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

2021 年（令和 3 年）3 月 30 日

各府省情報化統括責任者（ＣＩＯ）連絡会議決定

〔標準ガイドライン群ＩＤ〕
1003

〔キーワード〕
クラウドサービス、クラウド・バイ・デフォルト、パブリック・クラウド、プライベート・クラウド、IaaS、PaaS、SaaS、政府共通プラットフォーム、ISMAP

〔概要〕
政府情報システムのシステム方式について、コスト削減や柔軟なリソースの増減等の観点から、クラウドサービスの採用をデフォルト（第一候補）とし、府省ＣＩＯ補佐官の関与の下、事実に基づく客観的な比較を行いその利用を判断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
2021年3月30日		・ISMAPに関連する記述の追加及び修正
2018年6月7日	-	・初版決定

目次

１　はじめに

１．１　背景と目的

近年、急速に進化し発展したクラウドサービスは、正しい選択を行えば、コスト削減に加えて、情報システムの迅速な整備、柔軟なリソースの増減、自動化された運用による高度な信頼性、災害対策、テレワーク環境の実現等に寄与する可能性が大きく、政府情報システムにおいても、クラウドサービスを利用することで様々な課題が解決されることが期待される。

しかしながら、これまで政府では、情報セキュリティや移行リスクへの漠然とした不安、不十分な事実認識等から、クラウドサービスの利用に前向きでなかった側面が否定できない。一方、多方面にわたり、クラウドサービスの利用が増加してきている。

このような状況において、「世界最先端ＩＴ国家創造宣言・官民データ活用推進基本計画」（平成 29 年 5 月 30 日閣議決定）及び「デジタル・ガバメント推進方針」（平成 29 年 5 月 30 日高度情報通信ネットワーク社会推進戦略本部・官民データ活用推進戦略会議決定）では、クラウド・バイ・デフォルト原則、すなわち、政府情報システムを整備する際に、クラウドサービスの利用を第一候補とすることとされ、「デジタル・ガバメント実行計画」（平成 30 年 1 月 16 日 e ガバメント閣僚会議決定）において、「政府情報システムにおけるクラウド・バイ・デフォルトの基本的な考え方、各種クラウド（パブリッククラウド、プライベートクラウド等）の特徴、クラウド利用における留意点等を整理する」こととされたところである。

このため、本方針では、クラウド・バイ・デフォルト原則を具体化し、各府省が、効果的なクラウドサービスを採用し、かつ、クラウドサービスを効果的に利用するに当たり、クラウドサービス利用検討フェーズ[注記)]に係る基本的な考え方を示すものである。

注記）クラウドサービスを利用した情報システムに係るライフサイクルは、クラウドサービス利用検討フェーズ、クラウドサービス導入フェーズ、クラウドサービスモニタリングフェーズ、クラウドサービス見直しフェーズに大きく分類できる。本方針は、クラウドサービス利用検討フェーズを主に取り扱っている。

１．２　適用対象

本方針の適用対象は、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、「標準ガイドライン第１編第３章１．適用対象」の規定に基づき適用対象外とされた事項については本方針の全部を適用対象外とする。

１．３　位置づけ

本文書は、標準ガイドライン群の一つとして位置づけられる。

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	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、柔軟性を持つ共用可能な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。
パブリック・クラウド	任意の組織で利用可能なクラウドサービスであり、リソースは事業者（クラウドサービス提供者）によって、制御される。
プライベート・クラウド	サービス提供元の組織でのみ利用可能なクラウドサービスであり、リソースも自らによって制御する。政府内においては、政府共通プラットフォームや各府省独自の共通基盤、共通プラットフォーム等が該当する。なお、組織でリソースを確保し、運用を民間に委託する形態等も含まれる。
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（データセンター、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

用語	意味
	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がサービスとして提供されるもの。具体的には、政府外においては、安否確認、ストレスチェック等の業務系のサービス、メールサービスやファイル保管等のコミュニケーション系のサービス等がある。政府内においては、府省共通システムによって提供される諸機能や、政府共通プラットフォーム上で提供されるコミュニケーション系のサービス・業務系のサービスが該当する。

１.５　クラウドサービスの利用メリット

情報システムの整備に際し、クラウドサービスを利用する主たるメリットとしては、以下が想定される。

1)　効率性の向上

クラウドサービスでは、多くの利用者間で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が公表されていることから、値下げ競争が起きている状況にある。

