大阪市クラウドサービス
関連ガイドライン

令和6年4月
デジタル統括室

改正履歴

改正日付	改正概要
令和　３年　４月　１日	新規作成
令和　４年　４月　１日	組織名変更に伴う変更及び大阪市共有クラウドに関する記載の追加等
令和　５年　４月　１日	・第５章（クラウドサービスの利用）を追加 ・各所、今現在の技術に合わせて変更 ・職制改正に伴う変更
令和　５年　９月　12 日	・ICT 関連経費等の予算算定・審査事務の見直しに伴う変更
令和　６年　４月　１日	・他のガイドライン等と重複する記載を削除 ・協議様式の変更に伴う記載の変更

目次

第１章　クラウドサービス関連ガイドライン

クラウドサービスについて

本ガイドラインの目的

本市では、「大阪市システム刷新計画」を策定し、システムの見直しにあたっては、クラウド・バイ・デフォルトに則り、クラウドサービスの利用を前提に検討していくこととしており、すでに複数の業務でクラウド技術の活用が始まっています。今後、本市のデジタル化において、市民・事業者・職員の多種多様な環境やニーズを踏まえて、利用者目線で誰もが、いつでも、どこでも、デジタル化の恩恵を享受できる社会を実現するため、本ガイドラインにより積極的なクラウドサービスの活用を推進していくことを目的としています。

１．　クラウドサービスについて

１．　クラウドサービスとは

クラウドサービスとは、従来は利用者が手元にあるコンピュータに導入して利用していたようなソフトウェアやデータを、インターネットなどのネットワーク経由で、必要に応じて利用者に提供するサービスです。

ここでは代表的なクラウドサービスの形態とクラウドサービスを利用する上での環境について説明します。なお、本市では、クラウドサービスは SaaS（ノーコード・ローコード含む）利用を基本とします。SaaS 利用が難しい場合は、IaaS、PaaS で大阪市共通クラウドの利用を検討してください。

(1)　クラウドサービスの形態

① SaaS（ASP）とは

クラウド上に用意されたソフトウェアをサービスとして提供するものであり、例えば業務を遂行するためのアプリケーション（給与計算や人事管理、販売管理、在庫管理等）がインターネットを通じて利用できるサービス形態です。

例：Gmail、Amazon Prime Video、e-Learning サービス、クラウドフォトサービス、Netflix、Spotify、Slack

なお、SaaS は例示のように、カスタマイズの余地がないものが一般的ですが、柔軟にカスタマイズが可能なものや、ノーコード・ローコードツールのようにアプリケーションを自身で作るものなど多種多様に存在します。

ASP（Application Service Provider）は、サービスを提供する事業者を指しますが、本ガイドラインにおいては、ASP が提供するサービスも SaaS として取り扱います。

② PaaS とは

クラウド上に用意された仮想のコンピュータに加えて、開発環境やデータ処理のためのミドルウェアやユーザインターフェイスモジュール等、コンピュータを使いこなすための道具類もセットにして提供するサービスです。IaaS 同様、コンピュータの上で自らアプリケーションを開発したり、インストールしたりして使用するレベルのユーザや、Web アプリケーションを構築して情報発信をするようなユーザが利用するのに適しています。

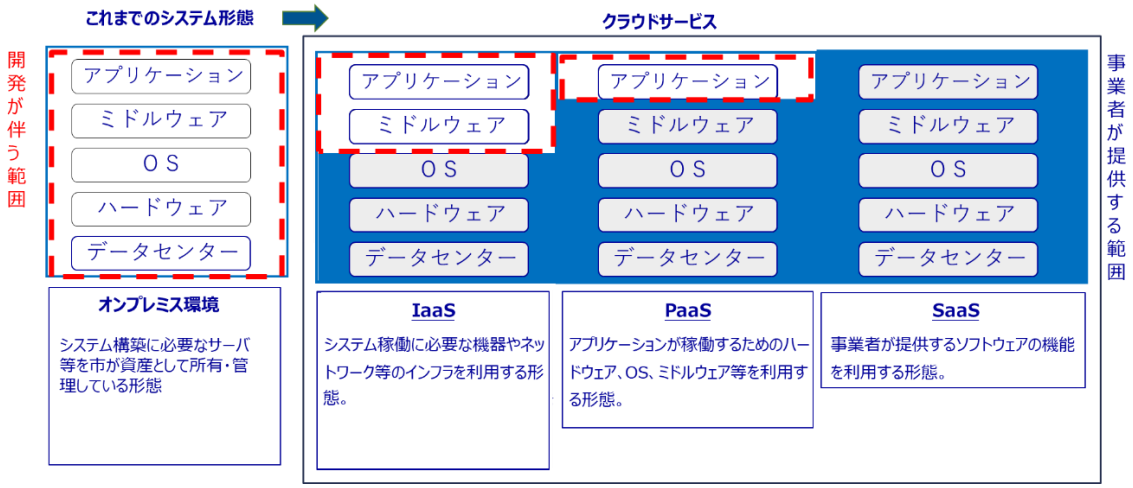
例：Amazon Web Services（アマゾン ウェブ サービス、略称：AWS）、Microsoft Azure（マイクロソフト・アジュール）、Google Cloud、IBM Cloud

③ IaaS とは

クラウド上に用意された仮想のコンピュータをユーザが直接利用するクラウドのサービス形態です。ユーザからは、一定の機能スペックのハードウェアの上に OS が設定された形で見えます。コンピュータの上で自らアプリケーションを開発したり、インストールしたりして使用するレベルのユーザが利用するのに適しています。

例：Google Cloud、Amazon Elastic Compute Cloud、Microsoft Azure（マイクロソフト・アジュール）、IBM

Cloud、レンタルサーバ



(2)　クラウド環境の種類

クラウドの環境には2種類あり、次のような特徴があります。また、各クラウドに本市から接続する方法もインターネット回線や専用線による接続があり、最適な形態を選択する必要があります。本市ではパブリック・クラウドの利用を前提に検討します。

① パブリック・クラウド

企業もしくは個人などユーザ全体に対して、サーバ、データベース、ソフトウェアや回線などの環境を提供するサービスのことを言います。企業でも個人でも利用したい人が利用したい時に必要な分を利用することができます。

② プライベート・クラウド

企業・組織が、自社内でクラウド環境を構築し、組織内での部署に対して提供する形態を言います。

【専用線について】
クラウドサービスを利用する際に、セキュリティ対策や通信速度の確保等により専用線を利用する場合があります。
本市においては、Microsoft Azure へ直接接続する帯域保証型のネットワークサービス「ExpressRoute（エクスプレスルート）」を利用しています。その他、AWS の「AWS Direct Connect」など様々なサービスがあります。
また、「VPN（Virtual Private Network、仮想専用線）」の技術による通信接続方法もあり、利用するクラウドサービス及び取り扱う情報等により必要となる通信方法を選択する必要があります。
なお、専用線を利用する場合は、基本的にクラウドサービスとは別に契約をする必要があります。

２．　クラウドサービス利用のメリット

１．　クラウドサービス利用のメリット

ここでは、オンプレミスとクラウドサービスとの比較におけるメリットについて説明します。

(1)　導入時の負荷軽減

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、一利用者当たりの利用料は低価格となります。また、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です。

(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ます。また、情報セキュリティ評価及び認証を受けてい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ます。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、市場において激しい競争環境下にあるクラウドサービスを利用する方が、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ます。

