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

２０２２年 10月

総務省

(This page is intentionally left blank.)

本ガイドラインの要旨

ここ数年、クラウドサービスを利用する事業者において、設定不備による顧客の個人情報の流失のおそれに至る事案が増加しており、クラウドサービスの利用におけるリスクとして社会的に問題となっている。また、独立行政法人情報処理推進機構（IPA）の「コンピュータウイルス・不正アクセスの届出状況 2021 年」によると、不正アクセスの原因別比率では、設定不備が全体のおよそ 17.7%で第 3 位となり、このような社会問題を引き起こす原因として無視できなくなっている。

このような設定不備は、直接的にはクラウドサービス利用者による単純なミスによるものと考えることもできる。しかし、これらの事案の真因を考察すると、利用側においては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、提供側においては利用側において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る。

そこで、本ガイドラインで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・提供に資することを目的として、利用者・事業者双方において共通的に認識しておくべき事項及び具体的な対策について整理し、取りまとめた。

クラウドサービスにおける設定不備の抑止・防止に向けた基本的な考え方は、下記の 3 つである。

① クラウドサービス利用者・事業者双方において、クラウドサービスの特性や、クラウドサービスの利用・提供におけるリスクについて認識すること

② クラウドサービス利用者・事業者双方において、自身の責任範囲や役割を理解し、それを共通認識とすること

③ クラウドサービス利用者・事業者間でコミュニケーションを密なものとしつつ、双方における設定不備の抑止・防止の対策を適切に実施すること

これらに資する情報として、本ガイドラインでは「前提および概要」においてクラウドサービスの設定不備のリスクや、クラウドサービスの設定に関する責任共有の考え方、設定不備の要因と対策の概要について記載した。

「クラウドサービス利用側に求められる対策」「クラウドサービス提供側に求められる対策」では、設定不備の抑止・防止のための具体的な対策やベストプラクティスについて記載している。まず「クラウドサービス利用側に求められる対策」では、クラウドサービス利用側における組織体制・人材育成、作業規則やマニュアルの整備、システム動作環境の設定管理、システム動作環境設定の方法論に関する対策を記載した。また、「クラウドサービス提供側に求められる対策」では、クラウドサービス提供側における組織体制や人材育成、提供するサービスの改善等の対策を記載するとともに、利用側に提供すべき情報や学習コンテンツ、学習機会、利用者を支援するツール等に関する対策を記載した。

目次

(This Page is intentionally left blank)

Ⅰ．序編

(This page is intentionally left blank.)

Ⅰ．１　はじめに

クラウドサービスの普及及び高度化に伴い、クラウドサービスは、社会経済活動を支える重要な ICT 基盤となっている。こうした中、多くの自治体や企業が主要なシステムをオンプレミス環境からクラウド環境へ移行している。更に、新型コロナウイルス感染症の感染拡大及びそれに伴う人の移動の制限は、多くのオフィスワーカーをリモートワーカーに変えただけでなく、教育現場における授業形態を対面授業からリモート授業に変えるきっかけともなっている。クラウドサービスは、これらの社会全体のデジタル化において不可欠な前提であり、クラウドサービスが存在しなければ、企業や消費者の新型コロナウイルス感染症の感染拡大への対応は、大きく異なっていたものと思われる。

このようにクラウドサービスが普及する一方で、大規模な情報漏えい等のインシデントが度々発生しており、インシデントの原因の多くを利用者によるクラウドサービスの設定不備が占めている [1]。

このため、クラウドサービスの設定不備に関する要因の考察及び我が国におけるクラウドサービス利用の特性も踏まえて、クラウドサービスの設定不備を発生させないための取組の推進が急務となっている。

現在のクラウドサービス利用・提供におけるガイドライン等の整備の状況としては、利用側に対するものとして、「クラウドを利用したシステム運用に関するガイダンス（詳細版）」（令和３年 11 月　内閣官房内閣サイバーセキュリティセンター）並びに「テレワークセキュリティガイドライン第５版」（令和３年５月　総務省）の「第２章　３．クラウドサービスの活用の考え方」や関連する対策一覧がある。また、提供側に対するものとして、情報セキュリティ対策におけるベースラインとして、「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）」（2021 年９月　総務省）がある。これらのガイドライン等に利用側、提供側における必要なセキュリティ対策が記載されているが、いずれも設定不備の抑止・防止に特化したものとはなっていない。

そこで、本ガイドラインは上記のガイドライン等をベースにしつつ、昨今のインシデントの発生を踏まえて、クラウドの利用場面、提供場面における適切な設定を促進するための対策に焦点を絞ったガイドラインとした。

なお、本ガイドラインは上述のとおり、クラウドサービスの利用・提供におけるクラウドサービスの適切な設定の促進を図り、安全安心なクラウドサービスの利活用を推進していくために推奨されるセキュリティ対策を記載するものであり、何ら法的な拘束力を有するものではなく、また、当事者間における交渉や契約の自由を何ら制約するものではないことを付言する。

[1]「コンピュータウイルス・不正アクセスの届出状況」，2018~2021 年，独立行政法人　情報処理推進機構（https://www.ipa.go.jp/security/outline/todokede-j.html）

Ⅰ．２ ガイドラインの位置付け

本ガイドラインは、クラウドサービス利用において設定不備に起因する情報漏えい等のインシデントを抑止・防止するため、クラウドサービス利用側、提供側それぞれで実施することが望ましい対策について記載している。

我が国におけるクラウドサービスの利用においては、クラウドサービスを利用する企業等の約 60%がクラウドの運用支援の全部又は一部をクラウドサービスの導入・構築・運用を支援するシステム・インテグレーター等（以下、SIer と略す）に委託する形態となっているという特徴がある [2]。また、クラウドサービス利用者や SaaS 事業者は、IaaS/PaaS を利用してサービスを提供することも少なくなく、この場合、クラウドサービスの提供側、利用側の両方の立場を兼ねることになる。

従って、本ガイドラインでは 図表 1.2-1 のとおり、幅広い読者を対象とする。クラウドサービスの利用側は、クラウドサービス利用者、SIer 及び SaaS 事業者（IaaS/PaaS 等を設定して利用する場合）、そして、クラウドサービスの提供側は、SaaS 事業者及び IaaS/PaaS 事業者である。

また、本ガイドライン内ではクラウドサービス利用者に関して、クラウドサービス利用における全社のセキュリティポリシーなどを策定する部門を「セキュリティ管理者」、全社向けのクラウドサービスを提供し運用管理を行う、又は各部門が利用するクラウドサービスの申請を受け、審査・承認を行う部門を「クラウドサービス管理者」、管理者の承認を得て自部門で独自にクラウドサービスを利用する部門を「（狭義の）クラウドサービス利用者」と呼ぶこととする。

本ガイドラインは、クラウドサービスの適切な設定を促進するという趣旨から、個人としてクラウドサービスを利用し設定等を行わないエンドユーザではなく、企業内においてサービス全体の動作に関わる設定を行う者を主たる対象としていることにご留意いただきたい。

[2]「国内クラウドサービス需要動向(2021 年版)」，2021 年 9 月，株式会社 MM 総研
(https://www.m2ri.jp/report/market/detail.html?id=64)

図表Ⅰ.2-1 本ガイドラインの想定読者

名称	定義
① クラウドサービス利用者	クラウドサービス（IaaS/PaaS/SaaS）の利用者。本ガイドライン内ではクラウドサービスを利用する組織内の立場によってさらに以下のような分類を設ける。 ・セキュリティ管理者：クラウドサービス利用における全社のセキュリティポリシーなどを策定する部門 ・クラウドサービス管理者：全社向けのクラウドサービスの運用管理や各部門が利用するクラウドサービスの審査・承認を行う部門 ・（狭義の）クラウドサービス利用者：管理者の承認を得て自部門で独自にクラウドサービスを利用する部門 ※IaaS/PaaS を利用して自社で内製アプリを開発・利用する場合、社内向けの SaaS 提供者の立場にもなる。 ※クラウドサービスを利用するだけで設定等を行わないエンドユーザは、本ガイドラインの対象外。
②SIer	クラウドサービス利用者から委託を受け、クラウドサービスの導入・構築・運用を支援する事業者。クラウドサービスの提供・利用の観点では、クラウドサービス利用者に該当する。（クラウドサービス利用者によるクラウドサービスの適切な利用を支援する位置付け）
③SaaS 事業者	自社で SaaS を開発し、サービスとしてクラウドサービス利用者に提供する事業者。 ※他社の IaaS/PaaS 基盤を利用する場合は、IaaS/PaaS 利用者の立場にもなる。
④IaaS/PaaS 事業者	自社で IaaS/PaaS を開発し、サービスとしてクラウドサービス利用者に提供する事業者。 ※必要に応じて、IaaS 事業者、PaaS 事業者と分けて記述する。

また、本ガイドラインは「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）」をベースとしている。クラウドサービス提供側における、基本的な情報セキュリティ対策については、こちらを参照されたい。

Ⅰ．３ ガイドライン活用の効果

本ガイドラインをそれぞれの読者が活用することで以下の効果が見込まれる。

① クラウドサービス利用者にとっては、自らが適切な設定を実践する際の指針となる。また、利用者組織のクラウドサービス管理者にとっては、事業部門が独自にクラウドサービスを利用する場合の設定不備をなくすための留意事項を示す指針となる。さらに、SIer などに外部委託する際の管理やコミュニケーションのための指針となる。また、SIer においても本ガイドラインを委託元との共通理解の醸成に活用することで、委託元との円滑なコミュニケーションを促進することが可能となる。

② SaaS 事業者にとっては、IaaS/PaaS を利用して自社サービスを展開する際に適切な設定を実践する際の指針となる。また、自ら提供する SaaS の設定項目について提供者側としてどのように利用者へ提示すべきか、設定不備の抑止・防止についてどのような対策を講ずべきかの指針となる。

③ IaaS/PaaS 事業者にとっては、IaaS/PaaS の設定項目について提供者側としてどのように利用者へ提示すべきか、設定不備の抑止・防止についてどのような対策を講ずべきかの指針となる。

Ⅰ．４ ガイドラインの全体構成

本ガイドラインは、「序編」、「前提および概要」、「クラウドサービス利用側に求められる対策」、「クラウドサービス提供側に求められる対策」及び「参考資料（ANNEX）」の５つの部分から構成されている。本ガイドラインの想定読者が、それぞれどの編を読むべきかについては、「Ⅰ．５．ガイドラインの読み方と利用方法」を参照されたい。

Ⅰ．序編

本ガイドラインの目的・位置付け・利用方法、使用している用語の定義等を記載している。

Ⅱ．前提および概要

クラウドサービスの利用側、クラウドサービスの提供側に共通して認識すべき基本的事項、設定不備によるリスク、設定不備の要因と対策等について取りまとめている。

Ⅲ．クラウドサービス利用側に求められる対策

クラウドサービスの利用側における、設定不備の抑止・防止のためのセキュリティ対策を取りまとめている。

Ⅳ．クラウドサービス提供側に求められる対策

クラウドサービスの提供側における、クラウドサービス利用者の設定不備発生の抑止・防止のためのセキュリティ対策を取りまとめている。

ANNEX　対策一覧

クラウドサービス利用側における対策及びクラウドサービス提供側における対策の対策項目について、一覧形式で示している。

Ⅰ．５ ガイドラインの読み方と利用方法

本ガイドラインを基に具体的な設定不備対策を実施する場合は、読み手ごとに、以下の手順に従って利用されることが望ましい。読んでいただきたい箇所の概要を図表Ⅰ． ５－１に示し、詳細を次に記述する。

図表 Ⅰ.５－１主に読んでいただきたい箇所

想定読者		主に読んでいただきたい部分		
分類	小分類	Ⅱ.前提および概要	Ⅲ.クラウドサービス利用側に求められる対策	Ⅳ.クラウドサービス提供側に求められる対策
①クラウドサービス利用者	経営層・セキュリティ管理者	◎	◎	-
	クラウドサービス管理者	◎	◎	-
	（狭義の）クラウドサービス利用者	◎	◎	-
	社内向けクラウドサービス開発者	◎	◎	◎
②SIer	-	◎	◎	-
③SaaS事業者	-	◎	○	◎
④IaaS/PaaS事業者	-	◎	-	◎

※◎:全ての読者が対象 ○：IaaS/PaaSを用いてサービス提供している場合に対象
-：必要に応じて読んでいただきたい部分

■（クラウドサービス利用者の）経営層やセキュリティ管理者等が組織のセキュリティ方針を定める場合

i. 『Ⅰ.序編』を読み、本ガイドラインの位置付け、利用方法、用語の定義等を確認する。

ii. 『Ⅱ.前提および概要』を読み設定不備の対策に関する内容や対策の前提となる事項を確認する。

iii. 『Ⅲ.クラウドサービス利用側に求められる対策』の各節冒頭にある【目的】の内容を把握することで、各設定不備対策の目的を知ることが出来る。

■（クラウドサービス利用者の）経営層やクラウドサービス管理者等がクラウドの利用方針等を定め、運用管理を行う場合

i. 『Ⅰ.序編』を読み、本ガイドラインの位置付け、利用方法、用語の定義等を確認する。
ii. 『Ⅱ.前提および概要』を読み設定不備の対策に関する内容や対策の前提となる事項を確認する。
iii. 『Ⅲ.クラウドサービス利用側に求められる対策』の各節の【基本】、【推奨】について把握することで、自組織に求められる対策をリストアップすることが可能となる。
iv. 上記でリストアップした対策をもとに、自組織のクラウドサービス利用方針及び運用管理基準等を策定する。対策を実施する際には、ベストプラクティスを参照すると良い。また、実施に当たっては、「基本」の対策から優先的に実施し、さらに「推奨」の対策を実施することが望ましい。

■（クラウドサービス利用者の）事業部門において、管理者の承認を得て独自にクラウドサービスを利用する場合

i. 『Ⅰ.序編』を読み、本ガイドラインの位置付け、利用方法、用語の定義等を確認する。
ii. 『Ⅱ.前提および概要』を読み設定不備の対策に関する内容や対策の前提となる事項を確認する。
iii. 『Ⅲ.クラウドサービス利用側に求められる対策』の各節の【基本】、【推奨】について把握することで、自部門に求められる対策をリストアップすることが可能となる。
iv. 管理者が策定した自組織のクラウドサービス利用方針、セキュリティ方針等に基づいて、上記でリストアップした対策を実施する。対策を実施する際には、ベストプラクティスを参照すると良い。また、実施に当たっては、「基本」の対策から優先的に実施し、さらに「推奨」の対策を実施することが望ましい。

