで、真に使いやすいシステムにできる。使いやすいシステムは多階層の大規模な画面構成とならないため、開発規模の適正化（開発コスト削減）にも寄与する
- フロントエンドとバックエンドを API によって独立させ、疎結合にすることで変更に強いアーキテクチャとなる。画面表示の修正はフロントエンドのみの修正、業務処理の修正はバックエンドのみの修正となり、将来の改修時の改修対象が限定、極小化され、保守費用が削減される
- 分離型にすると、バックエンドではインタフェースが API のみとなるのでアーキテクチャがシンプルになり、画面処理もなくなるのでセッション情報の維持なども減る。また、これまでサーバー側で処理していたレンダリング（画面生成）をクライアント側で行うので、サーバー（クラウド）側に必要なコンピュートリソースも少なくなってコスト削減につながる
- 更には、クライアントとサーバー（クラウド）間の通信も最小化され処理の高速化、ネットワーク負荷の軽減にも寄与する

・システムのスコープ（対象、範囲）と制度の見直しを行うこと

刷新においては、１システム単独では実現できない、より広いスコープでの検討が必要となる場合がある。よってシステムを広範に見直すタイミングにおいて、より広いスコープでの見直し、統合の検討を行うこと。統廃合されるシステムはその旨を将来の計画としてプロジェクト計画書に記すこと。

- 組織ごとに独立して実装していたシステムの統合
- 上流業務や下流業務との統合
- 類似業務、関係性の深い業務の統合
- 追加開発された機能が別システム化しているものの統合等

また、統合や業務観点での見直しに際して必要となる制度（法令、省令、内規、通知等）の変更、関連組織等との調整については、情報システム部門だけでなく、制度所管部門・業務実施部門が主体的に、広く関係者と連携して実施すること。

・クラウドに適した災害対策を行うこと

クラウド利用システムにおける災害対策は、オンプレミスとは異なり、データコピーの容易性、環境構築の俊敏性、リソースの柔軟性等、クラウドの特徴を活用し検討することに加え、災害対策のために利用する各リージョンで利用できるサービスに不足がないことを確認しながら設計することが必要となる。また、システムアーキテクチャ、システム構成及びコストに大きな影響を与えるため、関東圏全域といったリージョン全域にわたる大規模災害への対策を必要とするか否かも重要な要素となる。以下の選択肢を基本として、各々のシステム特性・ニーズをもとに検討する必要がある。

(1) リージョン全域にわたる大規模災害ではなく部分災害への対策に限定し、費用対効果が高く冗長性を担保したマルチゾーンパターン（シングルリージョン構成）

(2) リージョン全域にわたる大規模災害を想定し、データをクラウドの機能で遠隔保管することで費用対効果の高いバックアップパターン（シングルリージョン構成＋リージョン外へのデータ保管）

(3) コストはかかるものの災害対策用リージョンでは最小限の構成を保持しておき、リージョン全域にわたる大規模災害時には災害対策用リージョンで稼働を続けるウォームスタンバイパターン（マルチリージョン構

成）

(4)リージョン全域にわたる大規模災害時にコストをかけてでもサービスを変わらず継続する必要のあるアクティブ-アクティブパターン（マルチリージョン構成）

職員向けシステムや、一部の国民向けサービスは、基本的にパターン(1)か(2)になり、広く国民向けサービスのうち、停止すると国民生活に影響のあるもののみ(3)か(4)が想定されるが、各々の業務継続計画（BCP）に沿って目的に即した災害対策を選択するものとする。なお災害対策を目的としたマルチクラウド（複数の CSP による冗長化）は、費用対効果が特に悪いため、選択しないことを原則とする。

災害時の運用体制についても、自動化、IaC、リモート操作を前提に各々の業務継続計画（BCP）に沿って計画しておくこと。

・ライフサイクルコストを削減する観点から評価方法を工夫すること

刷新にかかるコストを削減するためには、前述の各項目に加えて更なる注意が必要となる。

SaaS 利用は開発量の削減となるため強く推奨されるが、無条件に推奨されるわけではない。利用者数の段階的な増加が見込まれる場合等、運用段階で SaaS 利用料が高額となるケースもあるため、ライフサイクルコストの観点から真にコスト削減効果が発現するかを慎重に評価する必要がある。例えば、SaaS と同様の機能を他のマネージドサービスで実現することが可能であれば、ライフサイクルコストの観点から両方式を比較して十分に評価すべきである。