(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、AI、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）が随時追加されます。そのため、クラウドサービスを比較、選定、導入することで、最新技術を活用することができます。

(4)　柔軟性の向上

クラウドサービスは、インターネットに接続できれば、デバイスや OS、庁内情報ネットワークへの接続有無にとらわれることなく利用できるため、様々な職場環境に適応します。

また、リソースの追加、変更等が容易であることや数か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ます。さらに、一般に汎用サービス化した機能の組合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など柔軟な対応が可能です。

(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ます。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ます。

３．　クラウドサービスを選定する際に注意すべきこと

１．　クラウドサービス利用において注意すべき点

クラウドサービスは、低廉な価格で多様なサービスが利用可能となり、第三者認証等を取得しているものであれば一定のセキュリティ水準を確保できるといったメリットがある一方、その契約条件として（民間事業者側が定めた）約款に則ることが義務付けられる場合が多いです。その場合、本市が求める情報セキュリティ対策が、当該クラウドサービスに十分に講じられない可能性があります。選定の際は、大阪市クラウドサービス利用基準「5 クラウドサービスを利用する上での留意事項」に記載されている点に注意してください。

第 2 章　クラウドサービス関連ガイドライン

クラウドサービスの調査

１．　クラウドサービスの調査

１．　SaaS 提供の有無の調査

クラウドサービスのうち、SaaS（ASP）の有無について調査します。調査をする場合には、RFI を行う等、広く情報を収集してください。

（1）　LGWAN-ASP サービスリスト

LGWAN-ASP サービスとして登録されているものは、J-LIS（地方公共団体情報システム機構）のサイト（https://lgwan-asp.j-lis.go.jp/service_list）に掲載されているため、LGWAN-ASP の利用を検討する際は、このサイトから存在するかどうかを確認することができます。

なお、各局等における LGWAN パソコンと LGWAN 接続系リモートデスクトップサービス（RDS）を合わせた LGWAN パソコン、通信量等の環境を考慮する必要があります。

（2）　SaaS について

業務にあったサービスについて、広く調査します。調査方法は、インターネットから検索、RFI、IT ソリューションが集まるイベントに参加、コンサルに依頼するなど様々な方法があります。業務に適合するサービスがない場合でも、複雑な業務でなければノーコード・ローコードツールで対応できる場合や、業務のうち一部を手作業により代替することでサービスに適合させることができる場合もあります。決め打ちで狭い範囲を調査するのではなく、業務をゼロベースで見直す前提で、幅広く調査しましょう。

例えば、〇〇業務の△△情報を地図上で管理できるシステム（個別具体の業務に特化したサービス）を求め、調査を行い、サービスが発見できなかった場合は、地図上で任意の情報を管理できるシステム(汎用的なシステム)を調査する。

また、実際に業務に適合するかを確認するためには、セミナーへの参加やトライアルの実施、事業者に直接説明を求めるなど、より踏み込んだ調査も行う必要があります。

２．　適切なクラウドサービスを選定する

１．　適切なクラウドサービスの選定

「大阪市クラウドサービス利用基準」で、取り扱う情報資産の種類によりクラウドサービスの選定条件を定めていますので、「６　クラウドサービスの利用（重要情報資産を取り扱う場合）」、「７　クラウドサービスの利用（重要情報資産を取り扱わない場合）」を参照のうえ、適切なクラウドサービスを選定してください。

庁内情報利用パソコンからクラウドサービスを利用する場合
インターネット接続の場合は本市側の次の環境等の制限を事前に確認する必要があります。

- ファイアウォール環境は http、https のみ許可している
- プラグイン等ソフトウェアの追加は不可
- 多段 PROXY の環境で使用できること
- 使用しているブラウザで稼働すること
- 推奨する回線速度を満たしていること、またネットワークに悪影響を与えるようなトラフィックの発生がないこと

（※庁内ポリシーについては、適宜見直しを行っているため、デジタル統括室と十分に協議を行い進めてください。）

なお、第１章「１．クラウドサービスについて」でも述べたとおり、IaaS・PaaS の場合は、原則として、大阪市共通クラウドを利用します。大阪市共通クラウドは、市民サービスの向上や行政運営の効率化に向けた「行政のデジタル化」を推進するため、パブリック・クラウドである「Microsoft Azure」を活用して、庁内情報ネットワークおよび公開系ネットワークで稼働する各業務システムの構築環境として導入されたものです。

IaaS・PaaS によるシステム構築を行う場合は、想定事業者に大阪市共通クラウド(Azure)上でのシステム構築が可能かを確認しましょう。

大阪市共通クラウドの利用にあたっての留意事項

- クラウドリフトではなく、PaaS を最大限活用したクラウドシフトを基本として移行を計画する
- オンプレミスとの費用比較だけでなく、不要となるハード保守や物理サーバ維持にかかる費用、利用効果等を抽出する
- クラウドの特性を考慮して、冗長構成やバックアップ（遠隔地保管）等のシステム構成や運用を見直す
- リソースの実績をもとに適切なサーバスペックに定期的に見直す（当初から将来を見据えた高スペックにしない）
- サーバの稼働停止の計画を立てて適切な運用を実施する（従量課金対策）
- デジタル統括室へリソース等の利用料を予算配付するため、次年度の稼働予測を立てる

Oracle 社製のデータベースについて

Oracle 社は、DBMS の提供において世界的な老舗です。安定性、パフォーマンス、拡張性など現在においても最も洗練された DBMS の一つであり、トップシェアとなっています。

しかしながら、Oracle Database の価格が競合のプロダクトと比較して高額である中で、価格改定や廉価版プロダクトの提供が停止されており、Oracle 社クラウド・プラットフォームでなければ高額なライセンス費用となる場合があります。

現行オンプレミスシステムで Oracle 社製のデータベースを利用している場合は、クラウドにした場合のライセンス費用が現行よりも高額になる可能性があるため、その点にも留意しつつ、システムの実現方式をご検討ください。

第３章　クラウドサービス関連ガイドライン

クラウドサービスの調達準備

１．　調達方法の選択について

1.　クラウドサービスの特性に合わせた調達方法

SaaS・PaaS・IaaS の一般的な調達方法について記載します。

（1）　SaaS（カスタマイズ無し）

市場に存在する SaaS 製品をそのままカスタマイズせず利用します。代表的な調達方法として、「サービス提供業務委託」、「利用申し込み」、「ライセンス調達委託」があり、さらに製品指定を行うか否かで対応が分かれます。

・サービス提供業務委託　例：e ラーニング

業務要件を満たすサービスが複数あり、サービスの販売方法が契約で対応可能なもの。本市の契約書による契約を行う。

・利用申し込み　例：EPARK、VoiceBiz

業務要件を満たし、他の選択の余地がない（他のサービスよりも相当に優れている）サービス、かつ、サービスの販売方法が、申込みしか対応できないもの。基本的に提供事業者の利用規約に従う必要があり、本市の特約条項にて契約することはできない。

・ライセンス調達委託　例：大容量ファイル送信サービス（製品指定）、議事録作成支援 SaaS（指定なし）

サービス提供に際し、再販事業者、販売代理店、パートナー企業（以下、「パートナー企業」という。）よりライセンス調達を行う。競争可能な複数事業者が存在するため、ライセンス調達業務委託（クレジット支払い代行業務委託も含む）の入札を行う。