■（クラウドサービス利用者が）自らクラウドサービスを自社内に提供する場合

i. 『Ⅰ.序編』を読み、本ガイドラインの位置付け、利用方法、用語の定義等を確認する。
ii. 『Ⅱ.前提および概要』を読み設定不備の対策に関する内容や対策の前提となる事項を確認する。
iii. 『Ⅲ.クラウドサービス利用側に求められる対策』及び『Ⅳ.クラウドサービス提供側に求められる対策』の各節の【基本】、【推奨】について把握することで、自組織に求められる対策をリストアップすることが可能となる。

iv. 上記でリストアップした対策を実施する。対策を実施する際には、ベストプラクティスを参照すると良い。また、実施に当たっては、「基本」の対策から優先的に実施し、さらに「推奨」の対策を実施することが望ましい。

■SIerの場合

i. 『Ⅰ.序編』を読み、本ガイドラインの位置付け、利用方法、用語の定義等を確認する。

ii. 『Ⅱ.前提および概要』を読み設定不備の対策に関する内容や対策の前提となる事項を確認する。顧客の設定不備対策について共通の理解を得ることが可能となる。

iii. 『Ⅲ.クラウドサービス利用側に求められる対策』の各節の【基本】、【推奨】について把握することで、設定不備の抑止・防止に関する顧客の要求事項を確認し、理解する等のコミュニケーションに利用することが可能となる。

iv. 顧客と共に選択した、『Ⅲ.クラウドサービス利用側に求められる対策』の各節の対策を実施する。対策を実施する際には、ベストプラクティスを参照すると良い。

■SaaS事業者の場合

i. 『Ⅰ.序編』を読み、本ガイドラインの位置付け、利用方法、用語の定義等を確認する。

ii. 『Ⅱ.前提および概要』を読み設定不備の対策に関する内容や対策の前提となる事項を確認する。

iii. 『Ⅳ.クラウドサービス提供側に求められる対策』の各節の【基本】、【推奨】について把握することで、自社サービスにもとめられる対策をリストアップすることが可能となる。

iv. 上記でリストアップした対策を実施する。対策を実施する際には、ベストプラクティスを参照すると良い。また、実施に当たっては、「基本」の対策から優先的に実施し、さらに「推奨」の対策を実施することが望ましい。

※他社PaaSを利用してサービスを提供する場合、上記に加えて、

v. 『Ⅲ.クラウドサービス利用側に求められる対策』の各節の【基本】、【推奨】について把握することで、自社サービスにもとめられる対策をリストアップすることが可能となる。

vi. 上記でリストアップした対策を実施する。対策を実施する際には、ベストプラクティスを参照すると良い。また、実施に当たっては、「基本」の対策から優先的に実施し、さらに「推奨」の対策を実施することが望ましい。

■IaaS/PaaS事業者の場合

i. 『Ⅰ.序編』を読み、本ガイドラインの位置付け、利用方法、用語の定義等を確認する。

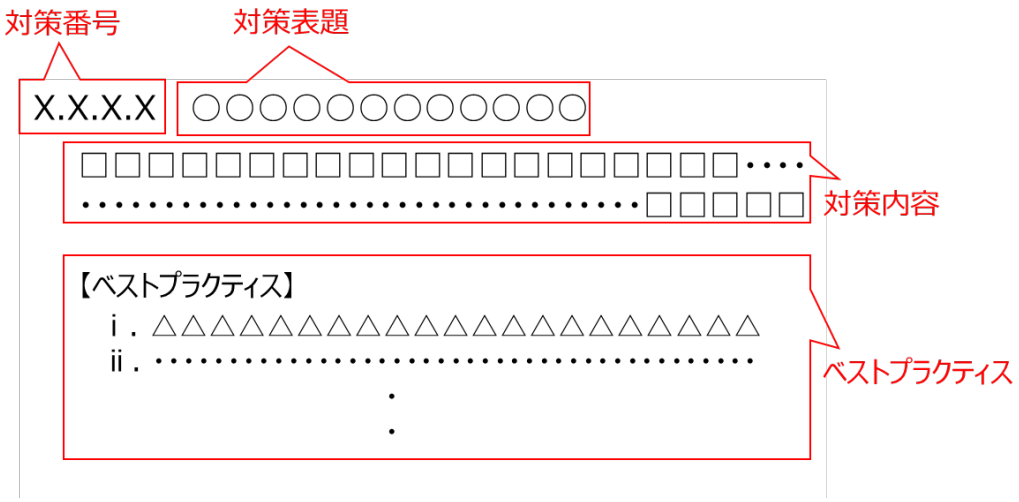
ii. 『Ⅱ.前提および概要』を読み基本事項を確認する。

iii. 『Ⅲ.クラウドサービス提供側に求められる対策』の各節の【基本】、【推奨】について把握することで、自社サービスに求められる対策をリストアップすることが可能となる。

iv. 上記でリストアップした対策を実施する。対策を実施する際には、ベストプラクティスを参照すると良い。また、実施に当たっては、「基本」の対策から優先的に実施し、さらに「推奨」の対策を実施することが望ましい。

本ガイドラインの利用において、凡例とそれぞれの意味を次に示す。図表Ⅰ.5-2の記載凡例で示すように、対策内容を記載している。また、必要に応じて【ベストプラクティス】を付記している。なお、ベストプラクティスは、優先度の高い順で記載している。

図表Ⅰ.5-2 記載凡例



それぞれの意味は、以下のとおりである。

1. 対策番号

各対策表題に対して一意に割り振られた番号

2. 対策表題

設定不備の抑止・防止のために実施すべき事項として、指標となるもの。

※対策表題の「基本」・「推奨」

「基本」：どのようなクラウドサービスでも基本的に実施することが求められる、ベースラインとも言うべき設定不備対策。

「推奨」：クラウドサービスでは、セキュリティ特性として、高い「機密性」「可用性」「完全性」が求められるサービスがある。このようなサービスでは、「基本」対策に加え、「推奨」で示すより高度な設定不備対策を実施することが望ましい。

３．対策内容

対策表題で示した事項について、クラウドサービス事業者やクラウドサービス利用者が実施すべき対策を述べたもの。

４．ベストプラクティス

対策内容に示した対策を実施するに当たって、参考となる具体的な実施手法や注意すべき点をとりまとめたもの。

Ⅰ．６ 用語の定義

アカウント

クラウドのシステムにアクセスする際のアクセス資格。

アクセス制御(JIS Q 27000 を基に定義)

資産へのアクセスが、事業上及びセキュリティ要求事項に基づいて認可及び制限されることを確実にする手段。

暗号鍵

暗号アルゴリズムの手順を制御するためのパラメータを構成するビット列、整数又は文字列。

オブジェクトストレージ

データをオブジェクト単位で扱うストレージ（記憶装置等）のアーキテクチャ。

外部ネットワーク

情報処理施設とその外部とを結ぶネットワークの総称で、クラウドサービス事業者とISP（インターネットサービスプロバイダ） 間、クラウドサービス事業者とサプライチェーン事業者間、クラウドサービス事業者の保守管理用回線等を指す。本ガイドラインの対象外である、利用者が契約する通信回線及びインターネット・サービスは除く。

仮想マシン

ホストOS上などで動作する仮想的なコンピュータ。

鍵管理

暗号鍵の管理又はその機構。

可用性(JIS Q 27000 を基に定義)

認可されたエンティティが要求したときに、アクセス及び使用が可能である特性。

完全性(JIS Q 27000 を基に定義)

正確さ及び完全さの特性。

機密性(JIS Q 27000 を基に定義)

認可されていない個人、エンティティ又はプロセスに対して、情報を使用不可又は非公開にする特性。

脅威(JIS Q 27000 を基に定義)

システム又は組織に損害を与える可能性がある、望ましくないインシデントの潜在的な原因。

クラウドサービス

クラウドコンピューティングが提供するサービス。SaaS/PaaS/IaaSのサービスモデルがある。

クラウドサービス事業者又は提供者

クラウドサービスをクラウドサービス利用者に提供する組織。クラウドサービスを提供するため、他の提供者からクラウドサービスの提供を受けて活用したり、他の提供者とデータ連携等を行うこともある。

クラウドサービス利用者

クラウドサービスを利用する法人又は個人。

構成要素

クラウドサービスの提供に用いるハードウェア、ソフトウェア、通信機器・回線、建物等の固定資産。

コンテナ

実行中OSの一部を分離してソフトウェアを動作させるコンテナ技術において、他と隔離された専用の領域。

サプライチェーン

クラウドサービス事業者と提供者、並びに提供者間において、データ、サービス等で連携してクラウドサービスを提供する際に構築される、各クラウドサービス事業者の情報処理施設がネットワークで連結された形態。

サプライチェーン事業者

サプライチェーンを構成する事業者。

システム動作環境

クラウドサービス利用側環境、提供側環境に関わらず、システム（基盤からアプリケーションまで含む）の動作を規定する環境。

情報開示

電子メール、電子ファイル、FAX、紙文書等の手段による、クラウドサービス利用者に対する情報の引き渡し。

情報セキュリティ(JIS Q 27000 を基に定義)

情報の機密性、完全性及び可用性を維持すること。さらに、真正性、責任追跡性、否認防止及び信頼性のような特性を維持することを含めてもよい。

情報セキュリティインシデント(JIS Q 27000 を基に定義)

望ましくない単独若しくは一連の情報セキュリティ事象、又は予期しない単独若しくは一連の情報セキュリティ事象であって、事業運営を危うくする確率及び情報セキュリティを脅

かす確率が高いもの。

情報提供

情報公開又は情報開示の実施。

ぜい弱性(JIS Q 27000 を基に定義)

脅威によって悪用される可能性がある欠陥や仕様上の問題。

セキュリティ特性

情報の機密性、完全性及び可用性のこと。他に真正性、責任追跡性、否認防止及び信頼性のような特性を含めることもある。

設定項目

システムのハードウェアコンポーネント、ソフトウェアコンポーネント又はファームウェアコンポーネントの値を変更できるパラメータ。

設定者

クラウドサービス利用側環境、提供側環境に関わらず、環境の設定を直接実施する者。

設定管理者

最終的な設定の確認を行い、また、正常な設定の維持に責任を持つ者。

多要素認証

2つ以上の異なる要素の組合せにより、強度を高める認証方式。要素は以下の3種類。

・利用者が知っている情報（例：ID・パスワードなど）

・利用者が所持している情報（例：ICカードなど）

・利用者自身の情報（例：生体情報）

特権アカウント

特権的な管理ツールの使用を許可された個人のアカウント。クラウドサービス事業者とクラウドサービス利用者のどちらに所属するかは問わない。

認証情報

パスワードや暗号鍵のこと。

プロビジョニング

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。

ペネトレーションテスト

インターネットに接続されているコンピュータシステムのセキュリティレベルをチェックするため

に、意図的にサイバー攻撃を実施して、システムに侵入することが出来るぜい弱性がないか確認するテスト。

マネージドサービス

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）。

マルウェア

コンピュータウイルス、ワーム、トロイの木馬、スパイウェアなどの不正かつ有害な動作を行う意図で作成された悪意のあるソフトウェアの総称。

リスク(JIS Q 27000 を基に定義)

目的に対して不確かさが与える影響。（事象の発生確率と事象の結果との組合せ）

ロギング

クラウドサービスにおけるハードウェア、ソフトウェア、ネットワーク等、構成要素の操作記録・通信記録・稼働記録などを取ること。

ASP（Application Service Provider）

本ガイドラインでは、SaaSと同定義とする。それに伴い、「ASP/SaaS」という表現を「SaaS」に統一する。

IaaS（Infrastructure as a Service）

サービスの形で提供されるインフラストラクチャ。IaaS事業者は、演算機能、ストレージ、ネットワーク他の基礎的コンピューティングリソースを配置し、クラウドサービス利用者に提供する。

IDとアクセス管理（IAM:Identity and Access Management）

クラウドサービスを使用する個人の識別と認証、アクセス権限の管理のこと。

PaaS（Platform as a Service）

サービスの形で提供されるプラッフォーム。PaaS事業者は、クラウドのインフラストラクチャ上で、アプリケーションを開発、実装、稼働できるようにするために、ミドルウェア等を提供する。

SaaS（Software as a Service）

サービスの形で提供されるソフトウェア。SaaS事業者は、クラウドのインフラストラクチャ上で稼働するアプリケーションをクラウドサービス利用者に提供する。

SLA（Service Level Agreement）

書面にしたサービス提供者と顧客との合意であって、サービス及び合意したサービスレベルを記載したもの（JIS Q 20000-1:2007）。

Ⅰ．７ 参考文献

- 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）
  2021 年 9 月　総務省
- クラウドを利用したシステム運用に関するガイダンス（詳細版）
  2021 年 11 月 30 日　内閣官房内閣サイバーセキュリティセンター
- テレワークセキュリティガイドライン第 5 版
  2021 年 5 月、総務省
- CIS Benchmarks[3]　Center for Internet Security®
- JIS Q 27000:2019 (ISO/IEC 27000:2019)
  「情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－用語」
- JIS Q 27001:2014 (ISO/IEC 27001:2013)
  「情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－要求事項」
- JIS Q 27002:2014 (ISO/IEC 27002:2013)
  「情報技術－セキュリティ技術－情報セキュリティ管理策の実践のための規範」
- JIS Q 27017:2016 (ISO/IEC 27017:2015)
  「情報技術―セキュリティ技術―JIS Q 27002に基づくクラウドサービスのための情報セキュリティ管理策の実践の規範」
- JIS X 9401：2016
  「情報技術―クラウドコンピューティング―概要及び用語」

[3] Center for Internet Security (https://downloads.cisecurity.org/#/)

(This page is intentionally left blank.)

Ⅱ．前提および概要

(This page is intentionally left blank.)