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。

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、「３．１クラウドサービスの利用検討プロセス」に基づき、情報システム化の対象となるサービス・業務、取扱う情報等を明確化した上で、メリット、開発の規模及び経費等を基に、検討するものとする。

なお、本プロセスは、技術の進展や選択肢となる新たなクラウドサービスの出現に応じて、各利用検討の内容や順序は、適宜見直しを行うものとする。

2．2　府省ＣＩＯ補佐官の関与

情報システム部門がクラウドサービスの利用を検討する場合には、事業者か

ら提供された情報を基に職員のみで判断するのではなく、企画段階及び予算要求段階から、府省ＣＩＯ補佐官の関与の下で、検討するものとする。

コラム：クラウドサービスが危険だろうと思い込んではいけない

従来のシステム方式であるオンプレミスは、クローズドなネットワーク内で利用されているため安全であり、一方オープンなネットワークを経由して利用するクラウドサービスは危険だろう、逆に、全てのクラウドサービスのコストが規模の経済によって安く、信頼性が高いだろうといった印象により、具体的な比較検討を行わずに、安易に判断することは避ける必要がある。

オンプレミスによる構築とクラウドサービスの利用における様々なサービス条件の選択肢を、複数の事業者等から情報を得た上で、利害関係者によるバイアスを排して客観的に比較し、利便性、情報セキュリティ、コスト等のバランスを踏まえ、事実に基づいた判断を行うことが望まれている。

最新技術の導入に、必ずしもクラウドサービスは必須ではないが、今日、クラウドサービスの利用が最新技術を合理的なコストで利用するための非常に有効な手段であることを鑑みると、最新技術の合理的な利用を目的としたクラウドサービスの採用についても積極的に検討する必要がある。

インターネットとの接続の有無のみによって、情報システムの安全性を単純に判断してはいけない。情報セキュリティを重視して情報システムをインターネットから物理的に分離する場合は、物理分離を実施していることだけをもって十分な情報セキュリティ対策を講じているわけではないことを理解し、物理分離と従来型のセキュリティ対策に加え、最新技術の適切な組み合わせによる多重防御を実施することが望ましい。また、インターネットに接続されていることだけからクラウドサービスが危険だろうと思い込んではいけない。

コラム：正しいクラウドサービスのみを選択

クラウドサービスの黎明期や成長期には、「クラウド」と名乗ることがビジネス戦略上の必要性となり、クラウドサービスの利用メリットを十分に享受できない、クラウドサービスも数多く出現した。

従来型の共同データセンタの単なる延長線上にあるものや、単に仮想化技術を採用しただけのものは、本方針におけるクラウドサービスの定義には該当しない。

クラウドサービスとは、前述「クラウドサービスの利用メリット」で記述

した「効率性の向上」、「セキュリティ水準の向上」、「技術革新対応の向上」、「柔軟性の向上」、「可用性の向上」に寄与するものであるとするものである。

特に IaaS/PaaS（パブリック・クラウド）においては、十分な稼働実績を有し、運用の自動化やサービスの高度化、情報セキュリティの強化、新機能の追加等に積極的かつ継続的な投資が行われているクラウドサービス提供者を選定することが重要である。