調達において、応札価格はその調達の対象、範囲に限定されたものであり、ライフサイクルコストの一部でしかない。事業者は応札価格を下げるために、応札価格に反映されない部分が高額となる提案を行う場合も想定される。そのため、総合評価落札方式の中でライフサイクルコストを低減させる提案を技術点として評価する等、評価方法を工夫することを推奨する。

2) システム方式（全体アーキテクチャ）の考え方

業務システムの実現方式、全体アーキテクチャについても、旧来方式の単純な継承はモダン化を大きく阻害する。以下の点を考慮して、システムの全体アーキテクチャを設計する必要がある。

・データ処理をクラウド内で完結させる

データ処理はクラウド内で行う原則として、端末やオンプレミス環境にデータを保存しない。ただし、処理速度の向上や災害対策などのために、一時的にデータをキャッシュしたり、バックアップデータを保管したりする場合は、セキュリティ対策を適切に実施する必要がある。

・紙文書の単純な電子化は行わない

紙文書を画像として電子化するのではなく、データとして活用できるように加工する。データ入力は原則としてシステム上で行い、データベースに保存する。申請や審査などのワークフローもシステム上で処理する。申請書や交付書類などの証拠となる文書は、必要に応じて検証可能な形式で生成する。

・作らないアプローチを徹底させる

SaaS とマネージドサービスを徹底し、開発量の削減や開発への生成 AI の活用を図る。SaaS 化されていないパッケージ利用は将来のサポート終了や提供終了に備えること。

・共通的に利用される機能の SaaS 化や共通サービス化を積極的に行う

共通システム、共通業務、共通機能等については、積極的に SaaS 化や共通サービス化を行う。また、各システムはこれらの SaaS や共通サービスを利用して開発量を削減させる。

・ウォーターフォールからアジャイルに発想を切り換える

机上での遠大な計画から、実践と測定された事実に基づく継続的な改善にアプローチを変更する。ピークに備えた大きなリソースを通常時に遊ばせておくことはクラウドではコストの無駄遣いとなる。

3) 刷新時のプロセス（システム計画工程）

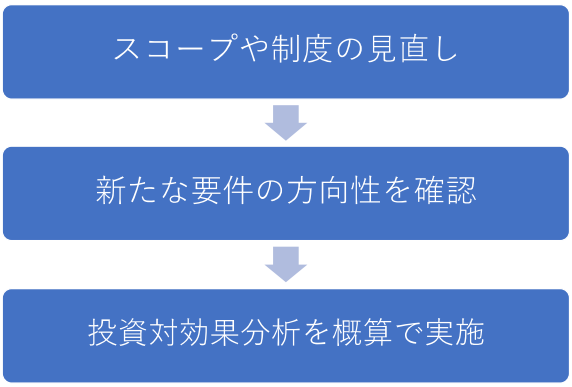

図 3-1　刷新時のプロセス（システム計画工程）

・スコープや制度の見直し

スコープや制度の見直しには時間がかかるため、システム計画工程内ですべてを完了できない場合もあるが、この工程から見直しに着手することが重要である。

・新たな要件の方向性を確認

「業務観点の見直し」と「システム観点の見直し」を方向性の確認レベルで実施する。「業務観点での見直し」では、スコープや制度の見直しを前提に、基本的な業務フローの作成までを行う。例外処理等の細部への踏み込みは、本工程では避けるべきである。「システム観点の見直し」では、全体アーキテクチャ、システム構成の作成までをガバメントクラウドが用意するリファレンスアーキテクチャを参照して実施する。現行システムの技術的な分析は行わない。