【仕様書作成時の注意点】

製品指定しない場合、仕様書に必要機能等を記載することになりますが、書きすぎるとほぼ製品を指定した仕様書になり、あまり書かないと導入された SaaS では業務が実施できない事態となる可能性があるため、仕様書の記載時には注意が必要です。導入した SaaS で想定した作業ができなかったとしても、仕様書の機能要件を絶対に満たしていないことを証明するのは相当に困難であると想定されます（仕様書にどこまで明確に記載できるか、代替手段が全くないか　など）。

SaaS においては、無料期間でトライアルするなど、必要な機能等の整理を十分に行ってください。

※総合評価やプロポーザルで選定できる場合は、導入する SaaS そのものを評価できるので本内容の対象とはなりません。

（2）　SaaS（カスタマイズ有り）

市場に存在する SaaS 製品では求める要件を満たさない場合、その製品をカスタマイズ（元々なかったオプション機能を新たに追加させる等）して利用する方法もあります。

また、市場にない製品であっても、構築するシステムが汎用的であり、構築後に別の団体にも提供できる可能性があるものについては、「SaaS 構築委託業務」として契約を行います（例：行政オンラインシステム）。この場合は、RFI 等により事業者の意思を確認したうえで調達を進めることとなります。

なお、大阪市しか使用しないサービスは、基本方針書の No.7「システム構成」欄について、「SaaS」ではなく、「その他」を選択し、カッコ内に「大阪市専用 SaaS」と記載してください。

（3）　SaaS（ノーコード・ローコードツール）

ノーコード・ローコードツール（以下、「ノーコード等ツール」については、パートナー企業へのライセンス調達委託となりますが、「ライセンスのみ」と「開発込み」の調達があります。

・ライセンスのみ　例：kintone

ノーコード等ツールを使って、業務で利用するアプリケーションを内製（職員で作成）するもの。(1)と同様。

・開発込み　例：kintone、予算編成システム
　ノーコード等ツールを使ったシステム構築を行うもの。仕様書の記載内容は基本的にシステム構築と相違なし。

（4）　IaaS・PaaS

原則として、大阪市共通クラウド（Azure）を利用します。IaaS・PaaS　部分は、デジタル統括室への申請により利用可能となりますので、サーバ構築及びアプリケーション開発を業務委託することとなります。

仕様書においては、大阪市共通クラウド（Azure）前提の構築・開発となることを記載する必要があります。

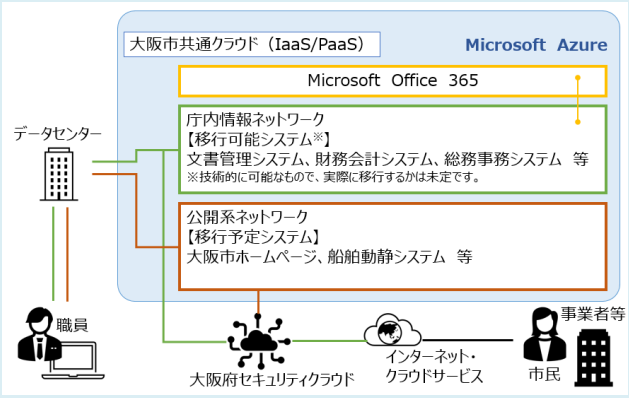
【大阪市共通クラウドに移行できるシステムについて】

大阪市共通クラウドは、IaaS/PaaS 環境であり、システムが稼働するために必要となるサーバ等を、物理的な機器と遜色なく仮想的に構築し、利用することができます。

利用環境として、「庁内情報ネットワーク」、「公開系ネットワーク」があります。

この内、庁内情報ネットワークにおいては、文書管理システム※のような本市内部で稼動するシステム（外部のインターネットを介さず利用できるシステム）の構築が可能となります。

また、公開系ネットワークにおいては、職員側と市民（外部）公開側に分けて利用することが可能で、大阪市ホームページ等の職員、市民両方が利用するシステムの構築が可能です。

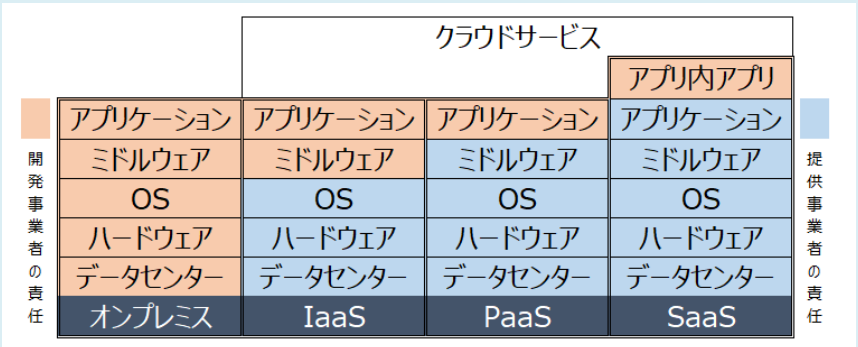


なお、公開系ネットワークにおいては、職員側・市民公開側と分かれて利用することを基本としていますが、一般的なIaaS/PaaS の利用として、例えば、本市が用意する指定管理者向けのシステムなど市民公開側のみを利用することも可能です（ただし、システム所有権が本市のものに限る）。

※技術的に可能なもので、実際に移行するかは未定です。

【SaaS（ノーコード等ツール）にてアプリ開発を委託する場合の責任分界】

ノーコード等ツールそのものは、SaaS ですが、その SaaS を使って、その SaaS 内で稼動するアプリケーション（アプリ内アプリ）開発を委託する場合があります。



通常、この場合において、アプリ内アプリの権利は本市に帰属するものとなります。

なお、調達方法については、「アプリケーション開発＋ライセンス調達」を１つの契約で行う場合と、「ライセンス調達」を本市でしたうえで、その調達した SaaS（ノーコード等ツール）にて「アプリケーション開発」をするという2つの契約で行う場合があります。後者としては別の業務で利用している SaaS（ノーコード等ツール）を利用する場合が想定されます。

ノーコード等ツールプラットフォームを含めてアプリ内アプリを純粋な SaaS（本書で言う「SaaS（カスタマイズ無し）・（カスタマイズ有り）」）で提供させることも可能ですが、ノーコード等ツールの利点を消し、費用増、ベンダロックインのリスクがあります。

２．　要件定義について

1.　サービスの要件定義について

第２章「クラウドサービスの調査」で把握した業務の現状や、調査したクラウドサービスの仕様等の情報を基に調達準備を行います。その際、クラウドサービスにおいて、誰が、何をするのか、どこまでするのか、というサービスの要件を定義していきます。

「第２章２．　適切なクラウドサービスを選定する」、「第４章　クラウドサービスの利用」及び選定しようとしているいくつかのクラウドサービスの仕様も参考に、取扱う業務の内容に応じて、クラウドサービスに求める要件を定めます。

2.　機能要件・非機能要件について

クラウドサービス利用において、必要に応じて機能・非機能要件を定めていきます。

(1)　機能要件について

機能要件においては、本市がクラウドサービスに求める必須要件を提示することが必要となります。

※ただし、これまでの開発を伴う情報システムの構築を同様に検討している場合、業務要件を満たすことが最優先され、コスト削減やクラウドのメリットが充分に出ない可能性があります。ここでは参考にイメージを示します。

基本要件

機能要件		項目	定義内容
共通機能における基本要件	…	…	…
…	…	…	…
業務機能における基本要件	…	…	…
…	…	…	…
システム連携機能における基本要件	…	…	…