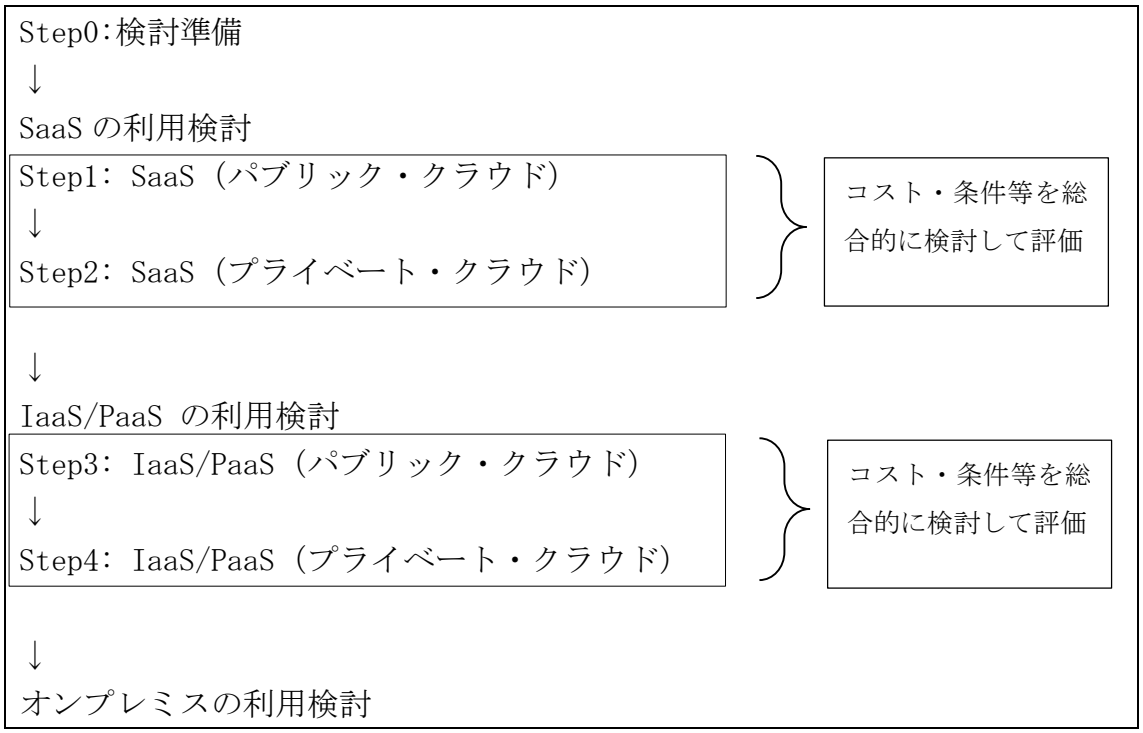
なお、SaaS（パブリック・クラウド）においては、未だ市場が流動的であることから、後述「SaaS（パブリック・クラウド）の利用検討と利用方針」を活用して慎重に検討することが望まれる。

3　具体方針

3.1　クラウドサービスの利用検討プロセス

クラウドサービスの利用に係る検討は、その対象となるサービス・業務及び取り扱う情報を明確化した上で、クラウドサービスの利用メリットを最大化並びに開発の規模及び経費の最小化の観点により、表 3-1 のプロセスで評価検討するものとする。その結果、いずれのクラウドサービスもその利用が著しく困難である場合、又はいずれのクラウドサービスの利用メリットがなく、かつ、クラウドサービスによる経費面の優位性も認められない場合のみオンプレミスとする。

表 3-1 クラウド・バイ・デフォルト原則に基づく利用検討プロセス



３．２ Step0:検討準備

クラウドサービスの利用検討に先立ち、対象となるサービス・業務及び情報といった以下の事項を可能な限り明確化するものとする。

1) 業務の基本属性

(1) 主なサービス利用者（国民向けサービスか、職員向けサービスか）及びその利用者の詳細
(2) インターネット利用を前提とした業務か否か
(3) サービスの種別（特定の業務か、コミュニケーション系か）等
(4) 他のサービスやシステムとの連携

2) 必要なサービスレベル

(1) サービス提供時間
(2) 障害発生時の復旧許容時間
(3) 災害対策の要否等

3) サービス・業務の定常性

(1) 定常的なサービス・業務か、試行的又は一時的なサービス・業務か

4) 業務量

(1) 業務処理量の総量、単位時間当たりの処理量の予測

(2) 業務処理量の変動（増加・減少、ピーク特性等）予測

5) 取り扱う情報

(1) 府省の情報セキュリティポリシー等に基づいた情報の格付け（機密性、完全性、可用性)、取扱制限

３．３ Step1:SaaS（パブリック・クラウド）の利用検討と利用方針

検討準備の検討結果を踏まえ、その行うサービス・業務における情報システム化に係るものについて、その一部又は全部が SaaS（パブリック・クラウド）により提供されている場合（SaaS（パブリック・クラウド）の仕様に合わせ、サービス・業務内容を見直す場合も含まれる。）には、クラウドサービス提供者が提供する SaaS（パブリック・クラウド）が利用検討の対象となる[注記)]。

注記）例えば、SaaS（パブリック・クラウド）を利用する政府情報システムとしては、業務系のクラウドサービスでは、災害時の安否確認システム、職員の業務管理システム、職員及び外部委託先等のプロジェクト管理システム等への利用が挙げられる。また、コミュニケーション系のクラウドサービスでは、メール・スケジュール管理等を中核とする統合コミュニケーションシステム、オンラインストレージ等が想定される。

