クラウドの設定ミス対策

ガイドブック

２０２４．４

総務省

目次

コラム

第１章

本ガイドブックの目的と使い方

本ガイドブックの目的・対象読者・構成

■本ガイドブックの目的

このガイドブックは、総務省が令和４年１０月に公表した「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」（以下「設定ガイドライン」という。）の内容を、わかりやすく解説するために作成したものです。設定ガイドラインをさらに多くの方に活用していただくことにより、クラウドの設定ミスの防止に役立ててもらうことを目的としています。

■対象読者

このガイドブックは、クラウドサービスを利用する企業等を主なターゲットにしています。利用企業等から委託を受けて、クラウドの設定を行う企業も含まれます。

なお、クラウドサービスには、主にＳａａＳ（Software as a Service）、Ｐａａ Ｓ（Platform as a Service）、Ｉａａ Ｓ（Infrastructure as a Service）の３種類がありますが、すべてのクラウドサービスの利用者を対象としています。

部門としては、クラウドの設定に責任のある部署を対象としています。これは、いわゆる情報システム部門に限りません。事業部門やスタッフ部門で、個別にクラウドサービスを導入している場合もあるので、そういう部門の方も人も対象に含まれます。

■ガイドブックの構成と使い方

このガイドブックは、本章と設定ミス対策の前提となる考え方、設定ミスの対策の３章構成になっています。

設定ミスの対策については、自社の条件に合うものを選択して実施してください。また、対策の詳細については、ぜひ設定ガイドラインを参照してください。本文に（→III.1.1.1）のような番号が出てくるのは、設定ガイドラインの関連する目次の番号を表しています。

このガイドブックは、クラウドサービスを導入する際にも、導入中のクラウドサービスを点検する際にもご活用ください。

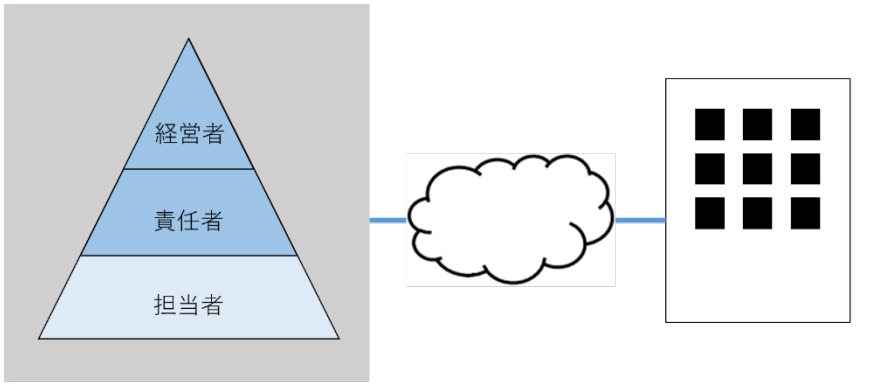
なお、設定ガイドラインは、以下のアドレスからダウンロードできます。

https://www.soumu.go.jp/main_content/000843318.pdf

●クラウドサービスの種類

種類	読み方	概要
ＳａａＳ（Software as a Service）	サース	業務に使われるアプリケーション（ソフトウェア）を提供するサービス。会計、名刺管理、Ｗｅｂ会議など、各種の業務用アプリケーションを提供。
ＰａａＳ（Platform as a Service）	パース	ソフトウェアの開発や実行に必要な環境を提供するサービス。開発支援ツールやデータベースなどのミドルウェア（ソフトウェア）などを提供。
ＩａａＳ（Infrastructure as a Service）	イアース	システムのインフラであるハードウェアを提供するサービス。ＣＰＵ（演算装置）、ストレージ、ネットワークなどを提供

●対象読者は利用者側の責任者・経営者



●本ガイドブックの構成

章	内容
第１章　本ガイドブックの目的と使い方	クラウドの設定ガイドライン策定の経緯と本ガイドブックの目的等について説明します。
第２章　設定ミス対策の前提となる考え方	設定ミスの対策を検討する上で、その前提となる基本的な考え方について説明します。
第３章　設定ミスの対策	設定ガイドラインにある設定ミスの対策を、４つに分類して解説します。
コラム	クラウドサービスの最新の動向について解説します。