大規模なシステム等、難易度の高いシステムについては一括刷新を避けるために、サブシステム（サービス）単位での分割と刷新の単位・優先度（順序）の検討を行う。一括刷新であっても、この段階で、システムを疎結合な複数の（サブ）システムに分割することが、これ以降のシステム開発や運用費用削減に資するため、これを試みる。また、システム分割したうえで、一部のシステムについては外部の他システムと統合できるとより効率がよいため、これも検討する。

・投資対効果分析を概算で実施

新たな要件の方向性をベースに、投資対効果分析を行う。現行システムをベースとした費用見積りは行わない。新たな要件の方向性を前提にデータ移行のある新規システムとして見積りを取得すること。システムのスリム化とモダン化でアプリケーション開発コスト（整備経費）を抑制し、運

用方式のモダン化、自動化の徹底等でランニングコスト（運用経費）についても抑制すること。

また現行システムと新システムでスコープが異なる場合は、適正な評価となるよう、可能な限りスコープを一致させること。スコープの一致が難しい場合は、スコープの相違を考慮した評価を行うこと。

4) 刷新時のプロセス（要件定義工程）

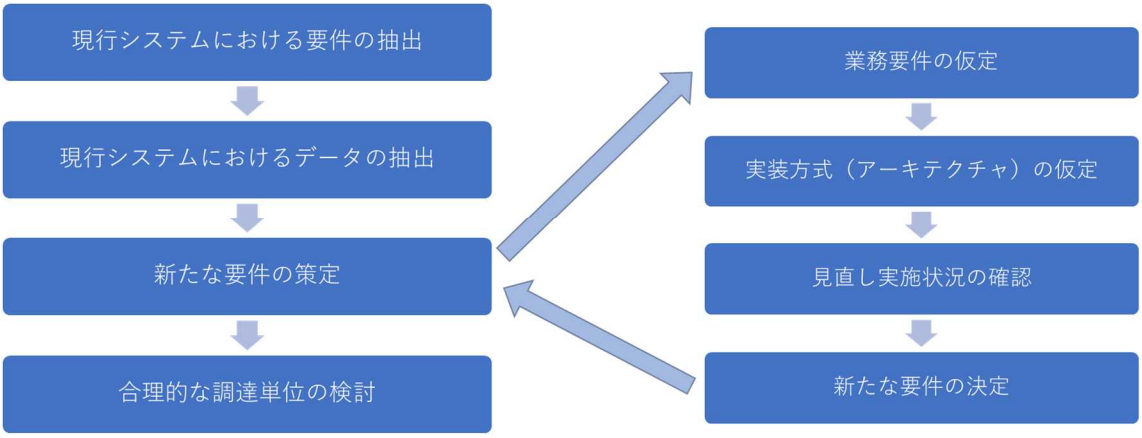

図 3-2　刷新時のプロセス（要件定義工程）

・現行システムにおける要件の抽出

設計書等を中心に現行システムの業務要件を抽出する。業務観点で「やらなければいけないこと」「制度からの要求」「継続が必要なもの」を抽出する。統合等でシステムのスコープが拡大される場合は、全体を俯瞰して実施すること。

・現行システムにおけるデータの抽出

設計書や実際のデータベース等を確認して、データ移行されるべきデータの把握を行う。

・新たな要件の策定

以下の詳細プロセスで実施する。

- 業務要件の仮定：

  「業務観点の見直し」を行うにあたって、「やらなければいけないこと」を再確認し、「制度からの要求」についても必要であれば見直し、「継続が必要なもの」と不要なもの、改善されるべきものを分類し、

新システムで実現されるべき新たな要件を仮定する。

- 実装方式（アーキテクチャ）の仮定：
  「システム観点の見直し」を前提にアーキテクチャを新たに検討する。ガバメントクラウドが用意するリファレンスアーキテクチャ等を活用すること。また、UX を担うフロントエンドと業務処理を担うバックエンドを独立的に検討すること。
- 見直しの実現状況の確認：
  「業務観点の見直し」と「システム観点の見直し」の実現状況を確認する。
- 新たな要件の決定：
  上記の詳細プロセスを反復的に実施し総合的に調整して新たな要件とする。