☆　機能要件の例については「大阪市システム構成検討ガイドライン」別紙：機能一覧（サンプル）を参考にしてください。

(2)　非機能要件について

非機能要件とは、機能要件以外にクラウドサービスが稼働するうえで必要となる機能（ユーザビリティ、処理性能や拡張性、セキュリティなど）を言います。非機能要件については、本市側がクラウドサービスに求める「質」を提示することで定められます。非機能要件に求める条件は多岐に渡り、全ての要件を考慮することは困難です。そのため、必須要件を整理し、RFI 等で事前に確認を行ってください。

3.　サービスレベルアグリーメント（SLA）について

サービスレベルアグリーメント（Service Level Agreement、以下 SLA とする）とは、業者に委託した作業の品質維持・向上のため、本市と契約先の業者にてサービス提供の水準について明文化し、合意するものです。クラウド事業者と利用者との契約に含まれる内容になります。SLA の内容は情報漏えい等の法的リスクや損害賠償の内容と関連する契約条項となりますが、主に稼働率や障害時の復旧時間、処理レスポンス等について定義する傾向にあります。例えば、サービス稼働率について、利用者は SLA に基づき、サービスの停止時間を想定し、許容するこ

とになります。

稼働率以外にも、クラウドサービスによって SLA の内容は様々ですので、必須要件を整理し、RFI 等で事前に確認を行ってください。

以下に一般的な SLA（例）を示しますが、SaaS・PaaS・IaaS それぞれで非機能要件を設定できる範囲が異なりますので精査のうえ仕様書に記載してください。

クラウドサービス利用における SLA については、高いサービスレベルを求めれば求めるほど、費用が高くなる傾向にあります。利用するクラウドサービスにおいて必要性の高い SLA の項目を検討したうえで、該当する項目を中心に、クラウドサービス事業者に対して合意を求めていくことが重要となります。

SLA（例）

分類	項	項目	内容	評価項目	本市要件
サービス基本特性					
サービス品質	1	稼動率	年間総稼働時間から計画停止時間を控除したシステム稼働時間のうち、計画外停止時間を差し引いた稼働時間の割合	サービスの稼働率	年●●.●%以上
	2	サービスパフォーマンスの管理	機器障害やシステム遅延の監視間隔及び本市への通知に要する時間	a）パフォーマンス監視間隔	●●分
				b）通知時間（異常検知後、本市に通知するまでの時間）	●●分
	3	バックアップ対策	バックアップ実施間隔及びバックアップ保存世代数	a)バックアップ実施間隔	●回／●日
				b)バックアップ世代数	●世代
アプリケーション、基盤、ストレージ等					
セキュリティ	4	ウイルス対策	ウイルス対策のパターンファイルの更新間隔（ベンダリリースからの時間）	パターンファイルの更新間隔	ベンダリリースから●●時間以内
	5	記録(ログ等)	システム利用者（職員ユーザの操作ログ及び市民ユーザの操作ログ）の利用状況の記録の保存期間及び例外処理及び情報セキュリティ事象の記録（ログ等）の保存期間	a)システム利用者の利用状況の保存期間	●●ケ月
				b）例外処理及び情報セキュリティ事象の記録（ログ等）の保存期間	●●年
	6	ID,パスワードの運用管理	ID やパスワードの運用管理方法の規定の有無		有
	7	セキュリティパッチ管理	パッチの更新間隔	OS、その他ソフトウェアに対するパッチ更新作業の着手までの時間	緊急度の高いものについてはベンダリリースから●●時間以内
サービスサポート					
サービス窓口	8	営業日・時間	営業曜日、営業時間	サービスサポートの受付時間	月～金(祝日、12/29～1/3 を除く)9:00～17:30

３．　クラウドサービスのライフサイクルについて

クラウドサービスは日々進化し、変化を遂げています。したがって、各所属においてはクラウドサービス導入後も課題を整理し、また同様のサービスの動向を把握しておく必要があります。

SaaS については、３年を目途に現行のクラウドサービスが適切に稼働しているか、また同様のクラウドサービスでより効率的に利用できるものはないか等情報を集め、現行サービスの継続の可否を検討してください。

大阪市共通クラウド（IaaS/PaaS）については、機器のリース期間にとらわれる必要はありませんが、SaaS 利用の可否についての検討を継続して行い、オンプレミスのシステムと同様に、OS やパッケージソフト等のサポート期間を考慮して更新計画を立てることが必要です。

第 4 章　クラウドサービス関連ガイドライン

クラウドサービスの利用

1.　クラウドサービス利用に際し知っておくべきこと

クラウドサービス利用に関する理解不足や不十分な管理・作業体制、設定不備を起こさせないための情報・ツール提供不足やミスを起こさせにくい設計への配慮不足など、様々な要因が複雑に絡み合いながら積み重なることによって設定不備事案の発生に至っていることが想定されます。

本章においては、これらの設定不備が発生しないよう、安全安心なクラウドサービスの利用に資することを目的として、認識しておくべき事項について取りまとめました。

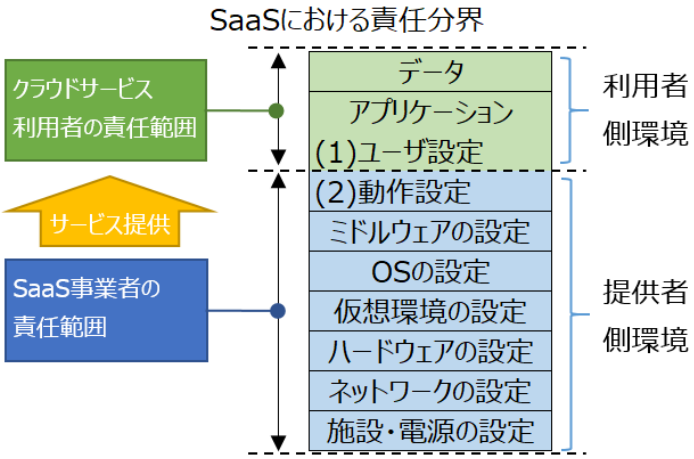
なお、本章内容は 2022 年 10 月総務省発行の「クラウドサービス利用・提供における適切な設定のためのガイドライン」を本市向けに編集したものです。

2.　責任分界

1.　SaaS の設定に関する責任分界

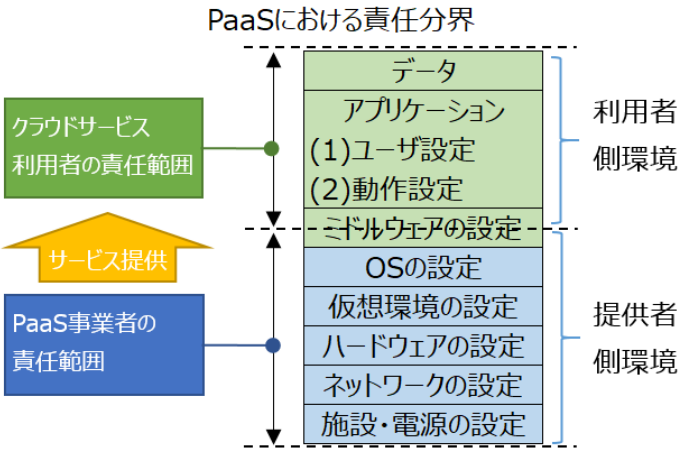
SaaS を利用する場合、右図に示すとおり、クラウドサービス利用者が責任を負う部分は、データとアプリケーションの管理の一部となります。アプリケーションの動作に係る設定は SaaS 事業者が責任を負う一方、利用者アカウントや業務データの設定については、クラウドサービス利用者の責任となります。