設定ガイドライン策定の背景

■クラウドサービスの普及と設定ミスの増加

クラウドサービスが普及し、重要な社会インフラになるとともに、その設定ミスによる情報漏洩等のトラブルが増えています。ＩＰＡ（情報処理推進機構）が毎年発表している「情報セキュリティ１０大脅威」でも、2024 年には「不注意による情報漏洩等の被害」が 6 位にランクインしています。

■設定ミスのリスク

クラウドの設定ミスによるリスクで代表的なものは、情報漏洩が起きることです。特に、個人情報や機密情報が漏洩するとより深刻な事態になります（→Ⅱ.1.1）。設定ミスの事故の報道は情報漏洩に関するものが多いです。

なお、悪意を持った攻撃者による情報の窃取だけでなく、意図せず一般の人に個人情報が公開されることも問題になります。

情報漏洩の他にも、ファイルへのアクセスの設定にミスがあると、ファイルが破壊（削除、改ざん）される可能性があります。また、マルウェアを送り込まれて、感染してしまうことも考えられます。

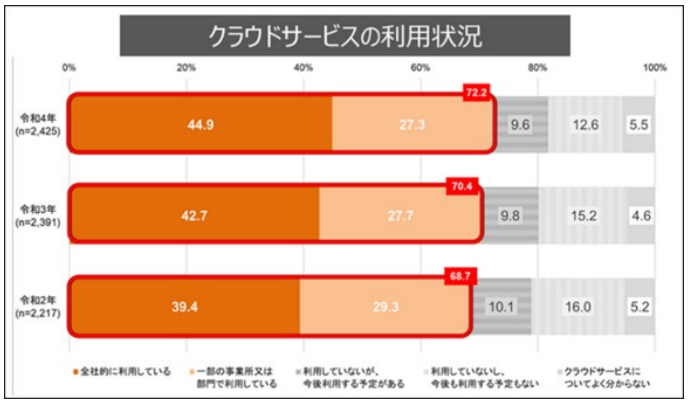
さらに、管理者のＩＤやパスワードが漏洩すれば、システムが乗っ取られたり、システムが停止したりするなど、あらゆる脅威の発生が考えられます。（→Ⅱ.1.1）

■情報漏洩やファイル破壊が引き起こすもの

設定ミスにより、情報漏洩やファイル破壊、さらにはシステム停止などの事故が起きると、企業の経営にも大きな影響が出る可能性があります。

情報漏洩により、企業の信用が失墜して受注機会を失うかもしれません。被害者から損害賠償を求められたり、破壊されたファイルの復旧に費用がかかって、損失が発生するかもしれません。設定ミスから経営問題にまで発展する可能性があることを理解しておく必要があります。