本編では、本ガイドラインの概要として、クラウドサービス事業者とクラウドサービス利用者の責任と役割、環境の設定における留意すべきパターン及びガイドライン構成の基盤となる設定不備の要因と対策について述べる。本編には、「Ⅲ.クラウドサービス利用側に求められる対策」や「Ⅳ.クラウドサービス提供側に求められる対策」を読むために必要な前提知識も含まれている。

Ⅱ．１　本ガイドラインの前提事項

本章では、本ガイドライン全体の前提事項として、クラウドサービス事業者とクラウドサービス利用者の責任共有モデル、クラウドサービス利用者の状況を含めたサプライチェーン及びコミュニケーションの重要性について述べる。

Ⅱ．１．１　クラウドサービスにおける典型的なセキュリティ設定項目と設定不備があった場合のリスク

クラウドサービスには、様々なセキュリティに関する設定項目がある。しかしながら、現存する全製品のセキュリティ設定を把握することは現実的には極めて難しいと言わざるを得ない。そこで、米国 CIS(Center for Internet Security)が発行する CIS Benchmarks®で示されている主要なクラウド基盤の各プロダクト[4]におけるクラウドセキュリティ設定項目を比較し、下表のとおり分類した。

これらをセキュリティ設定項目の類型と定義する。設定項目の意味について、図表　Ⅱ．１．１―１に示す。

4　比較したプロダクトは、次のとおり。
Amazon Web Service、Microsoft Azure、Google Cloud Platform、IBM Cloud、Oracle Cloud Infrastracture、Alibaba Cloud、Microsoft 365、Google Workspace

図表Ⅱ．１．１－１　セキュリティ設定項目の類型と類型項目の意味

No.	セキュリティ設定項目の類型	類型項目の意味
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。ID には、大別してユーザー、管理者及び開発者等の人間に対するアカウントとアプリケーションなどが API 等で使用するサービスアカウントがある。これらに対するアカウントグループやアクセス権等の設定がある
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り、ロギングを有効にするための設定、モニタリングを行うためのフィルタ設定及びログの保存期間設定などがある。
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、アクセス制御の設定、データの外部漏えいに備えた暗号化、ロギング及び一定期間経過後に削除するなどのライフサイクル設定等がある。
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、境界防護等に関する設定等がある。
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が提供されている場合があり、使用するための各種設定がある。
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ものであり、使用するクラウドに応じた適切な設定がある。
6.2	PaaS が提供するアプリケーション	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。コンテナエンジンに係るセキュリティ関連の設定がある。
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がある。

クラウドサービスにおけるセキュリティ設定項目の類型と設定不備があった場合の典型的なリスクと考えられる事項を図表　Ⅱ．１．１―２に示す。

表に示す設定項目について、クラウドサービス利用者がどこまで責任を持つかについては、次節の「Ⅱ．１．２　クラウドサービス事業者とクラウドサービス利用者の責任と役割」に示す。

クラウドサービスの利用側、提供側ともに、それぞれの設定項目が持つリスクを十分に理解し、本ガイドラインの対策項目を実践することが求められる。さらに、クラウド事業者からセキュリティ設定値群（例えば、マルウェア対策等）が明示されている場合は、本表でカバーされている範囲外であっても運用上差し支えない範囲で最も高いセキュリティ設定とするなどの配慮を行うべきである。

セキュリティ設定項目の類型に関するそれぞれの対策事項は、「Ⅲ．３．１．１【基本】設定項目の把握と設定」の「図表Ⅲ．3．１－１クラウドにおけるセキュリティ設定項目の類型と対策」を参照されたい。

なお、国際的な規格や文書である ISO/IEC 27017、NIST SP 800-53 Revision 5 及び NIST SP 800-171 Revision 1[5]の管理策については、本ガイドラインの設定項目の対策の一部を広い意味で含むものの、より一般的な内容となっている。このため、より包括的な管理策を確認したい場合には、個々のケースに応じてそれぞれの文書を参考にされたい。

[5] いくつかの NIST 文書については独立行政法人情報処理推進機構から日本語訳が公開されている。
https://www.ipa.go.jp/security/publications/nist/

図表Ⅱ．１．１－２　セキュリティ設定項目に対する設定不備のリスク

No.	セキュリティ設定項目の類型	考えられるリスク
1	ID とアクセス管理 （IAM）	クラウドサービスの一般利用者と管理者等のユーザ ID やパスワードを設定する際、明確に分離して認証の設定・管理を行わないことで、管理者権限の設定が甘いものとなり、外部からのハッキングにより簡単に情報漏えいしてしまう。また、アクセス管理の設定の際に、厳密に設定・管理を行わないことで、アクセス管理に不慣れな一般利用者が不注意で個人情報をインターネットに全面公開してしまい、個人情報の漏えいにつながる。さらに、退職者のユーザ ID やパスワードの失効管理を実施せずに放置したり、ゲストユーザーに対する設定が甘かったりすると、不正に利用されることにより情報漏洩等が発生するリスクがある。また、サービスアカウントに対しては、プログラム等が使用する API のアクセスキー及びシークレットキー（クレデンシャル情報）の設定管理についても不十分であるとシステム全体の乗っ取りなどのリスクがある。
2	ロギングとモニタリング	ロギングの設定はデフォルトでオフになっていることが多い。クラウドサービスを利用する際にオフ設定の解除を忘れて、モニタリングが機能しない、異常が起きても気が付かない、モニタリングが機能していてもログの保存期間を適切に設定しないで異常時の解析が出来ないなどのリスクが発生することがある。また、ログを取得する際の留意点としてはログ監視ソフトのぜい弱性への対策があげられる。実際に、OSS（Open Source Software）のログ監視ソフトを使用していたケースで、OSS のぜい弱性が判明し、そのぜい弱性をつかれて情報漏えいした事例がある。
3	オブジェクトストレージ	クラウドサービスで提供されるファイルの保存などに使用されるオブジェクトストレージのアクセス権設定を厳密に行わずに情報漏えいを引き起こした事例がある。また、ログ情報などが改ざんされたり、ライフサイクル設定を適切に行わなかったためにデータ喪失を引き起こすリスクなどが考えられる。
4	インフラ管理	
4.1	仮想マシン（VM,VPS）	仮想マシンのぜい弱性を解消するためのセキュリティパッチを怠り、そのままの状態で使用を続けると、仮想マシンが不正アクセスを受けたり、マルウェアに感染するリスクがある。
4.2	ネットワーク	クラウド利用は、インターネット経由での利用となるため、基本的なネットワークセキュリティの設定を確実に行わずに利用すると、不正アクセスやマルウェア感染のリスクが高まる。
5	セキュリティ等の集中管理	IaaS/PaaS が提供する各種の集中管理機能は、デフォルトで起動していないことが多い。さらに、GUI(Graphical User Interface)等で使いやすくなっている反面、慎重に設定しないと広範囲に及ぶインシデント等が発生するリスクがある。
6	IaaS／PaaS が提供する、その他のサービスや機能	
6.1	鍵管理	秘密鍵を KMS（鍵管理システム）の使用や秘密鍵を保存したオブジェクトストレージの暗号化等の対策を行わずに保管すると、サーバが不正アクセスを受けたり、マルウェアに感染した場合に、攻撃者に鍵が漏えいし、情報漏えいや不正操作につながるリスクが高まる。
6.2	PaaS が提供するアプリケーション	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わないと、不正アクセスを受け、情報漏えい等を引き起こすリスクがある。
6.4	コンテナ	クラウドサービスのアプリケーション構築で広く利用されているコンテナそのものとコンテナ管理システムに対するセキュリティ設定を確実に行わないと、不正アクセスやコンテナを標的にしたマルウェアの感染リスクがある。

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、バックアップ等のサービスについては IaaS/PaaS 事業者から提示されるセキュリティ設定を適切に設定しないと広範囲に及ぶインシデント等が発生するリスクがある。

Ⅱ．１．２ クラウドサービス事業者とクラウドサービス利用者の責任と役割

クラウドサービスの情報セキュリティを高めるためには、クラウドサービス事業者とクラウドサービス利用者が協力して、クラウドサービスに対する責任を共有する必要がある。この責任を共有するという考え方（責任共有モデルと呼ぶ）を多くのクラウドサービス事業者が採用している。責任共有モデルの基本については、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）の「Ⅰ．6．クラウドサービス事業者とクラウドサービス利用者の責任」を参照されたい。

本ガイドラインにおいては、設定に着目し、責任共有モデルにおけるクラウドサービス事業者とクラウドサービス利用者に課される責任と役割について述べる。クラウドサービスの適切な設定を促進するためには、クラウドサービス事業者側が適切な設定のための対策を施したサービス提供やクラウドサービス利用者への分かりやすい情報提供を行うとともに、クラウドサービス利用者がそれを受けて適切な設定を行うという、両者の協力が重要である。

実際のクラウドサービスにおける環境の設定については、クラウドサービス事業者とクラウドサービス利用者の責任範囲・内容は一律に決まるものではなく、クラウドサービスの内容やクラウドサービス利用条件・環境ごとに異なるので、クラウドサービス事業者の免責事項等の責任分界の確認が必要である[6]。

クラウドサービス利用者の責任範囲は、SaaS、PaaS 及び IaaS の利用形態によって変化する。ここではクラウドサービス利用者が責任を持つ環境の設定を「利用側環境の設定」、提供する事業者が責任を持つ環境の設定を「提供側環境の設定」と呼ぶこととする。また、利用側環境、提供側環境に関わらず、環境の設定には直接設定を実施する者と、責任を持って最終的な設定の確認を行い、また、正常な設定の維持に責任を持つ者が役割として必要となる。前者を設定者、後者を設定管理者と呼ぶこととする。

システム全体の動作環境の設定について、本ガイドラインで使用するシステム動作環境のレイヤモデルに、それぞれどの設定項目が存在するかを図表Ⅱ．１．２－１に示す。設定項目が存在する場合は丸印とした。これらの対応関係と具体的な設定項目との対応関係を図表Ⅱ.１．２－２に示す。

[6] クラウドサービスの利用における通信の確保に関する責任は、原則としてクラウドサービス事業者側ではなくクラウドサービス利用者側に帰属する。BCP の観点から通信回線の冗長性をクラウドサービス利用者が事前に検討しておくことも重要である。

図表Ⅱ．１．２－１システム動作環境のレイヤモデルと対応する設定項目

	対応する設定項目									
システム動作環境のレイヤモデル	1.IDとアクセス管理	2.ロギングとモニタリング	3.オブジェクトストレージ	4.1 仮想マシン	4.2 ネットワーク	5.セキュリティ等の集中管理	6.1 鍵管理	6.2PaaSが提供するアプリケーション	6.3 データベース	6.4 コンテナ
データ	○	○	○			○				
アプリケーション	○	○				○	○	○		
ミドルウェアの設定		○	○			○	○		○	○
OSの設定		○				○	○			○
仮想環境の設定		○		○		○				○
ハードウェアの設定		○				○				
ネットワークの設定		○			○	○				
施設・電源の設定		○				○				

図表Ⅱ．１．２－２　各設定項目とレイヤとの対応関係

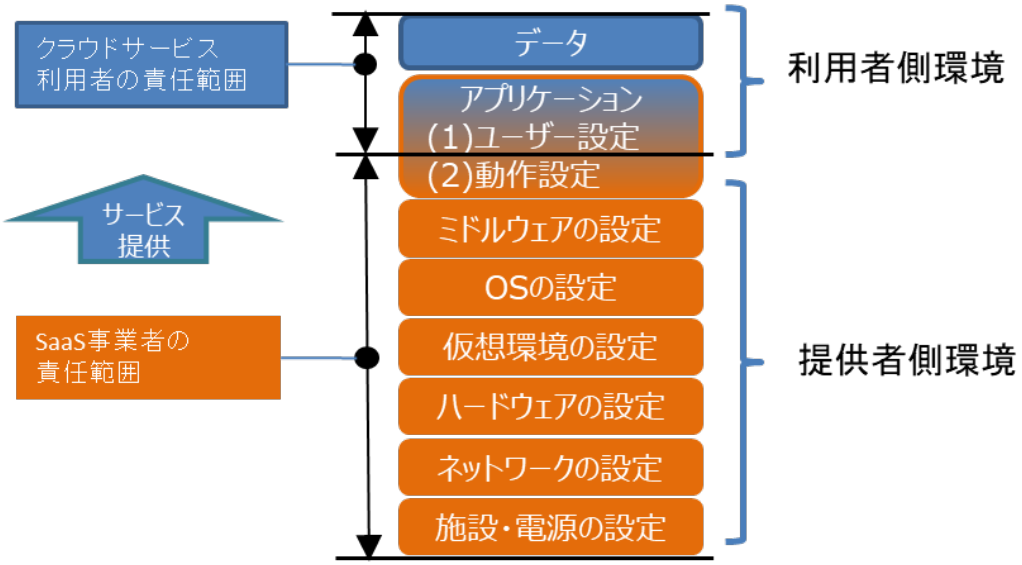
No.	セキュリティ設定項目の類型	各レイヤとの対応関係
1	ID とアクセス管理（IAM）	利用者のユーザ ID 設定や利用者のデータへのアクセス、システムへのアクセスに関する設定項目がある。
2	ロギングとモニタリング	ロギングは、全てのレイヤに関連し、システムの運用条件によってどこまでモニタリングするかが決まり、それに対応する設定項目がある。
3	オブジェクトストレージ	利用者のファイル等を格納するためのオブジェクトストレージに対する設定がある。オブジェクトストレージの動作等を規定するミドルウェアレイヤの設定と、データのアクセス設定等を規定するデータレイヤの設定項目がある。
4	インフラ管理	
4.1	仮想マシン（VM,VPS）	仮想環境レイヤに対応する設定項目がある。
4.2	ネットワーク	ネットワークレイヤに対応する設定項目がある。
5	セキュリティ等の集中管理	IaaS/PaaS 事業者から提供される各種の集中管理サービスは、当該クラウド基盤のアプリケーションとして提供され、監視対象としては各レイヤに関連する項目がある。
6	IaaS／PaaS が提供する、その他のサービスや機能	
6.1	鍵管理	暗号化が関連するレイヤに暗号鍵の設定項目がある。通常は、利用者のアプリケーション、ミドルウェア、OS 等に対応する。
6.2	PaaS が提供するアプリケーション	メールシステム等の PaaS が提供するアプリケーションそれぞれにおいて、設定項目がある。
6.3	データベース	データベースは、通常、ミドルウェアレイヤに相当し、関連する設定項目がある。
6.4	コンテナ	コンテナについては、コンテナエンジンを仮想環境上で構築する場合と、OS 上でそのまま利用する場合がある。コンテナエンジンに対応する設定項目がある。

