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。

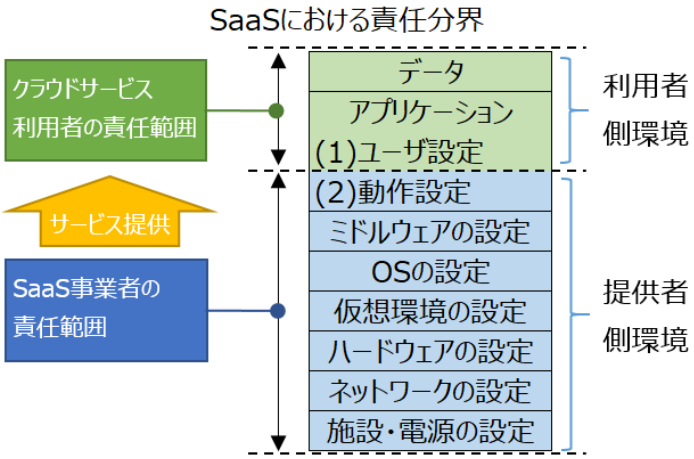
なお、本章内容は 2022 年 10 月総務省発行の「クラウドサービス利用・提供における適切な設定のためのガイドライン」を本市向けに編集したものです。

2.　責任分界

1.　SaaS の設定に関する責任分界

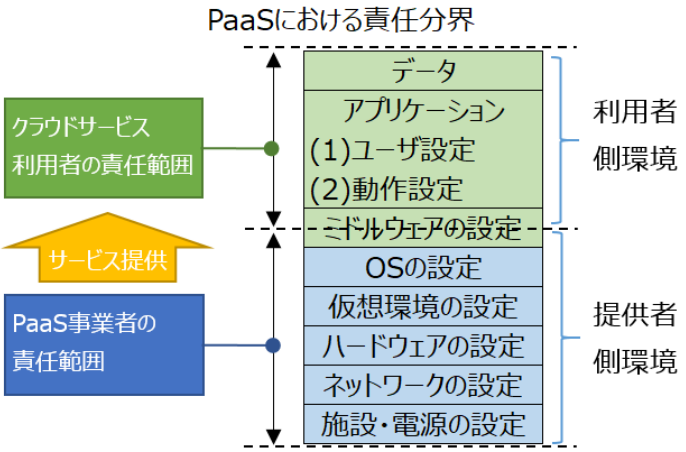
SaaS を利用する場合、右図に示すとおり、クラウドサービス利用者が責任を負う部分は、データとアプリケーションの管理の一部となります。アプリケーションの動作に係る設定は SaaS 事業者が責任を負う一方、利用者アカウントや業務データの設定については、クラウドサービス利用者の責任となります。

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

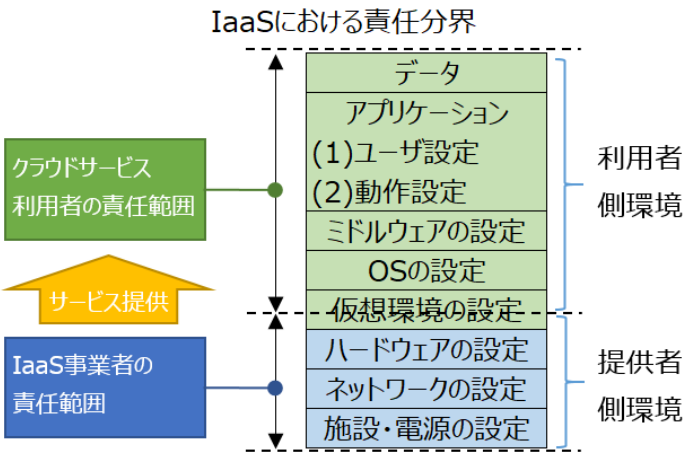


す。また、クラウドサービス利用者はクラウドサービス事業者が提供するプログラミング環境やSQL等のユーティリティインターフェースを利用してミドルウェア層を利用します（クラウドサービス事業者によっては、完全にユーザが責任を持って利用することが前提で用意されているミドルウェアもあります。）。

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。

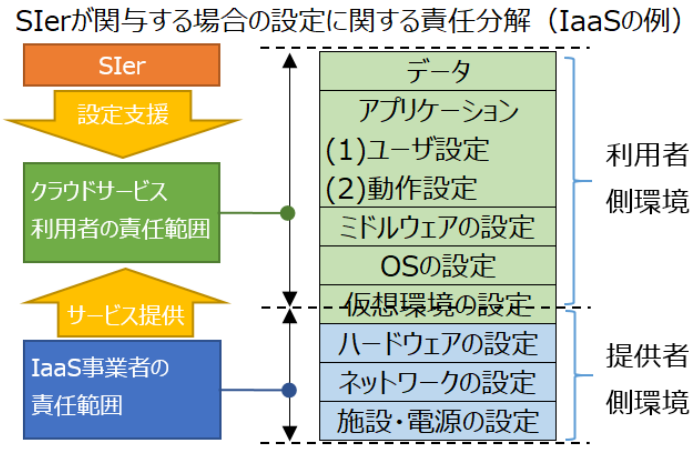


仮想環境の動作に係る設定については、IaaS 事業者が責任を負います。仮想環境を利用するための設定については、クラウドサービス利用者の責任となります。クラウドサービス利用者の役割としては、利用側環境の設定者と設定管理者の両方となります。IaaS 事業者は、提供する仮想環境以下の提供側環境の設定者と設定管理者になります。[2]

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。

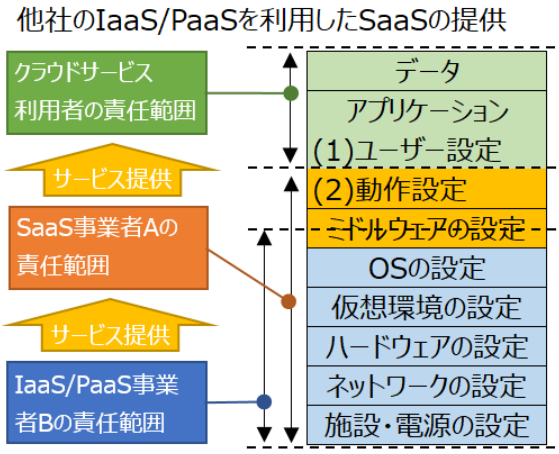
5.　SIer 等が SaaS を提供する場合

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。

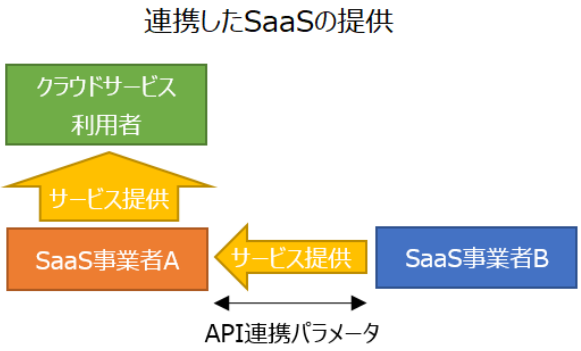
・提供しているクラウドサービスにおいて、IaaS/PaaS 事業者 B の管理範囲に帰する問題が発生した場合は、SaaS 事業者 A と IaaS/PaaS 事業者 B との契約に基づき対処する。

・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。