また、利便性及び性能に秀で、事業リスクを最小化する SaaS（パブリック・クラウド）を選定するため、次の事項を満たすものを利用するものとする。

1) クラウドサービスの選定

(1) SaaS（パブリック・クラウド）においては、コミュニケーション系のクラウドサービスでは、十分な稼働実績を有し、運用の自動化、サービスの高度化、情報セキュリティの強化、新機能の追加等に積極的かつ継続的な投資が行われ、サービス終了のリスクが低い、クラウドサービスを選定するものとする。IaaS/PaaS をインフラ部分として構築された業務系の SaaS については、少なくとも、そのインフラ部分において、コミュニケーション系のクラウドサービスと同等の投資が行われていることが望ましい。

(2) 統一基準に定める「クラウドサービスの利用に関する遵守事項」を満たすクラウドサービスを選定するものとする。

(3) クラウドサービスの調達を行う際は「政府情報システムのためのセキュリティ評価制度（ISMAP)」において登録されたサービスから調達することを原則とする。本原則による調達が困難な場合には暫定措置により対応することを検討する。さらに、暫定措置による対応も困難なクラウドサービスを調達する場合は、当該調達を行う府省の最高情報セキュリティ責任者の責任において、ISMAP の要求事項や管理基準を満たしていることを、それぞれの府省で確認する。なお、暫定措置により対応する場合及び暫定措置による対応も困難なクラウドサービスを調達する場合には、例えば ISMAP 以外のクラウドセキュリティ認証等（「４．１ISMAP 以外のクラウドセキュリティ認証等」参照）も参照することが考えられる[注記)]。

注記)「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）

(4) クラウドサービスに保存される利用者データの可用性の観点から、我が国の法律及び締結された条約が適用される国内データセンタと我が国に裁判管轄権があるクラウドサービスを採用候補とするものとする。ただし、データの保存性、災害対策等から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、又は争訟リスク等を踏まえ海外にあることが特に問題ないと認められる場合はこの限りではない。

2) 情報セキュリティ

(1) 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パブリック・クラウド上で扱わないものとする。

(2)クラウドサービス提供者から提供されているサービスが各府省の情報セキュリティポリシーを満たしていることを、ISMAP の管理基準への対応状況の確認結果又は ISMAP 以外のクラウドセキュリティ認証等の認証基準、監査フレームワークの監査報告書の活用や個別の調査等により確認するものとする。

(3) クラウドサービス利用時の伝送路は暗号化するものとする。格納されるデータやデータベースについても、機微な情報については暗号化を行

うものとする。データの暗号化に使用する鍵については、クラウドサービス提供者側よりも利用者側で管理することが望ましく、選択可能な場合は利用者側で鍵管理が可能な暗号機能を選ぶものとする。

3) クラウドサービスの利用

(1) データバックアップは、クラウドサービスの全体的な災害や障害に備え、クラウドサービスの外部でも保管することが望ましい。

(2) 将来、他のクラウドサービスに移行可能となるように、データ移行の手段を情報システムの要件定義当初から考慮しておくものとする。

(3) 情報システムの運用において管理に必要なログの種類とクラウドサービス上取得できるか否か、その際の利用料金等をあらかじめ確認しておくものとする。

３．４　Step2:SaaS（プライベート・クラウド）の利用検討

Step1 までの検討結果を踏まえ、その行うサービス・業務における情報システム化に係るものについて、その一部又は全部が、府省共通システムの諸機能、政府共通プラットフォーム、各府省の共通基盤等で提供されるコミュニケーション系のサービスや業務系のサービスを SaaS として、当該サービスが利用検討の対象となる[注記)]。

注記）例えば、SaaS（プライベート・クラウド）を利用する政府情報システムの例としては、府省共通又は府省内等に閉じて、行政に特化した業務サービスを提供する情報システム（人事給与サービス、旅費システム等)、行政データを提供・共有する情報システム（職員認証サービス（ＧＩＭＡ)、各種ＡＰＩでのサービス提供）等を利用する情報システムが想定される。

SaaS（プライベート・クラウド）の利用に当たっては、府省共通システム、政府共通プラットフォーム、各府省の共通基盤等で提供されるサービスの仕様及び運用ルールに従う必要がある。