上記を前提に、クラウドサービスのシステムを構成する動作環境の設定等について、SaaS、PaaS、IaaS ごとに責任範囲と責任共有の考え方を、以下に示す。

１．SaaS の設定に関する責任分界

SaaS を利用する場合、図表Ⅱ．１．２－３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る。アプリケーションの動作に係る設定（図の動作設定）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（図のユーザ設定）については、クラウドサービス利用者の責任となる。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両方となる。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る。

図表Ⅱ．１．２－３　SaaS における責任分界

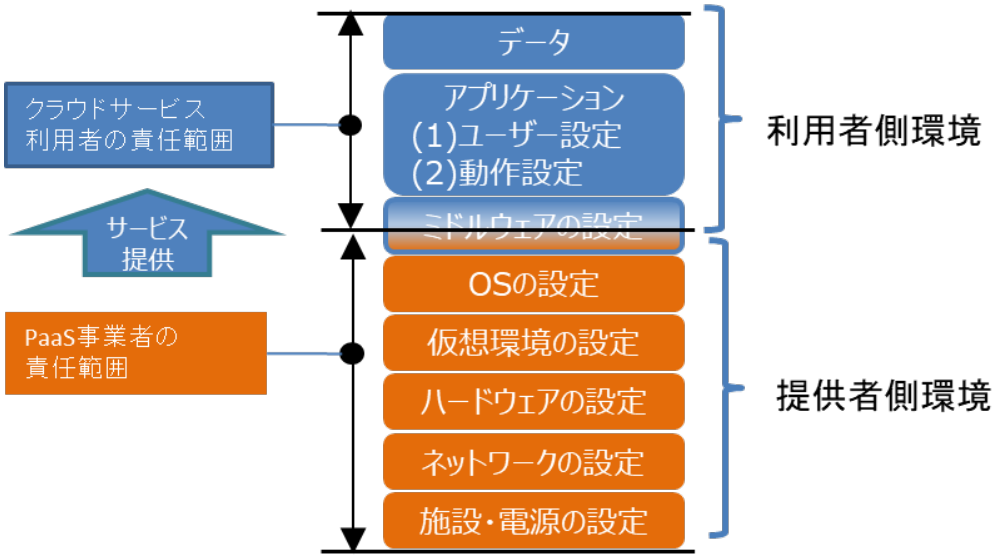


２．PaaS の設定に関する責任分界

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社内利用すること等が考えられる。その場合は、図表Ⅱ．１．２―４に示すとおり、データ、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う。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う。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する。（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る）。

ミドルウェアの動作に係る設定については、PaaS 事業者が責任を負う。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る。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両方となる。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る。

図表Ⅱ．１．２－４　PaaS の設定における責任分界



３．IaaS の設定に関する責任分界

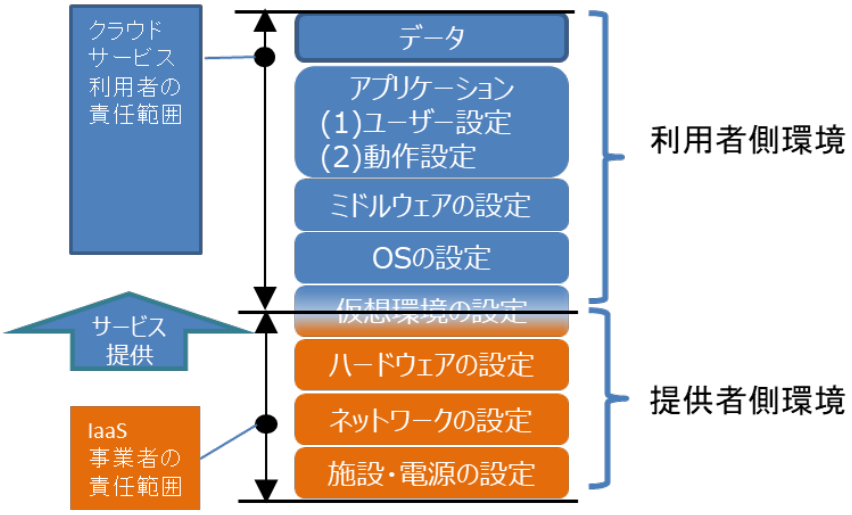
IaaS を利用する場合は、図表Ⅱ．１．２―５に示すとおり、クラウドサービス事業者は、クラウドサービス利用者との契約･SLA に基づき、ゲスト OS[7]等が動作するための仮想環境の構築と管理を提供する。クラウドサービス利用者は、仮想環境上で動作している OS を含めたすべてのソフトウェアの管理を行う。OS やミドルウェア層での障害対応や、ミドルウェアに対するパッチ適応やぜい弱性対応などは、クラウドサービス利用者の責任となる。

仮想環境の動作に係る設定については、IaaS 事業者が責任を負う。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る。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両方となる。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る。[8]

[7] 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。

[8] 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。

図表Ⅱ．１．２－５　IaaS の設定における責任分界



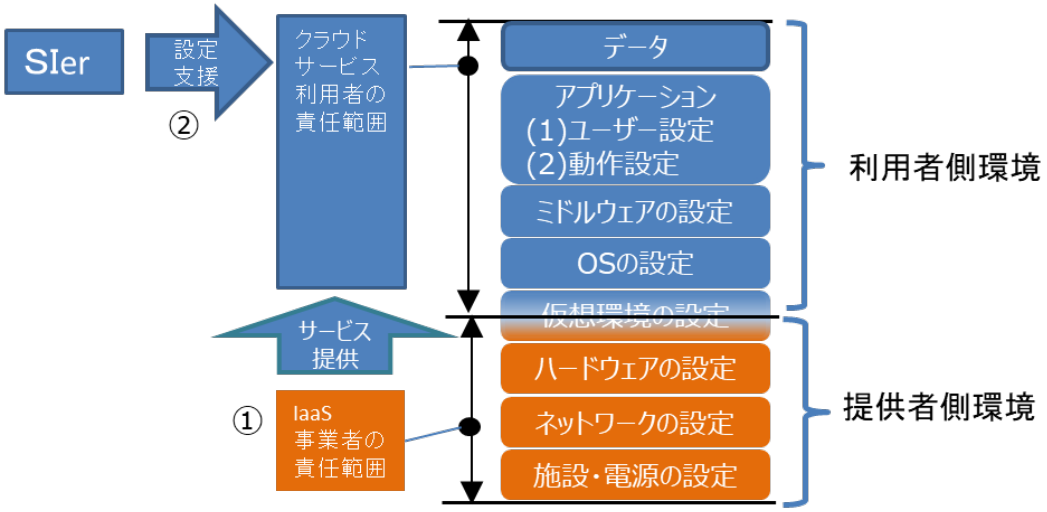
Ⅱ．１．３　環境の設定における留意すべきパターン

本節では、上記の責任共有モデルの変形として、特に留意すべきパターンの利用者と提供者の責任と役割について述べる。

１．IaaS 等の設定を SIer に外部委託する場合

クラウドサービス利用者がクラウドの動作環境設定を SIer に外部委託する場合の責任範囲と役割について IaaS 利用を例として、図表Ⅱ．１．３－１に示す。

図表Ⅱ．１．３－１　SIer が関与する場合の設定に関する責任分界（IaaS の例）



我が国においては、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多い。これらの作業は、環境の設定支援と位置付けられ、通常、準委任契約であり、最終責任はクラウドサービス利用者となる。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る。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る。

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含めて受託するマネージドサービスが登場しているが、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、設定管理者はクラウドサービス利用者となる。

２．SIer 等が SaaS を提供する場合

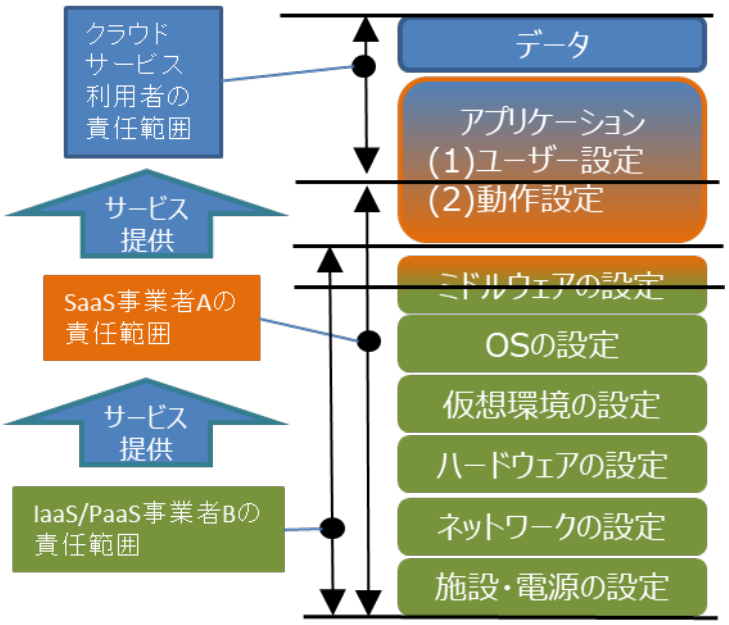
クラウドサービスの提供において、SIer 等（販売代理店も含む）が、クラウドサービス事業者とクラウドサービス利用者との間に入る場合がある。この場合、提供形態として様々なパターンがある。例えば、①SIer 等が、SaaS 事業者の代理店として利用契約を代行し、サービスをそのままもしくはアプリケーションをカスタマイズして SaaS として提供するパターン、②SIer 等は、運用保守等のサポートのみ行い、クラウドサービス利用者はクラウドサービス事業者と直接契約するパターン [9]、③SIer 等がクラウドサービス事業者のサービスをサポートなしで販売するのみのパターンなどである。いずれのパターンにしても、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、免責事項などを良く確認して契約を行う必要がある。

３．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る。図表Ⅱ．１．３－２にサプライチェーンを示す。

[9] 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。

図表Ⅱ．１．３－２　他社の PaaS を利用した SaaS の提供



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のユーザ設定を除く、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る。ただし、SaaS 事業者 A にサービス提供するするクラウドサービス(IaaS/PaaS)に帰する障害が発生した場合、契約によっては SaaS サービスの可用性について免責とする場合がある。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である。

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、次のとおりとなる。

・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。

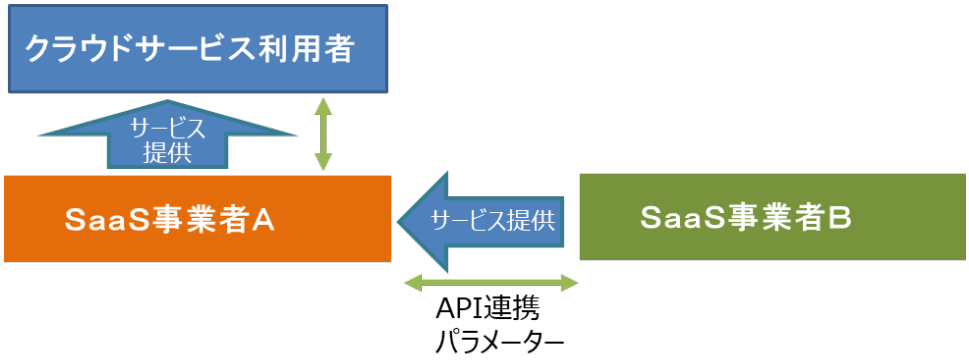
・提供しているクラウドサービスにおいて、IaaS/PaaS 事業者 B の管理範囲に帰する問題が発生した場合は、SaaS 事業者 A と IaaS/PaaS 事業者 B との契約に基づき、対処する。

・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。

４．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る。図表Ⅱ．１．３－３に SaaS 連携の概念図を示す。

図表Ⅱ．１．３－３　連携したSaaSの提供



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する。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する。利用側環境の設定に関しては、SaaS事業者Aが用意したGUI（Graphical User Interface）等で設定するので、クラウドサービス利用者は意識しないことが多いが、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上手くいっていないことなどを推測できる。

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、次のとおりとなる。

・SaaS事業者Aは、SaaS事業者B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に正しくタイムリーに伝える責任がある。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る。

クラウドサービス提供側のサプライチェーン構造には様々な形態が存在する。詳細については、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）の「Ⅰ．７．サプライチェーン」を参照されたい。

また、Ⅱ．１．１、Ⅱ．１．２で示したとおり、クラウドサービスの利用形態、提供形態に応じて環境の設定に関する責任と役割が変化するので、形態に応じた利害関係者同士のコミュニケーションが非常に重要となる。次章で述べる設定不備の要因と対策においてもコミュニケーションミスにより引き起こされたものが多く、本ガイドラインにおいても「Ⅲ．１．４．１．【基本】コミュニケーション」、「Ⅳ．１　情報提供」などのように、コミュニケーションの要素を様々な対策に組み込んでいる。

なお、クラウドサービスにおけるコミュニケーションの重要性については、「クラウドを利用したシステム運用に関するガイダンス [10]」に詳細に記載されているので、参考にされたい。

[10]「クラウドを利用したシステム運用に関するガイダンス」，2021 年 ， 内閣サイバーセキュリティセンター
https://www.nisc.go.jp/policy/group/infra/cloud_guidance.html

Ⅱ．２　設定不備の要因と対策

Ⅱ．２．１　設定不備の事例と要因分析

近年、クラウドサービスの設定不備により、以下のような情報漏えいの事例が発生している。

事例１

クラウドサービス提供事業者が、提供している SaaS の機能変更を行った。これに伴い、当該 SaaS のユーザーアクセスに関する設定について、結果的にデフォルトでセキュリティレベルが下がってしまった。利用企業側はこれに気づかず、低いセキュリティレベルのまま利用し続けた結果、機密情報が大量に流出した。

事例２

企業従業員が個人的にクラウドサービスを利用し、自社の業務で利用する機密情報を格納していた。後にこれらのファイルが公開設定であったことが外部からの指摘で判明した。

事例 3

ある企業の業務委託先が、サーバからクラウドサービスへのデータ移行を行う際に、ストレージの設定を公開設定としていた。これにより長期間機密情報が公開されている状態になった。

上記の事例の要因としては以下のような点が挙げられる。

・利用企業におけるクラウドサービス設定値に関する理解の不足と使用しているクラウドサービスに関する情報の不足
・委託先管理やシャドーIT への対応策などの体制面の不備
・設定不備を抑止するための体系的な対策の不備

これらの事例は、設定不備によってセキュリティ事案が発生し、公表に至った一部の例となり、実際には公開されていない事案も含めて、様々な事案が発生していることが想定される。このような事案を発生させないため、クラウドサービス事業者、利用者双方において様々な取組が進められている。