また、「新たな要件の策定」の実施時には以下に留意すること。

- マイクロサービス適用の検討：
  マイクロサービスの適用が合理的か否かを検討する。大規模なシステムについては、サービスの観点から調達を分割することで調達規模の適正化を検討する。
- リファレンスアーキテクチャ適用の検討：
  システムの特性に応じてガバメントクラウドが用意するリファレンスアーキテクチャの採用を検討する。全面適用しない場合についても、部分適用、エッセンスの活用も含めて検討する。
- 旧来技術の適用を厳に避ける：
  閉域網での利用ではなくインターネットでの利用（境界型セキュリティからゼロトラストへ）を原則とする。クライアントサーバー方式は採用せずフロントエンド・バックエンド分離型 Web システムを基本とする。シンクライアント(VDI 等)、DaaS(Desktop as a Service)等も避ける。
- 開発規模の適正化：
  開発量を削減するためSaaSや他のマネージドサービスの活用を検討する。業務観点の見直しによって法定帳票以外の帳票は極力削減し、帳票印刷処理もBI機能等での代替を原則とする。バッチ処理は設計レベルで見直して、合理性や経済性の観点から必要性が明らかなもののみとする。特に夜間バッチは夜間オペレーターや夜間の自動処理に必要な複雑なジョブネットによる夜間の自動処理を必要とするため、特に厳しく精査を行う。

- ローコード・ノーコードツール：
  従来型のローコード・ノーコードツールの適用は、ツールの有効性と効果、体制、システム開発における生成AI利用との比較等から慎重に検討する。

・合理的な調達単位の検討

新たな要件やアーキテクチャを前提に調達単位の整理を行う。マイクロサービス化による調達の分割、CI/CD実施による開発と運用保守の一体化等を検討する。

マイクロサービスの単位で調達を分割する場合は、１マイクロサービスを数人程度で開発するチームを前提にチーム構成を検討されたい。また、フロントエンド・バックエンド分離型 Web システムではフロントエンドの開発チームを独立させることが前提となる。一方で、調達単位を分割しすぎることで、発注者側の調達に係る負担や事業者の管理・調整に係る負荷が増大することから、プロジェクトの実効性が損なわれないよう留意する必要もある。いたずらに調達単位を分割しすぎず、全体を統括する役割を明確にしながら調達単位の適正化を図られたい。

5) 刷新時のプロセス（設計開発・運用保守工程）

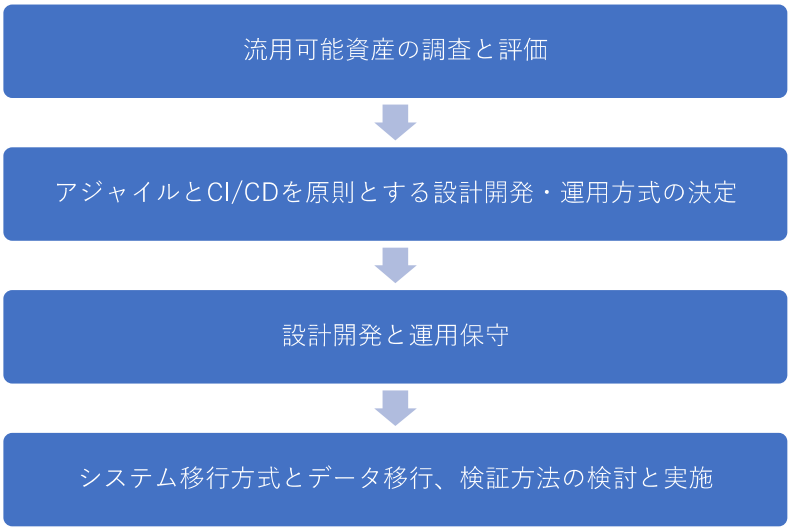

図 3-3 刷新時のプロセス（設計開発・運用保守工程）

・流用可能資産の調査と評価

現行システムから流用できる資産を調査し、評価する。業務やシステムを抜本的に見直す方針から、要件定義や見積りの段階では、原則として資

産の流用は前提としないが、新たな要件確定後の開発時には流用可能な資産（設計ドキュメントやソースコード等）の調査を行う。なお、流用資産は原則として単純流用するのではなく参考情報として活用する。