クラウドサービス利用者の役割としては、利用者側環境の設定者と設定管理者の両方となります。SaaS 事業者は、提供するアプリケーション以下の提供側環境の設定者と設定管理者になります。



2.　PaaS の設定に関する責任分界

PaaS を利用する場合、クラウドサービス利用者が自ら又は委託してアプリケーションを開発し利用すること等が考えられます。その場合は右図に示すとおり、データとアプリケーションともにクラウドサービス利用者が設定及び管理の責任を負います。PaaS を利用するクラウドサービス利用者は、クラウドサービス事業者との契約に示されている責任範囲を踏まえて、アプリケーションの開発、アプリケーションに対する管理を行いま

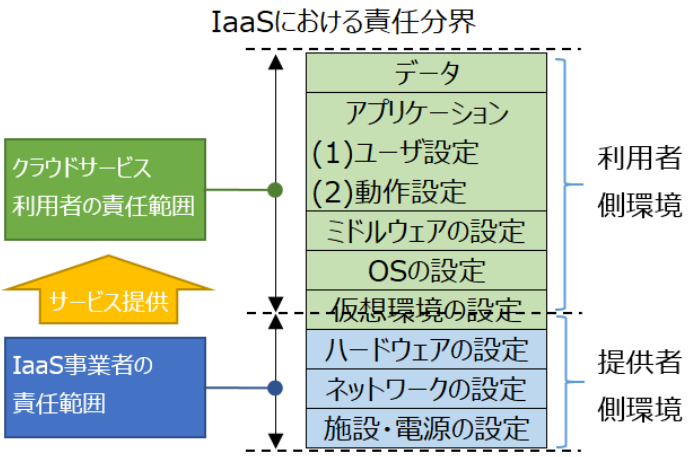


す。また、クラウドサービス利用者はクラウドサービス事業者が提供するプログラミング環境やSQL等のユーティリティインターフェースを利用してミドルウェア層を利用します（クラウドサービス事業者によっては、完全にユーザが責任を持って利用することが前提で用意されているミドルウェアもあります。）。

ミドルウェアの動作に係る設定については、PaaS事業者が責任を負います。ミドルウェアを利用するための設定については、クラウドサービス利用者の責任となります。クラウドサービス利用者の役割としては、利用者側環境の設定者と設定管理者の両方となります。PaaS事業者は、提供するミドルウェア以下の提供側環境の設定者と設定管理者になります。

3.　IaaSの設定に関する責任分界

IaaS を利用する場合は、右図に示すとおり、クラウドサービス事業者はクラウドサービス利用者との契約・SLA に基づき、ゲスト OS[1]等が動作するための仮想環境の構築と管理を提供します。クラウドサービス利用者は、仮想環境上で動作している OS を含めたすべてのソフトウェアの管理を行います。OS やミドルウェア層での障害対応や、ミドルウェアに対するパッチ適応や脆弱性対応などは、クラウドサービス利用者の責任となります。

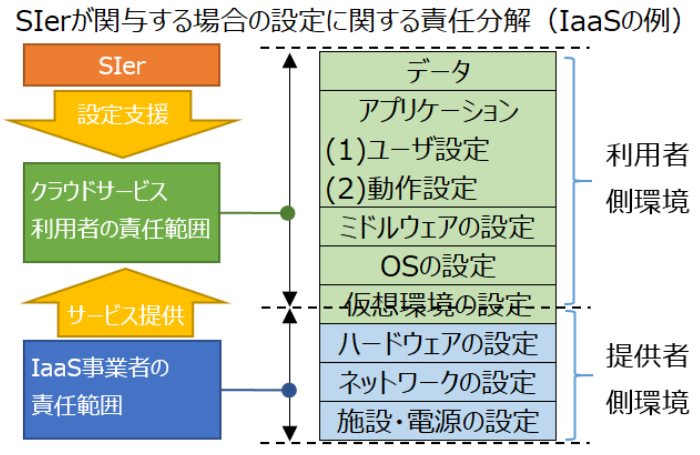


仮想環境の動作に係る設定については、IaaS 事業者が責任を負います。仮想環境を利用するための設定については、クラウドサービス利用者の責任となります。クラウドサービス利用者の役割としては、利用側環境の設定者と設定管理者の両方となります。IaaS 事業者は、提供する仮想環境以下の提供側環境の設定者と設定管理者になります。[2]

4.　IaaS 等の設定を SIer に外部委託する場合

本市において、ほとんどの場合、IaaS や PaaS の利用において、クラウドサービス利用者が動作環境設定等を SIer に外部委託することが想定されます。

これらの作業は、環境の設定支援と位置付けられ、最終責任はクラウドサービス利用者となります。SIer は作業については責任を持ち、正しく環境の設定を行って利用者に引き渡す必要があります。クラウドサービス利用者は発注者としての管理・監督責任があるので、大きな意味では SIer が設定者、クラウドサービス利用者が設定管理者となります。



また、SIer と類似したケースとして、クラウドサービス事業者がクラウドの運用までを含めて受託するマネージドサービス[3]が登場していますが、当該サービスの部分は準委任契約であることが多いので、この場合も設定管理者はクラ

1　一つのコンピュータ上のコンピュータを疑似動作させる環境を「仮想環境」という。この仮想環境上で動いている OS のことをゲスト OS という。

2　仮想ネットワークの設定については利用側の環境となる場合がある。また、クラウドサービスは多様であるため、利用の仕方によっては IaaS に限らず仮想ネットワークが利用側の環境となるケースも考えられる。

3　クラウドサービスの設計・構築、運用管理、保守、障害時の対応といった一連の業務を請け負うアウトソーシングサービス（外部委託）

ウドサービス利用者となります。

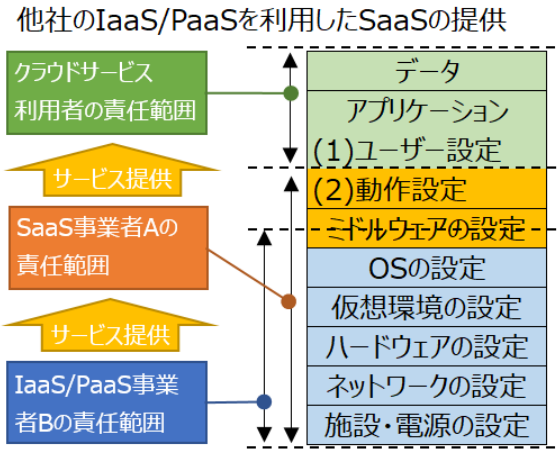
5.　SIer 等が SaaS を提供する場合

クラウドサービスの提供において、SIer 等（販売代理店も含む）が、クラウドサービス事業者とクラウドサービス利用者の間に入る場合があります。この場合、提供形態として様々なパターンがあります。例えば、①SIer 等が SaaS 事業者の代理店として利用契約を代行し、サービスをそのまま若しくはアプリケーションをカスタマイズして SaaS として提供するパターン、②SIer 等は、運用保守等のサポートのみを行い、クラウドサービス利用者はクラウドサービス事業者と直接契約するパターン[4]、③SIer 等がクラウドサービス事業者のサービスをサポートなしで販売するのみのパターンなどです。いずれのパターンにしても、クラウドサービス利用者は、契約締結の前に責任分界、運用上の役割、免責事項などをよく確認して契約を行う必要があります。