そこで、総務省では、クラウドサービス利用者及びクラウドサービス事業者に対してヒアリング調査を行った。ヒアリング調査の結果と公開事例の調査結果から得た個々の原因を４Ｍのフレームワーク（Man,Manual,Machine,Method）で公開事例の調査と併せて分類した。その結果、設定不備の要因については、下記のとおり大別されることが明らかになった。分類の要約については次のとおりである。また、結果を図表Ⅱ．２．１－１に示す。

１．人・組織に関するもの
設定不備に対する組織としての方針事項、技術情報収集、人材育成計画及び作業委託先やクラウドサービス提供者とのコミュニケーションが不十分であった。

２．作業規則・マニュアルに関するもの
環境の設定において、設定者の作業に対する設定管理者の承認などの作業規則やマニュアル整備

が不十分であった。

３．システム動作環境における設定管理に関するもの

クラウドシステム動作環境に対する知識が不十分であったことや、次々にリリースされるクラウドサービスにおけるシステム環境の変化に追随するためのプロビジョニングが不十分であった。

４．システム動作環境の設定の方法論に関するもの

複雑化するクラウドシステムにおける動作環境の設定に対応する、設定管理のためのツール利用方法や設定のための方法論が不十分であった。

図表Ⅱ．２．１－１ 設定不備の要因

1.人・組織に関するもの	
	1-1 方針レベル・ガバナンス不十分
	1-2 技術情報の収集不足
	1-3 知識・スキル不足
	1-4 コミュニケーション不足
2.作業規則・マニュアルに関するもの	
	2-1 作業規則やマニュアルが不十分
	2-2 単純ミス対策不十分
3. システム動作環境における設定管理に関するもの	
	3-1 環境の設定に対する知識不足
	3-2 設定の複雑さ対応不足
	3-3 アカウント監視不十分
	3-4 クラウド環境へのプロビジョニング不足
	3-5 その他
4. システム動作環境の設定の方法論に関するもの	
	4-1 環境の設定ノウハウの蓄積が不十分
	4-2 支援ツールなどの活用不十分
	4-3 定期的なチェック・監査不十分

上述の結果については利用者側だけでなく、クラウドサービス提供者側でも認識しておく必要がある。

Ⅱ．２．２ 要因に対する対策

要因の分析に続いて、個々の要因に対する対策の導出を行った。なお、一つの事業者がサービス利用者にもサービス提供者にもなり得るので、以降の分析等では、利用者・提供者という主体では分けず、利用場面、提供場面という概念を用い、利用側、提供側と呼ぶこととする。

【利用側での対策】

得られた利用側での対策について親和性（関連性）の高いグループを整理・体系化した結果、下記のような大項目にまとめられる。

１．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

２．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

３．システム動作環境における設定管理

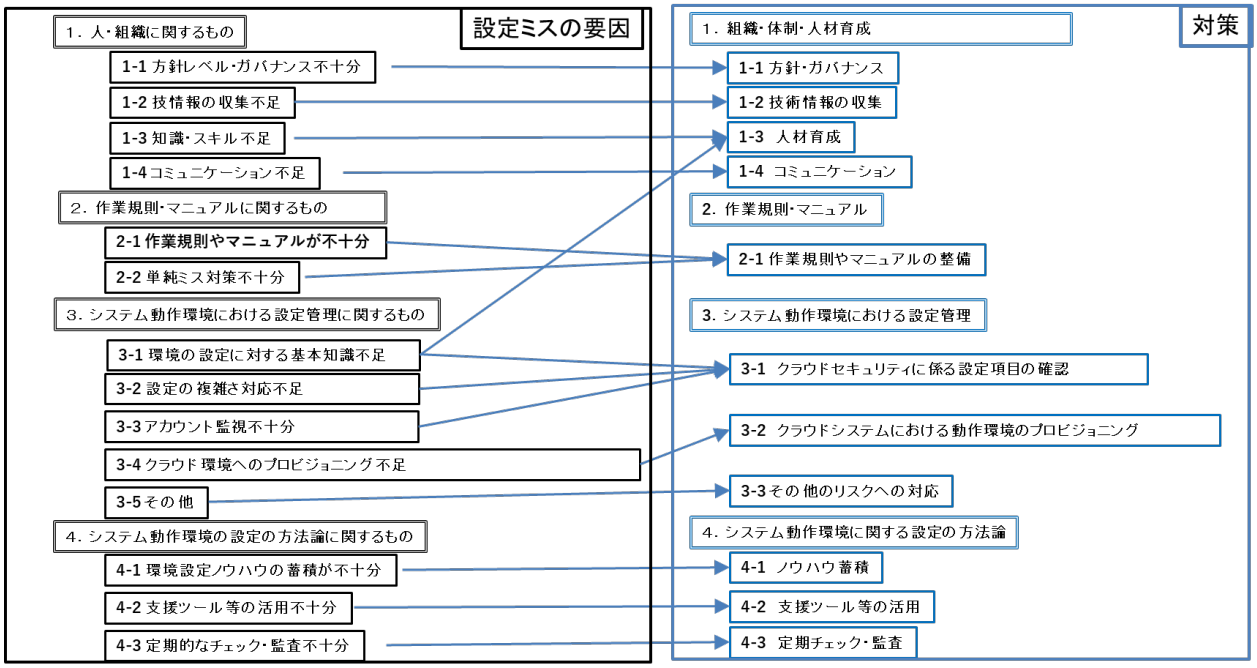
クラウドサービス利用者すべてが知っておくべきクラウドシステムの環境そのものについて、クラウドに関する設定項目の類型とクラウドシステムの機能追加などの環境変化に追随するための対策

４．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

図表Ⅱ．２．２―１にクラウドサービス利用側の要因と対策の関係を示す。

図表Ⅱ．２．２―１　クラウドサービス利用側の要因と対策の関係



これらの対策項目の詳細については、「Ⅲ.クラウドサービス利用側に求められる対策」に記載する。

【提供側の対策】

得られた提供側での対策について親和性（関連性）の高いグループを整理・体系化し、大項目にまとめた。さらに利用側に提供すべき対策と提供側が自ら取り組む対策に大別すると下記のようになる。

＜利用者に提供すべき対策＞

１．情報提供

クラウドサービス利用者に分かりやすく伝えることなどの対策

２．学習コンテンツや学習機会の提供

クラウドサービス利用者に提供する学習コンテンツを提供する際の留意点

３．支援ツールの提供

クラウドサービス利用者に提供する環境の設定に関連する支援ツールの提供についての事項

＜提供者が自ら取り組むべき対策＞

4．システム改善

クラウドサービスのシステムそのものを改善して、設定不備の発生しにくいシステムを提供する対策

5．組織的な改善活動

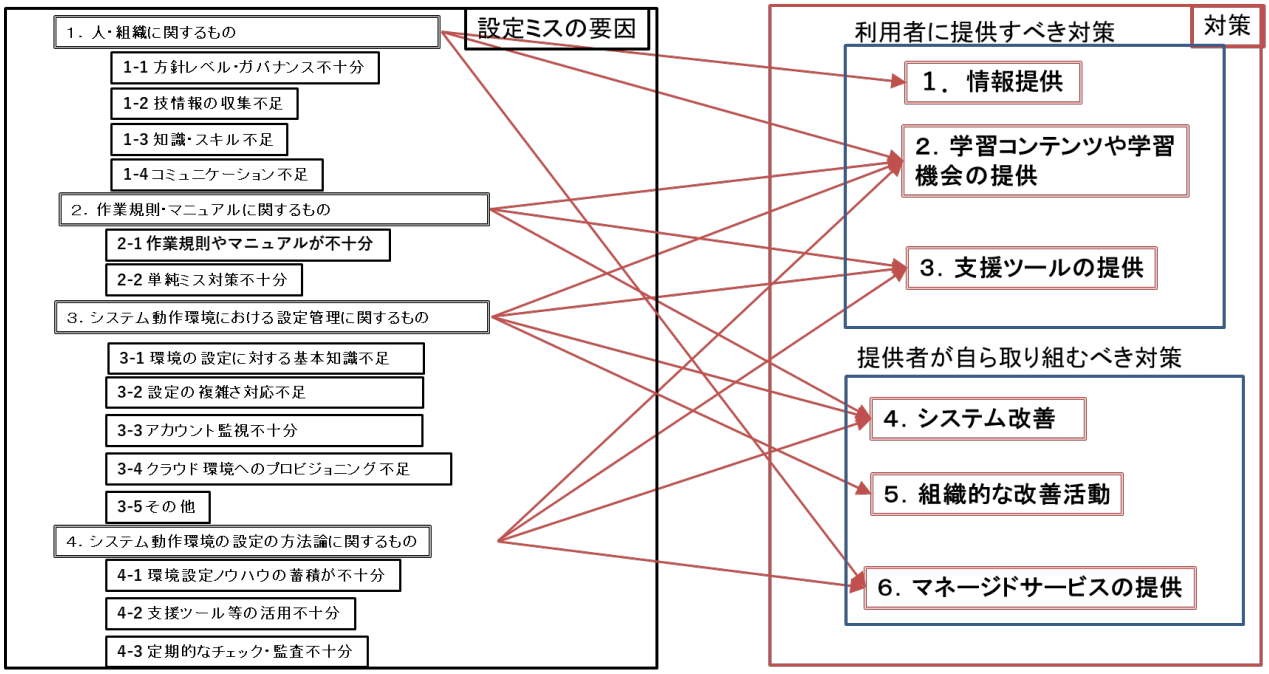
上記のシステム改善を続けていくための対策

6．マネージドサービスの提供

設定不備を抑止・防止するための負担軽減の方法の一つとして、マネージドサービスを用いる対策

図表Ⅱ．２．２－２にクラウドサービス提供側の要因と対策の関係を示す。

図表Ⅱ．２．２－２　クラウドサービス提供側の要因と対策の関係



これらの対策項目の詳細については、「Ⅳ.クラウドサービス提供側に求められる対策」に記載する。

Ⅲ．クラウドサービス利用側に求められる対策

(This page is intentionally left blank.)

Ⅲ．１　組織体制・人材育成

Ⅲ．１．１　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

【目的】

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する。

Ⅲ．１．１．１ 【基本】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、全社的又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すること。

【ベストプラクティス】

文書には、次の内容を含むことを推奨する。

i. 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社内セキュリティ部門やコンプライアンス部門などの管理部門を設置、整備する。
ii. 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規定やルールの作成。規定等の作成時には、「自社セキュリティポリシー」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。
iii. 設定不備の発見に寄与する内部監査基準を整備する。
iv. 定期的なシステムのチェックや内部監査を実施する。
v. 組織の許可なく利用されているクラウドサービスを発見、抑止する。併せてクラウド利用状況の可視化ツールとしてCASB(CloudAccessSecurityBroker)機能などの導入を検討する。
vi. 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。
vii. 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。
viii. 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。
ix. 企業や組織におけるクラウドの利用方針やガバナンスを集中的に行う役割として、CCoE(Cloud Center of Excellence)[11]を設置することは、組織横断的にクラウドのセキュリティに関する施策を行えるため、設定不備における課題に対しても有効である。

Ⅲ．１．１．２ 【基本】事業部門等が独自に利用する場合のルール形成

利用者組織において、利用者組織の事業部門等が独自にクラウドサービスを利用する場合がある。事業部門等が組織のセキュリティ管理者やクラウドサービス管理者が知らないままクラウドサービスを利用することがないように条件付きで許可するなど、組織のビジネス環境や方針に基づいて利用する場合のルールを明確にし、文書化すること。

---

[11] 部門横断的にクラウド戦略を推進していくために、必要な人材やリソースなどを集約した組織を指す用語として使われている。

【ベストプラクティス】

i. 事業部門等が独自にクラウドサービスを利用することを禁止する場合は、自社のIT環境が事業部門等のニーズを満たしているかを常に確認するなどの配慮をすること。

ii. 事業部門等が独自にクラウドサービスを利用することを許可する場合は、全社の管理部門が利用に当たっての責任を明確にし、ルールや規則を全社的に明確化し文書化して配布するなど組織全体への浸透を図ること。

iii. 上記のルールの文書化だけでなく、SASE（Secure Access Service Edge）などのセキュリティゲートウェイを必ず通すことやCSPM (Cloud Security Posture Management)などの管理部門が把握できる監視ツールを使用することなどの対策も併せて実施することを推奨する。

事業部門が独自に利用するサービスの設定値を客観的に評価するため、運用開始前に各種設定値の外部診断を受けることを推奨する。

Ⅲ．１．１．３ 【推奨】設定診断等の支援ツール利用に対する組織的取組

クラウドサービス利用の高度化・複雑化に伴い、設定が必要な項目の量的な増加や組合せの整合性を取ることなどの複雑化が課題となる。これらの課題に対処するため、クラウドサービス事業者や独立のツールベンダーから、設定値全体の監視やルールを外れた設定値を警告・復元するなどの支援ツールが提供されている場合がある。クラウドの導入や運用管理に当たり、これらの支援ツール等の積極的利用に取り組むことについて検討し、組織として予算化、計画化することが望ましい。

支援ツールの利用の詳細は、「Ⅲ．４．２　支援ツール等の活用」を参照されたい。

※環境の設定については、設定するだけではなく運用における監視も重要となる。特に重要な設定項目として、「Ⅲ．３．１．１ 【基本】設定項目の把握と設定」の「【評価項目】a.クラウドにおけるセキュリティ設定項目の類型と対策」のうち、「２　ロギングとモニタリング」がある。

Ⅲ．１．１．４ 【基本】クラウドに関する人材の組織的育成

設定に関する知識やノウハウの向上を実現するために、組織的にクラウド資格等の取得やクラウドサービス事業者が用意するセミナーの受講及び知識の組織内共有等について計画し、文書化すること。また、クラウドに関する人材を組織的に育成するために、クラウドに関する人材を適切に評価できる枠組みを構築すること。