３．５　Step3:IaaS/PaaS（パブリック・クラウド）の利用検討と利用方針

Step2 までの検討結果を踏まえ、SaaS の利用が著しく困難である場合、又は経費面の優位性その他利用メリットがない場合については、民間事業者が提供する IaaS/PaaS（パブリック・クラウド）が利用検討の対象となる[注記)]。

注記）例えば、IaaS/PaaS（パブリック・クラウド）を利用する政府情報シス

テムとしては、ハードウェアのスペックや数量といったリソースの正確な初期見積もり（サイジング）が困難又は大きな変動が見込まれる情報システム、24 時間 365 日のサービス提供や災害対策が特に必要な情報システム、インターネットを介して国民や法人に直接サービス（ＡＰＩを含む。）を提供する情報システム、最新技術を含めパブリック・クラウドの提供する技術・機能・サービス（運用管理、マイクロサービス、分析機能、ＡＩ等）の採用が基本となる情報システム等が想定される。

また、利便性及び性能に秀で、事業リスクを最小化する IaaS/PaaS（パブリック・クラウド）を選定するため、次の事項を満たすものを利用するものとする。

1) クラウドサービスの選定

(1) IaaS/PaaS（パブリック・クラウド）の利用においては、「３．３1)クラウドサービスの選定」の(1)から(4)までに掲げる事項と同様の取扱いとする。

(2) バックアップ環境や災害対策環境が、データの同期やバックアップへの切換の仕組みも含め、標準サービスとして提供されているクラウドサービスのみを選定するものとする。

2) 情報セキュリティ

(1) IaaS/PaaS（パブリック・クラウド）の利用においては、「３．３2)情報セキュリティ」の(1)から(3)までに掲げる事項と同様の取扱いとする。

(2)統一基準を満たすことを容易に確認できない場合には、任意機能の構築として、統一基準を満たす情報セキュリティ機能を利用者側で設計・実装する。

3) クラウドサービスの利用

(1) IaaS/PaaS（パブリック・クラウド）の利用においては、「３．３3)クラウドサービスの利用」の(2)に掲げる事項と同様の取扱いとするものとする。

(2) データバックアップは、データの完全性やデータリカバリのコストのバランスを踏まえ、同一クラウドサービスの内部で複数作成するものとする。また、クラウドサービスの全体的な災害や障害に備え、クラウドサービスとは別に外部でも保管することが望ましい。

(3) 24 時間 365 日のサービス提供が必要不可欠である情報システムについ

てはサービスの冗長化を行う。フェイルオーバー時の運用についてもあらかじめ準備を行っておくものとする。

4) システム移行

既存システムをクラウドサービスに移行させる際には、クラウドに最適化されたアプリケーションとして改修した上で移行することが望ましい。

5) オンプレミス等と連携するシステム形態について

パブリック・クラウドを利用する際に、オンプレミスやプライベート・クラウド上で運用する情報システムとパブリック・クラウド上で運用する情報システムとを連携させるシステム形態については、情報システムの複雑性が増し、結果として高コストとなること及び複雑性に起因する情報セキュリティ対策の困難さが増すことに留意するものとする。例えば、システム移行や既存システムとの連携等で当該形態とならざるを得ない場合や、連携させるオンプレミスやプライベート・クラウドが利用を検討しているパブリック・クラウドよりも明確に高い水準の情報セキュリティ対策を実装している場合は、メリットとリスクを明確にした上で利用するものとする。

コラム：パブリック・クラウドのグループ利用について

パブリック・クラウド、特に IaaS/PaaS を利用する際に、府省ＰMO等がクラウドサービスを一括して調達し、各ＰＪMOにそのリソースを使用させるグループ利用という選択肢も考えられる。

グループ利用は、以下のメリットが想定される。

(1) 各ＰＪMOが個別にクラウドサービスを調達する必要がなくなる。

(2) ＰMOによるＩＴガバナンスが強化され、運用や情報セキュリティ対策で一定水準以上を担保可能になる。

(3) 特に IaaS/PaaS においては、管理機能の共通化、情報セキュリティ対策の共通化等から全体コストの削減が期待される。

逆に、グループ利用は、以下のデメリットも想定される。

(1) クラウドサービスを一括調達し、グループ利用を管理する組織、プロセスが必要となる。

(2) 上記の管理組織を介することで、調達手続等が煩雑になることや即時性、柔軟性が阻害される可能性がある。

(3) 共同利用環境のため、利用条件に制約が生じることや機動性が失われて最新サービス・最新技術の適用が困難になる可能性がある。

グループ利用の是非については、上記のメリット・デメリットを十分に考慮して判断する必要がある。また、グループ利用を行う際には、上記のメリットを最大化しつつ、デメリットを最小化するアプローチが必須となる。