6.　SaaS 事業者が他社の IaaS/PaaS を利用してクラウドサービスを提供する場合

最近では、他社の IaaS/PaaS 事業者の環境を利用して自サービスを開発し、SaaS としてクラウドサービス利用者に提供することが多くなっています。

SaaS 事業者 A は、クラウドサービス利用者との契約者であることから、クラウドサービス利用者との契約に基づき、データとアプリケーションユーザ設定を除く、提供するクラウドサービス全体の管理責任を負うことが基本となります。ただし、SaaS 事業者 A にサービスの可用性について免責とする場合があります。そのため、クラウドサービス利用者は、そのサービスが免責とする事項について確認が必要となります。



SaaS 事業者 A と IaaS/PaaS 事業者 B の責任分担についての考え方は、次のとおり。

・SaaS 事業者 A は、IaaS/PaaS 事業者 B との契約に基づき IaaS/PaaS の利用側としての管理責任を負う。

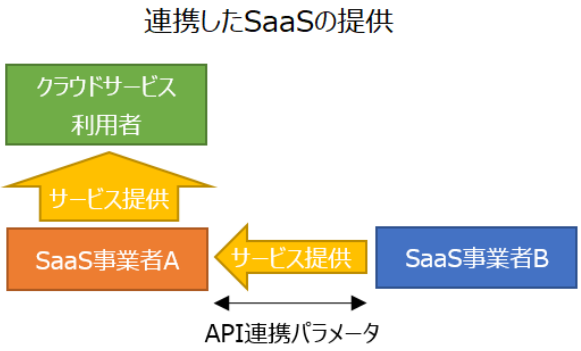
・提供しているクラウドサービスにおいて、IaaS/PaaS 事業者 B の管理範囲に帰する問題が発生した場合は、SaaS 事業者 A と IaaS/PaaS 事業者 B との契約に基づき対処する。

・SaaS 事業者 A は、クラウドサービス利用者との契約者であることから、クラウドサービス利用者との契約に基づき、提供するクラウドサービス全体の管理責任を負う。

7.　連携したクラウドサービスを提供する場合

SaaS 事業者が API（アプリケーション・プログラム・インターフェース）等で水平連携している場合があります。

この場合は、上記に加えて、API の連携パラメータが提供側環境の設定に相当します。API 連携の動作については、SaaS 事業者 A が SaaS 事業者 B との契約に基づいて動作を保証します。利用側環境の設定に関しては、SaaS 事業者 A が用意したGUI（グラフィカル・ユーザ・インターフェース）等で設定するので、クラウドサービス利用者は意識しな



[4] クラウドサービス利用者と SIer には保守契約が締結されていることもある。この場合、両者間の責任分界点は SLA によって決まることが多いので、その内容をよく吟味することが重要である。

いことが多いですが、クラウドサービスが連携していることを知っておくことにより、何らかの障害が発生した場合、API のパラメータの受け渡しが正常稼動していないことなどを推測できます。

SaaS 事業者 A と SaaS 事業者 B の責任分担についての考え方は、次のとおり。

・SaaS 事業者 A は、SaaS 事業者 B のとの契約に基づき、API 連携を通じて受ける SaaS サービス利用者としての管理責任を負う。

・提供しているクラウドサービスにおいて、SaaS 事業者 B の管理範囲に帰する問題が発生した場合は、SaaS 事業者 A と SaaS 事業者 B との契約に基づき、対処する。

・SaaS 事業者 A は、クラウドサービス利用者との契約者であることから、クラウドサービス利用者との契約に基づき、提供するクラウドサービス全体の管理責任を負う。

SaaS 事業者 B は、API 連携を通じて提供する SaaS サービスが正しく動作するための提供側環境に責任があり、パラメータの仕様に変更があれば、SaaS 事業者 A に遅滞なく伝える責任があります（ただし、Google が公開している API 等契約関係がないものあります）。SaaS 事業者 A は、クラウドサービス利用者が登録したデータについて、API に正しく設定し、SaaS 事業者 B に受け渡す責任があります。

３．　クラウドサービス利用側に求められる対策

利用側での対策について下記のような大項目にまとめられます。

【組織体制・人材育成】

組織におけるセキュリティ管理者やクラウドサービス管理者が実施すべき事項として、方針・ガバナンス、技術情報の収集、人材育成及びコミュニケーションに対する対策

【作業規則・マニュアル】

実際に環境の設定に係る、設定者及び設定管理者が実施すべき事項として、作業手順やマニュアルに関する対策

【システム動作環境における設定管理】

クラウドサービス利用者すべてが知っておくべきクラウドシステムの環境そのものについて、クラウドに関する設定項目の類型とクラウドシステムの機能追加などの環境変化に追随するための対策

【システム動作環境の設定の方法論】

環境の設定に対するやり方を工夫すべき点として、ノウハウの蓄積、動作環境設定の自動化や支援ツール等の利用、定期的なチェックなどの監査方法についての対策

１．　クラウドサービス設定不備の抑止・防止に係る方針的事項

クラウドサービス利用における設定不備の抑止・防止のための組織的方針を明確にします。

（1）クラウドサービス利用におけるガバナンスの確保

利用者は、当該利用部門内における組織全体での基本的な方針、役割、責任等を定めた文書（例えばクラウドサービス利用方針等）に設定不備対策を追記し、組織長の承認及び署名等を経て、組織内及び関係する組織に配布します。

文書への推奨記載内容は次のとおり。

①組織のクラウドサービス利用について、安全性を確保するためにセキュリティ担当などの管理部門を設置、整備する。

②利用者組織のセキュリティポリシー及びクラウドのセキュリティ規格に準拠したルールの作成。ルールの作成時には、「大阪市セキュリティ対策基準」等のポリシーへの準拠と、「クラウドのセキュリティ規格」（ISO、NIST 等）への準拠に留意する。

③設定不備の発見に寄与する内部監査基準を整備する。

④定期的なシステムのチェックや内部監査を実施する。

⑥クラウドサービス利用におけるシステムリスク評価と業務継続計画を作成する。

⑦クラウドサービス事業者との利用契約における免責事項を確認する。

⑧ユーザ ID などの設定項目については、失効管理にも注意を要する。

⑨バックアップ機能の有無を確認し、無い場合は、職員運用によるバックアップ取得を実施する。

2.　人材育成

クラウドサービスの設定における知識とノウハウの蓄積、利用におけるリテラシーの向上を確実にします。

（1）クラウドサービス利用におけるリテラシーの向上

利用側環境の設定不備によってどのようなリスクが生まれるのか、また、実際にどのようなインシデントを引き起こすリスクがあるのかについて組織のクラウドサービス利用者に周知します。

（2）クラウドシステム動作環境設定における技術力向上

クラウドシステムにおける動作環境の設定（以下、システム動作環境と略す）についての技術力を継続的に向上させます。また、組織の育成計画に従った施策の実施と実施状況を元にした改善のサイクルを回します。

3.　コミュニケーション

コミュニケーションの基本である利害関係者との窓口の明確化、定期的な情報交換、クラウドの利用に係る責任分担及びセキュリティに係る設定値の扱いなどコミュニケーションルート及びコミュニケーション方法などを確立すること。