人材育成の詳細は、「Ⅲ．１．３　人材育成」を参照されたい。

Ⅲ．１．２ 技術情報の収集

【目的】

クラウド技術は日進月歩であり、組織が利用するクラウドサービスについて、日頃からの情報収集、リスク分析、対策立案のサイクルを組織的に確立する。

Ⅲ．１．２．１【基本】技術情報の収集

クラウドサービスの変化に伴う各種設定値の変更等の技術情報については、組織として情報収集、リスク分析、対策立案プロセスを確立し文書化を行うこと。

【ベストプラクティス】

i. 組織のクラウドサービスの利用を管理する部門において一元的に技術情報を収集し、クラウドサービスを利用している部門に通知する等の体制を構築することが望ましい。また、通知に当たっては、メーリングリストやチャットシステムなどを活用することにより、複数人がチェックできるようにする。

ii. 利用側において、専門的で高度な技術が必要な場合は、IaaS/PaaS事業者から直接技術情報を収集可能な体制を構築することが望ましい。

iii. クラウドに関するベストプラクティスを適宜モニターしておくと良い。国際的に広く利用されるベストプラクティスとして、NIST SP-800[12]シリーズやCIS（Center for Internet Security）のCIS Controls、CIS Benchmarks[13]等がある。

Ⅲ．１．３ 人材育成

【目的】

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する。

Ⅲ．１．３．１【基本】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すること。

【ベストプラクティス】

i. 製品を提供するベンダーが用意するトレーニングコース（無料のものもある）の受講を奨励する。

ii. クラウドサービス導入時に管理部門等が企画してユーザ向け説明会等を実施する。

iii. クラウド利用における基本的な理解については、「テレワークセキュリティガイドライン第５版、令和３年５月、総務省[14]」の「第２章　３．クラウドサービスの活用の考え方」や関連する対策一覧を参考にすると良い。

iv. クラウドの運用における基本的な理解については、「クラウドを利用したシステム運用に関するガ

12 IPA セキュリティ関連 NIST 文書(https://www.ipa.go.jp/security/publications/nist/index.html)

13 CIS Benchmarks (https://www.cisecurity.org/cis-benchmarks/)

14 https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/

イダンス（詳細版）」を参考にすると良い。

v. インシデント、アクシデント等が発生した場合、その内容をケーススタディとして組織内で共有し理解度向上及び再発防止に活用する。

Ⅲ．１．３．２ 【基本】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ること。

【ベストプラクティス】

i. 製品を提供するベンダーが用意するトレーニングコース等の受講を奨励する。

ii. ベンダー資格等の取得を奨励する。

iii. CCSP®[15]、SANSトレーニングプログラム[16]、CCAK[17]等の資格の取得を奨励する。

iv. 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す。

Ⅲ．１．４ コミュニケーション

【目的】

組織として利害関係者とのコミュニケーションを円滑かつ確実に行う。

Ⅲ．１．４．１ 【基本】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すること。

【ベストプラクティス】

i. クラウドの運用におけるコミュニケーションのあり方については、「クラウドを利用したシステム運用に関するガイダンス（詳細版）」の「5．クラウド利用に当たってのコミュニケーションの在り方」を参考にすると良い。

クラウドサービス利用者

ii. 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。

iii. SIer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。

iv. 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。

[15] https://japan.isc2.org/ccsp_about.html
[16] https://www.sans-japan.jp/
[17] https://www.cloudsecurityalliance.jp/site/?page_id=432

v. 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

vi. 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。

vii. 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

viii. 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。

Ⅲ．２ 作業規則・マニュアル

Ⅲ．２．１ 作業規則やマニュアルの整備

【目的】

「Ⅲ．１．１ クラウド設定不備の抑止・防止に係る方針的事項」に示す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する。また、作業手順やマニュアルを確実に整備する。

Ⅲ．２．１．１ 【基本】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すること。

【ベストプラクティス】

i. 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、事業部門等が独自にクラウドサービスを利用する場合にも周知・徹底させる。

Ⅲ．２．１．２ 【基本】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、作業手順書を整備すること。

【ベストプラクティス】

ii. 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、手順を組み立てる。

iii. 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む。

iv. 自らインフラの設定を行う大規模なクラウドサービス利用者や、SIer、SaaS事業者等は、

IaaS/PaaSの設定について、IaC（Infrastructure as Code）ツールなどで手順のコード化・レビューを行い、繰り返し利用することを推奨する。

v. 手順書の作成について、CIS Benchmarksやクラウドベンダーが提供する技術的なベストプラクティスを参考にする。

Ⅲ．２．１．３ 【基本】ヒューマンエラー対策

作業手順書にヒューマンエラー対策を確実に組み込むこと。

【ベストプラクティス】

i. 設定者及び設定管理者によるダブルチェック等のプロセスを作業手順に組み込む。

ii. 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む。

iii. 先進的なユーザで、作業プロセス自動化のためCI/CD（Continuous Integration／Continuous Delivery）等に取り組んでいる場合は、設定者と設定管理者の適切なレビューと自動化プロセス運用のフィードバックを確実に行う。

Ⅲ．２．１．４ 【基本】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むこと。

Ⅲ．３　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

Ⅲ．３．１　クラウドセキュリティに係る設定項目の確認

【目的】

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する。

Ⅲ．３．１．１ 【基本】設定項目の把握と設定

典型的なクラウドの設定項目について理解し、自社で利用する IaaS/PaaS の設定項目を把握した上で設定すること。（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）

※セキュリティ設定項目の類型と対策を図表Ⅲ．３．１－１に示す。

設定項目の把握の前提となるシステムの構成要素及び構成管理については、「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）」「Ⅱ．４．５．構成管理」を参照されたい。

【ベストプラクティス】

i. 「図表Ⅲ．３．１－１クラウドにおけるセキュリティ設定項目の類型と対策」の活用例
   - 自社のクラウドの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。
   - 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。

ii. 特に重要な設定項目
   - 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。
   - 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
   - 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。
   - 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。

図表Ⅲ．３．１－１　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、CASB による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 が提供するアプリケーション	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。

Ⅲ．３．１．２ 【基本】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すること。

【ベストプラクティス】

i. 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。
ii. 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）
iii. 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）
iv. 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

v. 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）

Ⅲ．３．２　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

【目的】

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う。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ある。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る。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ある。

Ⅲ．３．２．１ 【基本】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、準備し対応すること。

【ベストプラクティス】

i. 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。
ii. 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。
iii. 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（Ⅲ．１．２．１．【基本】技術情報の収集　のベストプラクティスを参照）。
iv. 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。

Ⅲ．３．３　その他のリスクへの対応

【目的】

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う。

Ⅲ．３．３．１ 【基本】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、対応方針を文書化すること。

【ベストプラクティス】

i. 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。リスクマネジメントについては、「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）」「Ⅱ．９．事業継続マネジメントにおける情報セキュリティ」を参考にすると良い。
ii. 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。

iii. 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。

iv. 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。

v.

vi. OSS（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。

vii. 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[18]。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。

[18] このような場合は、クラウドサービス事業者が外国法に基づくデータ開示要請についてどういうスタンスをとっているかを考慮する必要がある。

Ⅲ．４　クラウドシステム動作環境に関する設定の方法論

Ⅲ．４．１　ノウハウの蓄積

【目的】

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する。

Ⅲ．４．１．１ 【推奨】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すること。

【ベストプラクティス】

クラウドサービス利用者

i. 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。
ii. 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。
iii. 運用の初期においては、自社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。
iv. 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）

v. 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

Ⅲ．４．２　支援ツール等の活用

【目的】

複雑化するシステム動作環境の設定項目の管理に対して、支援ツール等の活用を推奨する。

Ⅲ．４．２．１ 【推奨】支援ツールや外部診断サービス等の活用

システム動作環境の設定に関わる設定者及び設定管理者は、支援ツールや外部診断サービス等を活用すること。

【ベストプラクティス】

i. 下記のような機能を有するツールについて、ビジネス環境の要求に合わせて導入を検討する。
・設定不備の検出
・脅威の検出

・ファイアウォールやセキュリティグループのルールチェック
・ぜい弱性診断
・監視ツール（生存監視、性能監視、ログ監視、Web監視など）
・性能監視、ログ監視
・構成管理、構成記述ツール

ii. ツール等の利用に当たっては、ツール過信に陥らないよう、組織としてのレビュー及び判断を行う。

Ⅲ．４．３　定期的な設定のチェックと対応

【目的】

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、適切に対応する。

Ⅲ．４．３．１ 【基本】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、適切に対応すること。

【ベストプラクティス】

i. 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。
ii. 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。
iii. 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。
iv. 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。
v. 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。

(This page is intentionally left blank.)

Ⅳ クラウドサービス提供側に求められる対策

(This page is intentionally left blank.)

Ⅳ．１　組織体制・人材育成

Ⅳ．１．１　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

【目的】

クラウドサービス提供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する。

Ⅳ．１．１．１ 【基本】クラウドサービス提供におけるガバナンスの確保

クラウドサービス提供者は、設定不備の抑止・防止に関す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提供方針等）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すること。

【ベストプラクティス】

文書には、次の内容を含むことを推奨する。

i. 組織のクラウドサービス提供について安全性を確保するための部門の設置。

ii. 提供者側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規定やルールの作成。規定等の作成時には、「自社セキュリティポリシー」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。

iii. 一般のクラウドサービス利用者がSaaS、IaaS/PaaS等と契約する場合や、SaaS事業者が他社のIaaS/PaaS事業者と契約する場合等、いずれの契約においても、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の確認を行うこと。

iv. 利用者への情報提供に関するポリシー

※詳細については、「Ⅳ．２　情報提供」を参照されたい。

v. 利用者への学習コンテンツや学習機会の提供に関するポリシー

※詳細についてては、「Ⅳ．３　学習コンテンツや学習機会の提供」を参照されたい。

vi. 提供者側のシステム改善に関するポリシー

※詳細については、「Ⅳ．５　システムの改善　－　ミスが発生しにくいシステムの提供」を参照されたい。

vii. 提供者側組織の取組みに関するポリシー

※詳細については、「Ⅳ．６　継続的な改善　－　ＰＤＣＡを回す」を参照されたい。

viii. 提供者側組織のクラウドサービス利用における負担の軽減

※詳細に関しては、「Ⅳ．７　マネージドサービスの提供」を参照されたい。

Ⅳ．１．１．２ 【推奨】設定診断等の支援ツール提供に対する組織的取組

クラウドサービス利用の高度化・複雑化に伴い、設定が必要な項目の量的な増加や組合せの整合性を取ることなどの複雑化が課題となる。クラウドサービス利用者の立場に立った支援ツール等の提供について積極的に取り組むことを検討し、組織として予算化、計画化することが望ましい。

支援ツール提供の詳細は、「Ⅳ．４　利用者支援ツールの提供」を参照されたい。

Ⅳ．１．１．３ 【基本】クラウドに関する人材の組織的育成

クラウドサービス提供におけるシステム動作環境の設定に関する知識やノウハウの向上を実現するために、組織的にクラウド資格等の取得やセミナー受講等について計画し、文書化すること。また、クラウドに関する人材を組織的に育成するための基盤として、クラウドに関する人材を適切に評価できる枠組みを構築すること。

Ⅳ．２　情報提供

クラウドサービス事業者は、クラウドサービス利用者が正しく環境の設定ができるように、環境の設定に関する正しく適切な情報をタイムリーに提供する必要がある。

Ⅳ．２．１　正しい情報の提供

【目的】

設定マニュアルなどが間違っていれば、正しい設定はできない。組織としてシステム動作環境の設定に関する正しい情報を確実に提供すること。

Ⅳ．２．１．１　【基本】正しい情報の提供

利用者の環境の設定に関するマニュアル等については、間違いのないように複数の目でチェックを行い、品質を高めること。これはドキュメントの品質管理の問題であり、組織として対応する必要がある。

Ⅳ．２．２　十分な情報の提供

【目的】

クラウドサービス事業者には、自社のサービスについての説明責任があることから、クラウドサービス利用者に十分な情報を提供すること。一部の情報を提供しなかったため、正しい設定ができなかった場合は、クラウドサービス事業者側の責任が問われる可能性がある。

また、クラウドサービス事業者は、環境の設定におけるリスク分担や責任分担に関する情報も提供する必要がある。リスクが顕在化した際の損害賠償範囲なども明確にしておくことが望ましい。

Ⅳ．２．２．１　【基本】十分な情報の提供

組織としてシステム動作環境の設定に関する十分な情報を確実に提供すること。

【ベストプラクティス】

i. 情報の開示については、クラウドサービスが十分な情報開示ができているかを審査する、情報開示認定制度[19]があるので、取得を検討する。

ii. 第三者評価レポート（SOC2レポート等）を取得しクラウドサービス利用者に開示するのも、自社サービスに関する情報提供のための有効な手段である。

iii. 第三者認証や認定の取得に関して、取得状況について自社のWebサイトで発信していくことも情報提供として有効である。

Ⅳ．２．３　わかりやすい情報の提供

【目的】

システム動作環境の設定に関して、マニュアルがわかりにくいために利用者が設定を誤ることも十分起こりうる。また、サービスの利用者は、ＩＴに詳しい者とは限らない。利用マニュアル等は、初心者にもわかりやすい記述を心がける。

Ⅳ．２．３．１【基本】わかりやすい情報の提供

組織としてシステム動作環境の設定に関するわかりやすい情報を確実に提供すること。

【ベストプラクティス】

i. 各設定値の意味や背景となるセキュリティポリシーを解説するとともに、その設定値を選択した場合の影響等についても説明する必要がある。例えば暗号化設定の選択肢では、ぜい弱なものはその旨を明示する必要がある。

ii. 具体的な環境の設定に関する例を示すことも有効である。

iii. セキュリティ上のリスクがある設定など、特に注意が必要な箇所は必ず読まれるように工夫することが必要である。

iv. 分厚いマニュアルは読む気がしなかったり、読んでも理解できなかったりすることが多い。適切な分量のマニュアルを作成するとともに、要約版や検索ツールも同時に提供することが望ましい。

v. 利用者が行う環境の設定を動画で提供する企業が増えている。文字の情報だけでなく、画像や映像による情報提供はクラウドサービス利用者の理解を助ける。

[19] 総務省が策定・公表する「クラウドサービスの安全・信頼性に係る情報開示指針」に基づいて、一般社団法人日本クラウド産業協会（ASPIC）が、クラウド事業者からの情報開示が適切に行われていることについて、分野別の認定制度を設けている。

＜コラム＞　日本語（化）の問題

海外で開発されたサービスを日本で提供する場合、翻訳（日本語化）の際に十分注意する必要がある。翻訳された日本語がわかりにくかったために、設定ミスが起きた事例がある。設定メニューや設定マニュアル等の翻訳の際には、日本語がネイティブな担当者が最終チェックをすることが望ましい。