３．６　Step4:IaaS/PaaS（プライベート・クラウド）の利用検討

Step3 までの検討結果を踏まえ、IaaS/PaaS（パブリック・クラウド）の利用が著しく困難である場合、又は経費面の優位性その他利用メリットがない場合については、サーバ構築ができる政府共通プラットフォーム、各府省独自の共通基盤等を IaaS/PaaS として、当該サービスが利用検討の対象となる[注記)]。

注記）IaaS/PaaS（プライベート・クラウド）を利用する政府情報システムとしては、当該政府情報システムが扱う情報の格付けや情報セキュリティポリシー等でパブリック・クラウドの利用が明示的に禁じられている情報システム、府省共通システム等、政府共通プラットフォームが提供する共通機能・共通サービスの利用が基本となる情報システム、SaaS 利用で代替できない（独自システムの構築が必要な）小規模システム、情報システムを担当する職員等の体制が不十分であり、単独ではパブリック・クラウドの適切な利用が困難と想定される情報システム等が想定される。なお、IaaS/PaaS（プライベート・クラウド）にはパブリック・クラウドのグループ利用も想定される。

コラム：小規模システムは IaaS/PaaS （プライベート・クラウド）へ

SaaS 利用で代替できない（独自システムの構築が必要な）小規模システムが、独自に、インフラ環境を構築し、又は管理機能や情報セキュリティ対策を行うことは、コスト面において非効率となったり、情報セキュリティ、運用性等が不十分になることがある。

このため、SaaS 利用で代替ができない小規模システムは、上記の課題を解決するような IaaS/PaaS （プライベート・クラウド）が利用可能であれば、これを利用することが望ましい。

また、情報システムを担当する職員等の体制が不十分であり、単独ではパブリック・クラウドの適切な利用が困難と想定される情報システムについても、これらの課題を解決する IaaS/PaaS （プライベート・クラウド）が利用可能であれば、これを利用することが望ましい。

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、パブリック・クラウドに関しては、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。パブリック・クラウドにおいては、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_gold_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/WebTrsuts）（日本公認会計士協会 IT2 号）

コラム：パブリック・クラウドの調達について

パブリック・クラウド、特に IaaS/PaaS を利用する際には、各府省がクラウドサービス提供者と直接契約して利用料金を支払う形態と、情報システムの運用事業者を介して契約して支払業務を委託した上で支払う形態の２つが想定される。

直接契約は、サーバ等の物品を情報システムの開発とは別に調達する形に近い。ただし、利用量に応じて変動する月額料金等、従来の買取りやリース、レンタルとは異なる対応が必要となる。

運用事業者を介しての契約は、情報システムの設計・開発並びに運用及び保守と併せて一括して、運用事業者（設計・開発事業者及び保守事業者が運用事業者と同一となるものと想定している。）と契約するため、従来の一括調達（役務と物品）に近い形となる。ただし、クラウドの利用料金を固定的

な価格で契約する場合は、料金変動のリスクを運用事業者が負うことになるため、リスク分が上乗せされた費用となる可能性が高い。

なお、運用事業者を介しての契約の場合、クラウドサービスについては、調達仕様を満たすサービスを選定して提案することになるが、合理的な理由がある場合は、使用するクラウドサービスを製品指定することも可能である。

別紙　附則

附則（平成 30 年 6 月 7 日各府省情報化統括責任者（ＣＩＯ）連絡会議決定）

１　施行期日

本方針は、決定の日から施行する。

２　経過措置

本方針の施行日前に、政府情報システムの要件定義以降の工程を行った政府情報システムの整備及び管理に関する事項については、なお従前の例とする。ただし、本方針を踏まえ、クラウドサービスの利用検討を行うことを妨げるものではない。

附則（令和 3 年 3 月 30 日各府省情報化統括責任者（ＣＩＯ）連絡会議改定）

１　施行期日

本方針は、改定の日から施行し、改定後の本方針の規定は、令和 3 年 3 月 12 日から適用する。