（1）コミュニケーション

コミュニケーションの基本である利害関係者との窓口の明確化、定期的な情報交換、クラウドの利用に係る責任分担及びセキュリティに係る設定値の扱いなどのコミュニケーションルート及びコミュニケーション方法等を確立します。

【クラウドサービス利用者】

①クラウドサービス事業者の仕様変更や新機能のリリースのタイミングで利害関係者と協議する。

②SIer 等に委託している場合は、セキュリティ事故を起こさないための設定について責任分担やデフォルト値の設定変更の有無などについて説明を聞く。

③設定不備に起因するトラブルやインシデント等については、その事象及び対処について記録に残し、クラウドサービス提供者側と共有する。

④利用するクラウドサービスの信頼できるユーザーコミュニティがある場合、最新のサービスのリリースやトラブル対応等について相談し、内容を精査した上で参考とする。

【SIer】

⑤利用者にクラウドサービス事業者の仕様変更や新機能のリリースのタイミングを伝え、対応について協議する。

⑥セキュリティ上の問題がある場合には、クラウドサービス事業者からの技術支援体制の構築や定期的な会議

の実施を検討する。

【SaaS 事業者】

⑦利用している IaaS/PaaS とののサポート体制や技術支援などのコミュニケーションルートを確立する。

4.　作業規則やマニュアルの整備

組織の指針に沿った、クラウドシステムにおける動作環境の設定についての作業規則を確立します。また、作業手順やマニュアルを確実に整備します。

（1）作業規則の整備

設定不備を防ぐため、組織の指針に沿った作業規則を整備します。作業規則は、クラウドサービス利用者組織の管理部門が行う動作環境の設定だけでなく、利用所管等がクラウドサービスを利用する場合も含め周知・徹底させます。

（2）作業手順書の整備

システム動作環境の設定における設定不備を防ぐため、作業手順書を整備します。整備においては、クラウドサービス事業者が用意するマニュアルやリリースノート等の意味、内容を正確に理解したうえで、手順を組み立ててください。また、利用するクラウドサービスにおいてデフォルト値のままであるとセキュリティが弱い設定について、把握・レビューし、作業手順書に組み込みます。

（3）ヒューマンエラー対策

作業手順書に設定者及び設定管理者によるダブルチェック等のヒューマンエラー対策を確実に組み込みます。なお、作業手順書はチェックリスト形式とし、設定者及び設定管理者の証跡を残すことを作業手順に組み込んでください。

（4）作業手順書に係るマネジメント

作業手順書の定期的な見直し等をマネジメント体制に確実に組み込みます。

5.　クラウドサービスにおけるシステム動作環境の設定管理

（1）クラウドセキュリティに係る設定項目の確認

クラウドにおけるシステム動作環境の設定において、セキュリティに係る設定項目を確実に確認します。典型的なクラウドの設定項目について理解し、利用する IaaS/PaaS の設定項目を把握した上で設定してください。（クラウドサービスの設定について SIer が支援する場合は、双方において良く確認を行うこと）

①設定項目の洗い出し、チェックリスト作成、レビュー等に活用する。

②クラウドサービス利用者が SIer 等の設定者との環境の設定項目に関する調整に活用する。

③ユーザアカウントの管理においては、パスワード設定の厳格化や多要素認証の設定を行う。

④管理者や特権アカウントの管理においては、【1】多要素認証、【2】複数人でのチェック体制をとる。

⑤管理者や特権アカウントについては、認証、アクセスログ及び設定変更等のログ監視を行う。

⑥特権アカウント利用者や特権昇格可能なアカウントは、最小限とすることが望ましい。

クラウドにおけるセキュリティ設定項目の類型と対策

No.	セキュリティ設定項目の類型	類型項目における推奨設定の概要
1	ID とアクセス管理（IAM）	ID とアクセス管理とは、「誰が」「どのリソースに対し」「どのような操作ができるか」を定義し、アクセス制御を実現するために提供されているサービスである。 管理者はクラウド全体のセキュリティに関与するため、管理者アカウントとユーザアカウントを分離し、管理者アカウントには多要素認証を必須にする等の設定を確実に行うほか、組織の要件に応じてユーザアカウントの IP アドレス制限など各種設定を確実に行う必要がある。特にゲストユーザーについては、不要な情報公開を避けるため、必要最小限の権限とする。また、暗号化キーは統合管理サービスで集中管理することを推奨する。なお、管理者が ID とアカウントを網羅的に把握する仕組み（申請ベースで中央での払い出し、新規アカウントの個別発行不可等）を設ける必要がある。
2	ロギングとモニタリング	ロギングは、クラウドにおける挙動やアラート発報の基本となるものである。デフォルトでは、アクティブになっていないサービスもあるので、適切にロギング設定を行い、アラートや監査を行えるようにしておく必要がある。
3	オブジェクトストレージ	クラウド利用におけるオブジェクトストレージのセキュリティでは、データの外部漏えいに備えて暗号化等が基本となるが、暗号化キーの管理方法なども重要となる。また、オブジェクトストレージの公開設定などデフォルト値も確認しておく必要がある。
4	インフラ管理	
4.1	仮想マシン（VM,VPS）	物理サーバを論理的に分離する仮想マシンを利用する際、仮想マシンのディスク暗号化、エンドポイント保護などの設定を確実に行う必要がある。また、ホスト OS、ゲスト OS 等の最新パッチ、ウイルス対策（AV、 EDR 等）の設定及びその監視・運用（MDR、SOC 等）についても留意する必要がある。
4.2	ネットワーク	クラウド利用は、インターネット経由となるため、外部ネットワークとのアクセスに関する基本的なセキュリティ設定、仮想プライベートクラウドのセキュリティ設定、Firewall/IPS/IDS や WAF などによる境界防護および境界内防護等に関する設定を確実に行う必要がある。加えて、重要情報を扱うシステムでは、信頼できる VPN による通信の暗号化などのネットワークセキュリティ対策を検討する。
5	セキュリティ等の集中管理	IaaS/PaaS が提供するセキュリティ集中管理機能、キーマネジメントサービス、運用管理コンソール、監査ツール、コスト管理サービスなど、構成管理を横断的に集中管理可能なツールやサービスを積極的に利用することを推奨する。これらはデフォルトでは有効化されていない場合があるため、有効化のための設定確認を推奨する。
6	IaaS／PaaS が提供する、その他のサービスや機能 ※短期間に新たなサービスや機能が追加されることがあるため、下記の項目以外にも追加された時点で、設定値についても確認を行う必要がある。	
6.1	鍵管理	鍵管理は安全に秘密鍵を管理・作成・制御する方法を提供する。暗号化鍵の管理に係る設定については、ID とアクセス管理、ロギングとモニタリング等とも関連し、集中管理するサービスを提供するクラウドもある。使用するクラウドに応じた適切な設定を行う必要がある。
6.2	PaaS が提供するア	クラウドで提供されるアプリケーションには様々なものがあるが、個々の事