なお、国内企業の日本語母語話者が作成したマニュアルでも意味がわかりにくいものがあるので、組織としてのレビューが必要なのは同様である。

Ⅳ．２．４　利用者別の対応

【目的】

同じサービスを提供しても利用者の業務に関わる環境によってサービスの設定値が異なる場合がある。このような場合は、利用者ごとに必要とする情報が異なる。クラウドサービス事業者は、クラウドサービス利用者ごとの特性を考慮して、適切な情報提供を心がけること。

Ⅳ．２．４．１　【推奨】利用者の特性に応じた情報提供

クラウドサービス利用者ごとの特性に応じた情報を提供すること。

Ⅳ．２．５　タイムリーな情報提供

【目的】

システムのぜい弱性の解消のための設定変更など、すぐに対応すべき設定変更もある。クラウドサービス事業者は、クラウドサービス利用者に対してタイムリーな情報提供を心がける必要がある。

Ⅳ．２．５．１　【基本】システム動作環境の変更等に伴うタイムリーな情報提供

クラウドサービスの機能向上、ぜい弱性対処などのリリースに伴い、システム動作環境の設定変更が生じた場合などは、タイムリーに情報提供すること。

【ベストプラクティス】

i.　随時発生する仕様変更、ぜい弱性対応などに対応するため、オンラインマニュアルやチャット機能の整備を検討する。

Ⅳ．２．５．２　【基本】公開されたぜい弱性の影響に伴うタイムリーな情報提供

公開されたぜい弱性がクラウドサービスに与える影響を防止するために設定値等の変更が必要な場合は、タイムリーに情報提供すること。

【ベストプラクティス】

i.　他社ソフトウェアやOSS（Open Source Software）等を利用するクラウドサービス事業者

は、これらに関するぜい弱性が公開された場合、それがクラウドサービスに与える影響を防止する対策として設定値等の変更が必要な場合は、クラウドサービス利用者にタイムリーに情報提供できる体制を整備する。

※情報提供のみならず、緊急に対処が必要な場合等は、クラウドサービス提供者、クラウドサービス利用者で予め対処について合意しておくなどの措置が必要となる。

ii. 脆弱性は情報が更新されることもあるので、更新情報も正しく伝えられるように考慮する

Ⅳ．３　学習コンテンツや学習機会の提供

Ⅳ．３．１　学習コンテンツの提供

【目的】

クラウドサービス利用者の知識不足や理解不足による設定ミスを減らすためには、システム動作環境の設定そのものだけではなく、周辺知識を含む幅広い知識を身に着けてもらう必要がある。クラウドサービス事業者は、クラウドサービス利用者に環境の設定について正しく理解してもらうために、有償又は無償で、学習の機会やコンテンツを提供することが望ましい。

Ⅳ．３．１．１　【推奨】体系的な学習コンテンツの提供

クラウドコンピューティングのしくみ、自社のサービスの構成など、環境の設定を行うためのバックグラウンドの知識についてできるだけ体系的、網羅的に学ぶことのできる学習コンテンツをクラウドサービス利用者に提供すること。

Ⅳ．３．１．２　【推奨】わかりやすい形式のコンテンツの作成

学習コンテンツの提供においても、設定マニュアルと同様に、動画の活用等、できるだけわかりやすい形式での提供をこころがけること。

Ⅳ．３．２　学習機会の提供　－　環境の設定に関する説明

【目的】

設定マニュアルを読んだだけでは、理解が不十分な利用者もいる。説明を聞くことによって理解が深まることも多い。このため、環境の設定に関するセミナーや研修を開催し、クラウドサービス利用者が学習する機会を効率的に提供する等、クラウドサービス事業者がクラウドサービス利用者に環境の設定に関する説明を行う機会を設けることが望ましい。

Ⅳ．３．２．１　【推奨】セミナーや研修の開催

環境の設定に関する説明を行う機会として、セミナーや研修の開催を企画すること。

【ベストプラクティス】

i. セミナーの講師としては、認定取得者のように専門知識が豊富な者を選定する必要がある。
ii. ユーザを集めた「ユーザ会」を組織して、そこに対して上記のような学習の機会を提供している企業もある。ユーザ同士のコミュニティを形成することで、利用者同士の情報共有の機会にもなっている。

Ⅳ．３．２．２ 【推奨】コンサルティングサービスの提供

環境の設定に関する個別の相談に応じるために、できるだけコンサルティングサービス（有償又は無償）や当該クラウドサービスのパートナーとなる SIer 等に関する情報を提供すること。少なくとも相談窓口を明確にすること。

Ⅳ．４　利用者支援ツールの提供

クラウドサービス事業者は、利用者側の管理・運用を支援するツールを提供することが望ましい。

Ⅳ．４．１　設定項目管理ツールの提供

【目的】

利用者の管理作業を軽減することも設定ミスの削減につながる。クラウドサービス事業者は、できるだけシステム動作環境の設定項目管理ツールを提供することが望ましい。また、自社のツール以外に、サードパーティによる設定項目管理ツールを紹介することも考えられる。

Ⅳ．４．１．１　【推奨】設定項目管理ツールの提供

システム動作環境の設定項目について、利用者が把握し管理可能なツールを確実に提供すること。

Ⅳ．４．２　設定項目診断ツールの提供

【目的】

人間の作業にミスはつきものであり、ゼロにすることは難しいので、ミスをしても問題化する前に発見し修正する手段を用意しておく必要がある。そのために、クラウドサービス提供者は、クラウドサービス利用者が環境の設定を正しく行ったかをチェックするためのツールを提供することが望ましい。設定項目の診断ツールについてのイメージを図表Ⅳ．４．２－１に示す。危険のある設定値には、赤色で注意を促すなどで分かりやすく示すことが望ましい。また、自社のツール以外に、サードパーティによる設定項目診断ツールを紹介することも考えられる。

図表Ⅳ．４．２－１　設定項目診断ツールのイメージ

Ⅳ．４．２．１　【推奨】設定項目診断ツールの提供

利用者が設定したシステム動作環境の設定項目について、セキュリティ上の診断可能なツールを確実に提供すること。

【ベストプラクティス】

i. 特に重要であるIDの管理（IDとアクセス管理）については診断ツールを提供することが望ましい。

ii. 設定診断を実行した後、危険な設定になっているものを自動で復元する機能を持っているツールもある。

Ⅳ．５　システムの改善　－　ミスが発生しにくいシステムの提供

Ⅳ．５．１　設定方法の見直し

【目的】

クラウドサービス事業者は、そもそも設定ミスが発生しにくいシステムを開発するように努力すべきである。また、マニュアルを読まない利用者もいるので、読まなくても間違わないように設定メニューの工夫も必要である。

Ⅳ．５．１．１ 【基本】設定項目のメニュー化／リスト化

設定方法の簡素化を図ること。

【ベストプラクティス】

i. キーボードから文字を入力する方式より、メニューやリストからクリックやタップで選択する方式のほうが一般的に間違いが少なくなる。
ii. 選択肢ごとに、その意味や使い方を記述したヘルプウィンドウを出力する機能も利用者の助けとなる。
iii. 専門知識を持たない利用者が、当該設定項目に触れなくても済むようにシステム構成のテンプレート化や構成ツールを提供することを検討する。

Ⅳ．５．１．２　【基本】選択肢の表記の工夫

設定の選択肢には、できるだけ誤解を招きにくい表現を用いること。

【ベストプラクティス】

i. 表現については、「Ⅳ．２．３．１　【基本】分かりやすい情報の提供」を参照されたい。
ii. 専門知識を持たない利用者が、当該設定項目に触れなくても済むようにシステム構成のテンプレート化や構成ツールを提供することを検討する。

Ⅳ．５．２ デフォルト値の見直し

【目的】

デフォルト値のままで何も設定を行わなかったことが原因で、情報漏えい等の問題が起きた事例は多い。クラウドサービス利用者が設定を忘れた場合でも問題が発生しないように、デフォルト値はセキュリティの高い設定とすること。

Ⅳ．５．２．１ 【基本】デフォルト値の見直し

デフォルトで提供されるシステム動作環境の設定値は、可能な限りセキュリティの高い設定とすること。

【ベストプラクティス】

i. 認証方式、アクセス権限及び通信や操作ログの取得等はデフォルトでセキュリティが高くなるような設定としておくことが望ましい。

ii. 何も設定をしない場合は、セキュリティが最も高い設定となるようなシステム提供が望ましい。

iii. 専門知識を持たない利用者が、当該設定項目に触れなくても済むようにシステム構成のテンプレート化や構成ツールを提供することを検討する。

Ⅳ．５．３　セルフチェック機能の追加

【目的】

設定後にチェックしても、設定者がそういう設定にした理由や経緯を覚えていないことがある。クラウドサービス利用者が環境の設定作業を行う際に、作業完了前にチェックできる機能があることが望ましい。

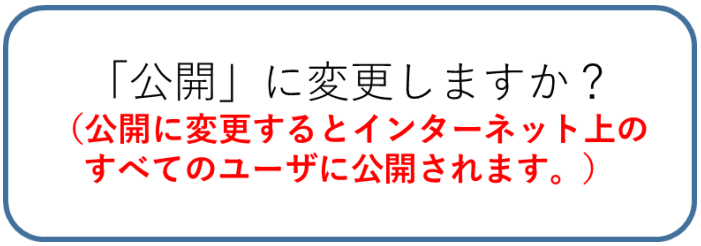
Ⅳ．５．３．１　【推奨】セルフチェック機能の追加

設定項目については、可能な限り、チェック機能を設けること。

【ベストプラクティス】

i. 設定項目を変更しようとする際に、セキュリティ上の危険が伴う可能性がある場合にアラームが出力されるシステムもある。
アラームのイメージを図表Ⅳ．５．３．１－１に示す。

図表Ⅳ．５．３．１－１



Ⅳ．５．４　利用者における設定機会の削減

【目的】

そもそも利用者（人間）が設定するためにミスが発生するのであれば、設定する項目を減らすのが有効である。クラウドサービス事業者は、不必要な設定や全ての利用者が同じ設定値を選択する項目等がないか等の洗い出しを行い項目数そのものを削減することや、セキュリティ上問題のある設定値が選択できないように、選択肢の削減に努めることが必要である。

Ⅳ．５．４．１ 【基本】設定項目数及び選択肢の削減

クラウドサービス利用者のシステム動作環境の設定における設定項目数及び選択肢の削減に努めること。

Ⅳ．５．４．２ 【基本】設定変更回数の削減

クラウドサービス利用者が設定変更をしなければならない機会をできるだけ少なくするよう努めること。

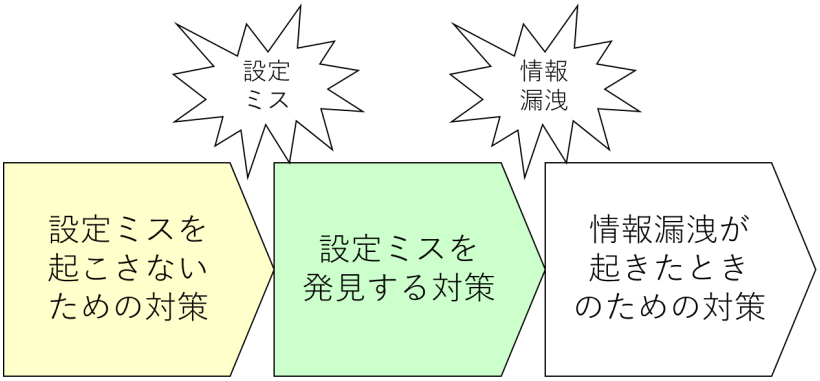
Ⅳ．５．５ 暗号化機能の提供

【目的】

クラウド設定の診断や調査を行っても設定不備が見つからず、情報漏えい等の問題が起きた事例も多い。設定ミスを突かれて情報漏えいが起きた場合の対策も考えておく必要がある。万が一、設定不備により情報が漏えいした場合の対策としては、データの暗号化機能の提供がある。

図表Ⅳ．５．５－１に事後対策としての暗号化のイメージを示す。

図表Ⅳ．５．５－１ 事後対策としての暗号化



Ⅳ．５．５．１ 【推奨】暗号化機能の提供と設定

暗号化の機能を提供し、利用者がセキュリティ上の脅威を考慮したうえで重要な情報において設定可能となるようにすること。

【ベストプラクティス】

i. パスワード、個人情報等の機密性の高い情報は暗号化し管理する。

ii. 暗号化のガイドラインとしては、下記のものがある。

・IPA 暗号鍵管理ガイドライン[20]

・CRYPTREC暗号リスト[21]

iii. 暗号化については、データベース上暗号化してもアクセス経路が乗っ取られた場合は平文で情報の詐取が行われる場合がある。セキュリティ上の危険性を十分理解して使用するように、クラウドサービス利用者に注意を促すこと。

[20] https://www.ipa.go.jp/security/vuln/ckms.html
[21] https://www.cryptrec.go.jp/list.html

Ⅳ．６　継続的な改善　－　ＰＤＣＡを回す

クラウドサービス事業者は、常に自社サービスのセキュリティ強化のための情報収集を行い、継続的にサービスの改善を行う必要がある。設定に関する課題に関しても、社内外の情報を蓄積・分析し、それに基づく組織的な改善活動を行う必要がある。

Ⅳ．６．１　情報収集

【目的】

「利用者からのフィードバック」、「公的機関等からの情報収集」及び「その他の情報収集における事実確認」等、重要な情報収集を確実に行う。

Ⅳ．６．１．１　【基本】利用者からのフィードバック情報収集

クラウドサービス利用者からのフィードバック情報の収集に努めること。

【ベストプラクティス】

i. 実際に設定不備が発生した場合は、詳細な情報を収集して分析する必要がある。
ii. 設定不備を削減するためには、バッドプラクティス（べからず集）を収集し、ユーザに提供することも有効である。
iii. クラウドサービス利用者と連携し、できればフィードバックの自動収集の仕組みを利用側環境に入れておくことが望ましい。

Ⅳ．６．１．２　【基本】公的機関等からの情報収集

内閣官房内閣サイバーセキュリティセンター（NISC）や情報処理推進機構（IPA）等の公的機関が提供しているセキュリティ情報等を収集し、自社サービスとの関連をチェックすること。

Ⅳ．６．１．３　【基本】その他の情報収集における事実確認

公的機関からの情報以外の情報は、事実を十分確認の上収集すること。

【ベストプラクティス】

i. ＯＳやミドルウェアの提供者からの情報を収集する。
ii. セキュリティベンダーからの情報を収集する。
iii. 他社の事例であっても設定不備に起因するセキュリティ事故に関する情報も参考とする。