・アジャイルと CI/CD を原則とする設計開発・運用方式の決定
　調達された事業者からの提案をベースにアジャイルと CI/CD を原則とする開発・運用方式、開発ツール等を決定する。

・設計開発と運用保守
　前述の要件定義や設計開発・運用方式を用いて設計開発・運用保守を行う。

・システム移行方式とデータ移行、検証方法の検討と実施
　システム移行方式、データ移行、結果検証方法等を決定し実行する。

6)　暫定対処時のプロセス（要件定義工程）

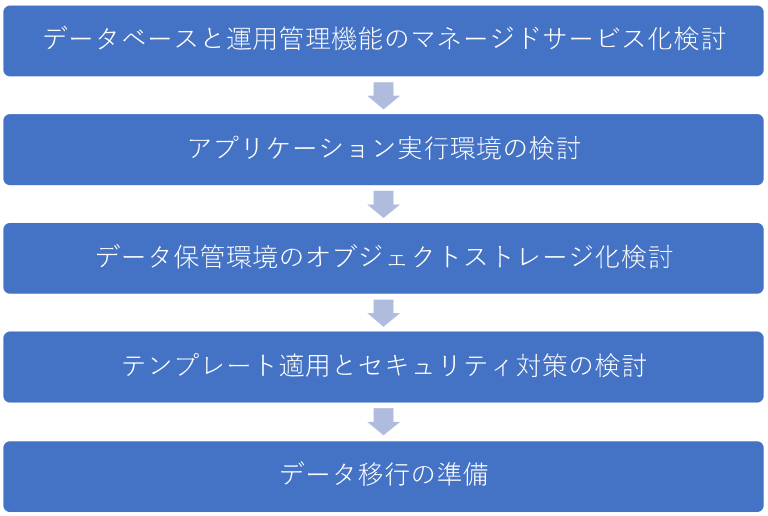

図 3-4　暫定対処時のプロセス（要件定義工程）

・データベースと運用管理機能のマネージドサービス化検討
　使用するサービスの検討とシステム構成図の作成を行う。

・アプリケーション実行環境の検討
　大規模な改修を要さない場合については、コンテナ化、サーバーレス等のアプリケーション実行環境を可能な範囲で検討する。

・データ保管環境のオブジェクトストレージ化検討
　データを共有ストレージに保管するのではなくオブジェクトストレージに保管するよう検討を行う。

・テンプレート適用とセキュリティ対策の検討
　ガバメントクラウドで要求されるテンプレートとセキュリティ対策を確認し、実現方法を検討する。

・データ移行の準備
　システム移行方式、データ移行、結果検証方法等を概要レベルで検討する。

7)　暫定対処時のプロセス（設計開発・運用保守工程）

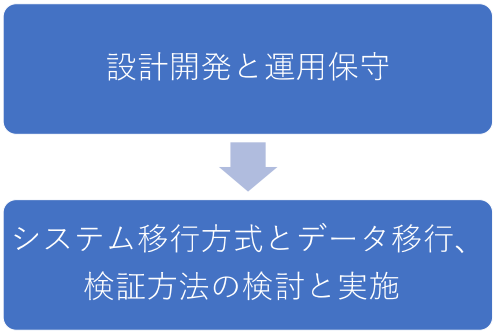

図 3-5　暫定対処時のプロセス（設計開発・運用保守工程）

・設計開発と運用保守
　現行システムでの方式にアジャイル要素を加味した設計開発・運用保守を行う。

・システム移行方式とデータ移行、検証方法の検討と実施
　システム移行方式、データ移行、結果検証方法等を決定し実行する。

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 等クラウドサービスリストに登録されていない場合、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

(1) 日本公認会計士協会　保証業務実務指針 3850
「情報セキュリティ等に関する受託業務の Trust に係る内部統制の保証報　告書に関する実務指針」

(2) AICPA　SOC2/SOC3

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 28 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。

附則（令和５年９月 29 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。

附則（令和７年５月 27 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。

附則（令和８年 X 月 XX 日デジタル社会推進会議幹事会改定）

２　施行期日

本方針は、改定の日から施行する。

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））