	プリケーション	業者から提示されるアクセス許可などの設定やデフォルトの公開範囲等の設定を確実に行う必要がある。
6.3	データベース	クラウドで使用するデータベースの保護、監査、暗号化などの設定及びデフォルト設定値の確認を確実に行う必要がある。
6.4	コンテナ	コンテナとは、ホスト OS 上で「コンテナエンジン」と呼ばれるシステムを動作させ、「コンテナ」と呼ばれる実行環境を複数構築する技術である。コンテナを利用する際は、コンテナエンジンに係るセキュリティ関連の設定を確実に行う必要がある。
7	その他の設定項目	上記以外のクラウドサービス事業者が提供する統合資産管理、モバイルデバイス管理等のサービス等については、個々の事業者から提示されるセキュリティ設定を確実に行う必要がある。また、これらはデフォルトでは起動していないことが多いので、起動のための設定値を確認することを推奨する。

（2）設定項目の管理

設定項目の管理の仕組みとして、設定不備のリスクを顕在化させないための措置（予防的措置）と顕在化しても即時に対応できる措置（発見的措置）を実施できる体制を構築します。

①管理については、サードパーティやクラウドサービス事業者から提供される設定項目の可視化ツール等を利用する。

②初期の設定だけでなく、設定値の監視の仕組み等を構築する。（予防的措置）

③外部の設定値診断サービス等を活用して定期的に設定値の診断を行う。（予防的措置）

④設定が変更されたことが検知されたら、なるべく早く適正な設定値に戻す、又は自動で復元する仕組みを組み込んでおく。（発見的措置）

【IaaS/PaaS を利用している場合】

⑤侵害テスト（ペネトレーションテスト）により、リスクのある設定不備を検出する。（発見的措置）

6.　クラウドシステムにおける動作環境のプロビジョニング

プロビジョニングとは、一般に、システムの環境変化に応じてネットワークやコンピュータなどの設備を予測し、需要に合わせて事前に用意することを言います。このプロビジョニングに当たっても、環境の設定について同様な対応が必要です。また、 IaaS/PaaS の仕様変更や機能追加等により、デフォルトで権限が広がる等の変更が含まれる場合があります。システムの環境変化に合わせて環境の設定項目についても事前に準備することが必要です。

（1）変化への適応及び体制整備

クラウドシステムの環境の変化に対し、準備し対応します。

①クラウドサービス事業者からのリリースノートに基づく設定値の見直しを行う。

②クラウドシステムの環境の変化についてクラウドサービスを使用している事業部門等へ周知する。

③日々変化するクラウドサービスについて情報収集し対応策を検討できる体制を整備する。

④システムの設定値を組み込んだ基盤ソフトのインストールやアプリケーションのシステムへの展開に関してはクラウドサービス事業者が用意するツールやサードパーティーツールを利用すると素早く対応可能となる。

7.　　その他のリスクへの対応

環境の設定におけるその他のリスクへの対応を確実に行います。

（1）システム動作環境の設定に関連するその他のリスク対応

クラウド運用時の設定値に関連するその他のリスク対応について明確にし、対応方針を文書化します。

①リスクマネジメントを導入し、リスク対応項目について設定値に反映する。

②設定不備に起因するトラブルやインシデント等については、その事象及び対処について記録に残し、クラウドサービス提供者側と共有する。

③情報流出に備え、業務要件に応じて暗号化設定等を必須化することを検討する。

④クラウド利用コストの計画と管理について明確化し、課金管理等の設定に反映する。

⑤OSS（Open Source Software）の利用に関しては、IaaS/PaaS ベンダーが一部運用を代行するサービスから可能な限り選択して利用する。海外企業が提供するクラウドサービスの利用に当たり、利用規約等を確認して、準拠法が国内か外国かを必ず確認する。IaaS/PaaS によっては、初期状態で外国になっており、準拠法を国内としたい場合には、環境の設定で変更が必要なものがある。

⑥データセンタが海外に置かれる場合は、外国の法律などの適用を受ける可能性がある。特に機密性の高いデータを扱う場合は、データセンタ所在国、所在地域及び運用体制などを確認する。

８.　ノウハウの蓄積

システム動作環境は常に変化することを前提として、設定方法についてのノウハウを着実に蓄積します。

（１）クラウドシステム動作環境設定に関するノウハウの蓄積

クラウドシステムにおける動作環境の設定方法について、組織のノウハウとして蓄積することを定めて文書化します。

【クラウドサービス利用者】

①環境の設定に関するノウハウの属人化を回避するため、共有・蓄積方法をマニュアル化する。

②組織としてノウハウを管理・共有するためのツールを導入する。

③運用の初期においては、本市のセキュリティポリシーにあっているか確認したうえで、外部等のマネージドサービスを利用しノウハウに関する情報を収集することを推奨する。

④クラウドシステムの設定項目について、外部診断サービスで診断しフィードバックを蓄積する。

【SIer、SaaS 事業者（他社の IaaS/PaaS 利用）】

⑤組織として、次のようなノウハウについての蓄積を推進する。

・設定項目変更の自動検知と自動復旧の仕組み

・開発/検証/本番環境の用意、本番環境への展開の手法

・異常系テストや不安定動作への対応手法

・動作確認の際の支援ツール利用、定期監視

９.　定期的な設定のチェックと対応

システム動作環境の設定に関する定期的なチェックと対処を実施し、必要に応じて組織の内部基準に基づく監査を実施し、適切に対応します。

（１）システム動作環境の設定に関する定期的なチェックと対応

システム動作環境の設定項目の保全のため、定期的なチェックと対処を実施し、必要に応じて組織の内部基準に基づく監査を実施し、適切に対応します。

①組織としての管理の枠組みを構築し、定期的にチェックし、不備がある場合は対処する。

②必要に応じて組織の内部基準に基づく内部監査等を行い、組織的な不備がある場合は教訓事項としてノウハウの蓄積を行う。

③定期的なチェックや内部監査等にツールを使用し効率化を行う。

④定期的にシステム動作環境の設定値について外部診断サービス等を受ける。

⑤クラウドサービスの機能追加や仕様変更に対しては定期的ではなく特別に注意してチェック及び対応を行う。

第 5 章 クラウドサービス関連ガイドライン

参考ガイドライン

1.　参考ガイドライン

1.　本ガイドラインを作成するにあたって参考としたガイドライン

本ガイドラインを作成するにあたって参考としたガイドラインは次のものです。必要に応じて参照してください。

No	資料名	発行者	発行・改定年度
1	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	デジタル社会推進会議幹事会	令和4年度
2	デジタル・ガバメント推進標準ガイドライン	デジタル社会推進会議幹事会	令和4年度
3	デジタル・ガバメント推進標準ガイドライン解説書	デジタル庁	令和4年度
4	総合行政ネットワーク ASP ガイドライン	地方公共団体情報システム機構	令和元年度
5	地方公共団体における情報セキュリティポリシーに関するガイドライン	総務省	令和4年度
6	クラウドサービス提供における情報セキュリティ対策ガイドライン（第3版）	総務省	令和3年度
7	エンタープライズクラウド選定ガイド　クラウド選びで困ったら～要求仕様作成と提案書評価のための基礎知識～	JASA-クラウドセキュリティ推進協議会	平成 27 年度
8	政府機関等の情報セキュリティ対策のための統一基準群	内閣サイバーセキュリティセンター（NISC）	令和5年度
9	クラウドサービスの安全性評価に関する検討会　とりまとめ	クラウドサービスの安全性評価に関する検討会	令和元年度
10	政府情報システムのためのセキュリティ評価制度（ISMAP)について	NISC・デジタル庁・総務省・経済産業省	令和5年度
11	クラウドを利用したシステムに関するガイダンス	内閣サイバーセキュリティセンター（NISC）	令和4年度