Ⅳ．６．２ サービスの改善

【目的】

収集した情報に基づき、組織としてサービスの改善を確実に行う。

Ⅳ．６．２．１ 【基本】サービスの改善

収集した情報に基づき、自社のサービスを改善すること。

【ベストプラクティス】

i. 社内での検討会を開催し、システムやサービスの改善計画に反映すること。

ii. 改善計画に基づき、システムの改善や、設定マニュアルの改定等のサービスの改善を行う。

iii. チェックリスト等の追加もサービスの改善につながる。

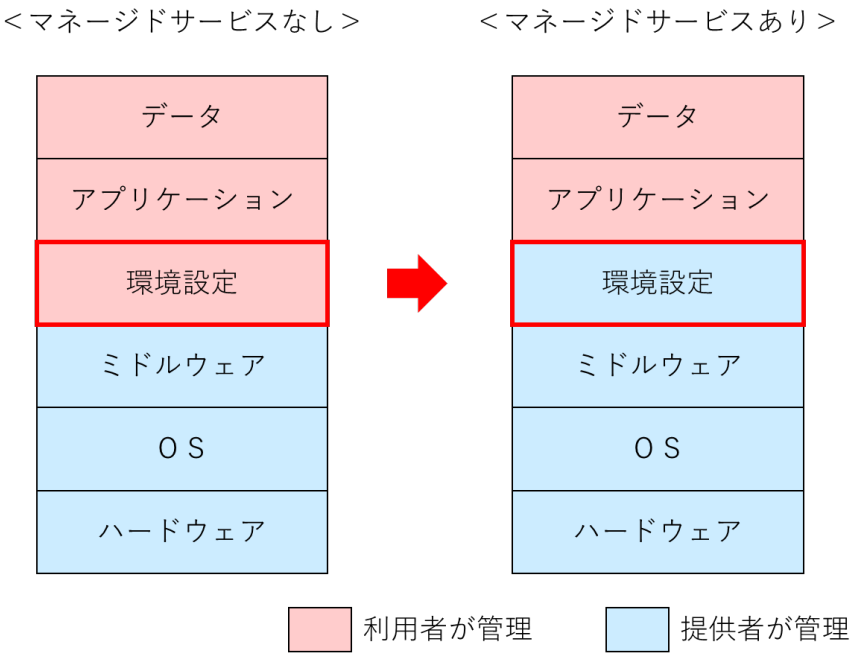
Ⅳ．７　マネージドサービスの提供

Ⅳ．７．１　マネージドサービスの提供

【目的】

近年、クラウドサービス事業者の中には、ソフトウェアの管理・運用を含めて一体的に請け負うサービスである「マネージドサービス」を提供する企業が出てきている。このサービスを利用すれば、クラウドサービス利用者は利用者で実施すべき環境設定作業から解放され、一部の設定に関する負担をクラウドサービス事業者側に移転させることが可能となる。図表Ⅳ．７．１－１にマネージドサービス提供による利用者の負担軽減イメージを示す。

図表Ⅳ．７．１－１　マネージドサービスによる利用者の負担軽減イメージ



Ⅳ．７．１．１　【推奨】マネージドサービスの提供

クラウドサービス利用者のニーズ等も勘案して、適切な範囲でマネージドサービスの提供を検討すること。あるいは、自社の提供サービスに対する外部のマネージドサービス事業者を紹介すること。

参考資料

ANNEX 対策一覧

項番	対策項目	対策内容	区分
Ⅲ クラウドサービス利用側に求められる対策			
Ⅲ．１ 組織体制・人材育成			
Ⅲ．１．１ 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			
Ⅲ．１．１．１	**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、全社的又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すること。	基本
Ⅲ．１．１．２	**事業部門等が独自に利用する場合のルール形成**	利用者組織において、利用者組織の事業部門等が独自にクラウドサービスを利用する場合がある。事業部門等が組織のセキュリティ管理者やクラウドサービス管理者が知らないままクラウドサービスを利用することがないように条件付きで許可するなど、組織のビジネス環境や方針に基づいて利用する場合のルールを明確にし、文書化すること。	基本
Ⅲ．１．１．３	**設定診断等の支援ツール利用に組織として取り組む**	クラウドサービス利用の高度化・複雑化に伴い、設定が必要な項目の量的な増加や組合せの整合性を取ることなどの複雑化が課題となる。これらの課題に対処するため、クラウドサービス事業者や独立のツールベンダーから、設定値全体の監視やルールを外れた設定値を警告・復元するなどの支援ツールが提供されている場合がある。クラウドの導入や運用管理に当たり、これらの支援ツール等の積極的利用に取り組むことについて検討し、組織として予算化、計画化することが望ましい。	推奨
Ⅲ．１．１．４	**クラウドに関する人材の組織的育成**	設定に関する知識やノウハウの向上を実現するために、組織的にクラウド資格等の取得やクラウドサービス事業者が用意するセミナーの受講及び知識の組織内共有等について計画し、文書化すること。また、クラウドに関する人材を組織的に育成するため、クラウドに関する人材を適切に評価できる枠組みを構築すること。	基本
Ⅲ．１．２ 技術情報の収集			
Ⅲ．１．２．１	**技術情報の収集**	クラウドサービスの変化に伴う各種設定値の変更等の技術情報については、組織として情報収集、リスク分析、対策立案プロセスを確立し文書化を行うこと。	基本
Ⅲ．１．３ 人材育成			
Ⅲ．１．３．１	**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すること。	基本
Ⅲ．１．３．２	**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についての技術力を継続的に向上させること。	基本
Ⅲ．１．４ コミュニケーション			
Ⅲ．１．４．１	**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すること。	基本
Ⅲ．２ 作業規則・マニュアル			
Ⅲ．２．１ 作業規則やマニュアルの整備			
Ⅲ．２．１．１	**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すること。	基本
Ⅲ．２．１．２	**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の混入を防ぐため、作業手順書を整備すること。	基本
Ⅲ．２．１．３	**ヒューマンエラー対策**	作業手順書にヒューマンエラー対策を確実に組み込むことと。	基本
Ⅲ．２．１．４	**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むこと。	基本
Ⅲ．３ クラウドシステム動作環境の設定管理			
Ⅲ．３．１ クラウドセキュリティに係る設定項目の確認			
Ⅲ．３．１．１	**設定項目の把握と設定**	典型的なクラウドの設定項目について知り、自社で利用する IaaS/PaaS の設定項目を把握し設定すること。（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）	基本
Ⅲ．３．１．２	**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（予防的措置と呼ぶ）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すること。	基本
Ⅲ．３．２ 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			
Ⅲ．３．２．１	**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、準備し対応すること。	基本

Ⅲ．３．３　その他のリスクへの対応			
Ⅲ．３．３．１	**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、対応方針を文書化すること。	基本
Ⅲ．４　クラウドシステム動作環境に関する設定の方法論			
Ⅲ．４．１　ノウハウの蓄積			
Ⅲ．４．１．１	**クラウドシステムの動作環境設定に関するノウハウ蓄積**	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すること。	推奨
Ⅲ．４．２　支援ツール等の活用			
Ⅲ．４．２．１	**支援ツールや外部診断サービス等の活用**	システム動作環境の設定に関わる設定者及び管理者は、支援ツールや外部診断サービス等を活用すること。	推奨
Ⅲ．４．３　定期的な設定値のチェックと対応			
Ⅲ．４．３．１	**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、適切に対応すること。	基本
Ⅳ　クラウドサービス提供側に求められる対策			
Ⅳ．１　組織体制・人材育成			
Ⅳ．１．１　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			
Ⅳ．１．１．１	**クラウドサービス提供におけるガバナンスの確保**	クラウドサービス提供者は、設定不備の抑止・防止に関す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提供方針等）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すること。	基本
Ⅳ．１．１．２	**設定診断等の支援ツール提供に対する組織的取組**	クラウドサービス利用の高度化・複雑化に伴い、設定が必要な項目が量的な増加や組合せの整合性を取ることなどの複雑化が課題となる。クラウドサービス利用者の立場に立った支援ツール等の提供について積極的に取り組むことを検討し、組織として予算化、計画化することが望ましい。	推奨
Ⅳ．１．１．３	**クラウドに関する人材の組織的育成**	クラウドサービス提供におけるシステム動作環境の設定に関する知識やノウハウの向上を実現するために、組織的にクラウド資格等の取得やセミナー受講等について計画し、文書化すること。また、クラウドに関する人材を組織的に育成するための基盤として、クラウドに関する人材を適切に評価できる枠組みを構築すること。	基本
Ⅳ．２　情報提供			
Ⅳ．２．１　正しい情報の提供			
Ⅳ．２．１．１	**正しい情報の提供**	組織としてシステム動作環境の設定に関する正しい情報を確実に提供すること。	基本
Ⅳ．２．２　十分な情報の提供			
Ⅳ．２．２．１	**十分な情報の提供**	組織としてシステム動作環境の設定に関する十分な情報を確実に提供すること。	基本
Ⅳ．２．３　わかりやすい情報の提供			
Ⅳ．２．３．１	**わかりやすい情報の提供**	組織としてシステム動作環境の設定に関するわかりやすい情報を確実に提供すること。	基本
Ⅳ．２．４　利用者別の対応			
Ⅳ．２．４．１	**利用者の特性に応じた情報提供**	クラウドサービス利用者ごとの特性に応じた情報を提供すること。	推奨
Ⅳ．２．５　タイムリーな情報提供			
Ⅳ．２．５．１	**システム動作環境の変更等に伴うタイムリーな情報提供**	クラウドサービスの機能向上、ぜい弱性対処などのリリースに伴い、システム動作環境の設定変更が生じた場合などは、タイムリーに情報提供すること。	基本
Ⅳ．２．５．２	**公開されたぜい弱性の影響に伴うタイムリーな情報提供**	公開されたぜい弱性がクラウドサービスに与える影響にを防止するために設定値等の変更が必要な場合は、タイムリーに情報提供すること。	基本
Ⅳ．３　学習コンテンツや学習機会の提供			
Ⅳ．３．１　学習コンテンツの提供			
Ⅳ．３．１．１	**体系的な学習コンテンツの提供**	クラウドコンピューティングのしくみ、自社のサービスの構成など、環境の設定を行うためのバックグラウンドの知識についてできるだけ体系的、網羅的に学ぶことのできる学習コンテンツをクラウドサービス利用者に提供すること。	推奨
Ⅳ．３．１．２	**わかりやすい形式のコンテンツの作成**	学習コンテンツの提供においても、設定マニュアルと同様に、動画の活用等、できるだけわかりやすい形式での提供をこころがけること。	推奨
Ⅳ．３．２　学習機会の提供　ー　環境の設定に関する説明			
Ⅳ．３．２．１	**セミナーや研修の開催**	環境の設定に関する説明を行う機会として、セミナーや研修の開催を企画すること。	推奨

Ⅳ．３．２．２	**コンサルティングサービスの提供**	環境の設定に関する個別の相談に応じるために、できるだけコンサルティングサービス（有償又は無償）や当該クラウドサービスのパートナーとなる SIer 等に関する情報を提供すること。少なくとも相談窓口を明確にすること。	推奨
Ⅳ．４　利用者支援ツールの提供			
Ⅳ．４．１　設定項目管理ツールの提供			
Ⅳ．４．１．１	**設定項目管理ツールの提供**	システム動作環境の設定項目について、利用者が把握し管理可能なツールを確実に提供すること。	推奨
Ⅳ．４．２　設定項目診断ツールの提供			
Ⅳ．４．２．１	**設定項目診断ツールの提供**	利用者が設定したシステム動作環境の設定項目について、セキュリティ上の診断可能なツールを確実に提供すること。	推奨
Ⅳ．５　システムの改善　－　ミスが発生しにくいシステムの提供			
Ⅳ．５．１　設定方法の見直し			
Ⅳ．５．１．１	**設定項目のメニュー化／リスト化**	設定方法の簡素化を図ること。	基本
Ⅳ．５．１．２	**選択肢の表記の工夫**	設定の選択肢には、できるだけ誤解を招きにくい表現を用いること。	基本
Ⅳ．５．２　デフォルト値の見直し			
Ⅳ．５．２．１	**デフォルト値の見直し**	デフォルトで提供されるシステム動作環境の設定値は、可能な限りセキュリティの高い設定とすること。	基本
Ⅳ．５．３　セルフチェック機能の追加			
Ⅳ．５．３．１	**セルフチェック機能の追加**	設定項目については、可能な限りチェック機能を設けること。	推奨
Ⅳ．５．４　利用者における設定機会の削減			
Ⅳ．５．４．１	**設定項目数及び選択肢の削減**	クラウドサービス利用者のシステム動作環境の設定における設定項目数及び選択肢の削減に努めること。	基本
Ⅳ．５．４．２	**設定変更回数の削減**	クラウドサービス利用者が設定変更をしなければならなくなる機会をできるだけ少なくするよう努めること。	基本
Ⅳ．５．５　暗号化機能の提供			
Ⅳ．５．５．１	**暗号化機能の提供と設定**	暗号化の機能を提供し、利用者がセキュリティ上の脅威を考慮したうえで重要な情報において設定可能となるようにすること。	推奨
Ⅳ．６　継続的な改善　－　ＰＤＣＡを回す			
Ⅳ．６．１　情報収集			
Ⅳ．６．１．１	**利用者からのフィードバック情報収集**	クラウドサービス利用者からのフィードバックの収集に努めること。	基本
Ⅳ．６．１．２	**公的機関等からの情報収集**	内閣サイバーセキュリティセンター（NISC）や情報処理推進機構（IPA）等の公的機関が提供しているセキュリティ情報等を収集し、自社サービスとの関連をチェックすること。	基本
Ⅳ．６．１．３	**その他の情報収集における事実確認**	公的機関からの情報以外の情報は、事実を十分確認の上、収集すること。	基本
Ⅳ．６．２サービスの改善			
Ⅳ．６．２．１	**サービスの改善**	収集した情報に基づき、自社のサービスを改善すること。	基本
Ⅳ．７　マネージドサービスの提供			
Ⅳ．７．１　マネージドサービスの提供			
Ⅳ．７．１．１	**マネージドサービスの提供**	クラウドサービス利用者のニーズ等も勘案して、適切な範囲でマネージドサービスの提供を検討することや自社の提供サービスに対する外部のマネージドサービス事業者を紹介すること。	推奨