●クラウドサービスの普及　―　クラウドサービスの利用者は７０％を超える

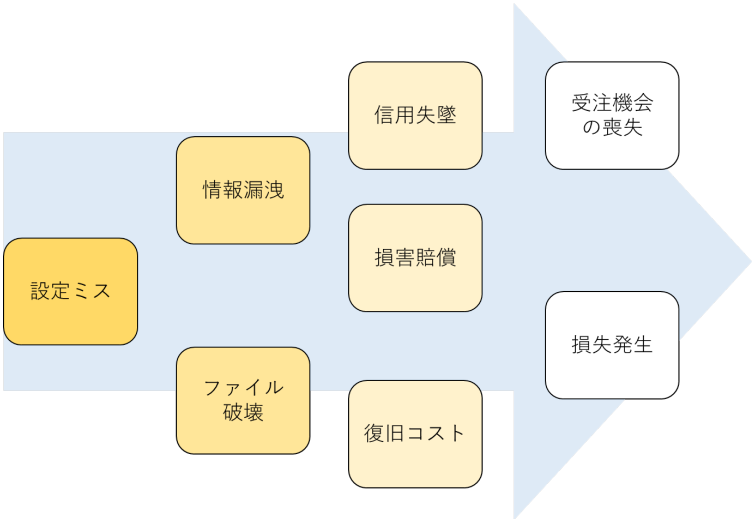


総務省「令和４年度通信利用動向調査」より

●不注意による情報漏洩

順位	「組織」向け脅威	初選出年	10 大脅威での取り扱い（2016 年以降）
1	ランサムウェアによる被害	2016 年	9 年連続 9 回目
2	サプライチェーンの弱点を悪用した攻撃	2019 年	6 年連続 6 回目
3	内部不正による情報漏洩等の被害	2016 年	9 年連続 9 回目
4	標的型攻撃による機密情報の窃取	2016 年	9 年連続 9 回目
5	修正前を狙う攻撃（ゼロデイ攻撃）	2022 年	3 年連続 3 回目
6	不注意による情報漏洩等の被害	2016 年	6 年連続 7 回目
7	脆弱性対策情報の公開に伴う悪用増加	2016 年	4 年連続 7 回目

●設定ミスのリスク



設定ミスの事例

■設定ガイドラインにある事例

設定ガイドラインでは、以下の３つの事例を紹介しています。（→Ⅱ.2.1）

①デフォルト変更の事例

クラウドサービス提供者（ＳａａＳ事業者）が、サービスの機能変更を行った際に、ユーザアクセスに関する設定のデフォルト（既定値）のセキュリティレベルが下がってしまい、利用者が設定を行わずに、デフォルトのまま利用したため、機密情報が流出した事例です。

②個人利用の事例

従業員が個人的にクラウドサービスを利用し、自社の業務で扱う機密情報をファイルに保存していた事例で、こ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発覚ました。

③業務委託先のミスの事例

自社のシステムをクラウドに移行する際に、ストレージの設定が「公開」になっていたため、長期間機密情報が公開されていたという事例で、業務委託先による設定ミスでした。

■2023 年度の事例

2023 年度にも事故が発生しています。その中でも、特に注目すべきものを紹介します。

①取引先の設定ミス　－　中小企業も狙われている

これは最も話題になった事例で、大手企業の取引先である子会社でクラウドの設定ミスがあり、大量の個人データが閲覧可能になっていたという事例です。

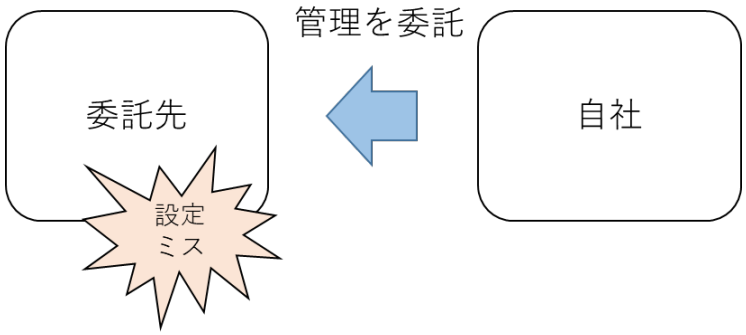
この事例の教訓として、自社のセキュリティだけでなく、取引先のセキュリティにも留意する必要があることがあげられます。

②協力企業の設定ミス　－　専門家でもミスをする

最近では、設定自体を自社ではなく、協力企業に委託して行うことも増えています。この事例は、委託した企業が設定ミスをしたという事例です。

この事例から、専門家であってもミスをすることがあるので、システムによるチェックなどを含めた総合的な対策が必要なことがわかります。

●委託先のミスの事例



プロでもミスをすることがある

●2023 年度の設定ミスの事例

発生年	概要
2024 年	セミナーのオンライン受講システムで、受講者が、過去に他のコースを受講した人の名前、メールアドレス、受講履歴などの個人情報が閲覧できる状態になっていた。
2023 年	ファイル共有サービスの情報公開範囲の設定のミスにより、自社やグループ会社の顧客、取引先、退職者などの情報が「リンクを知っているインターネット上のすべての人」に閲覧可能だった。
2023 年	イベントの申し込みフォームの設定を誤り、他の参加者の個人情報がインターネット上で閲覧できる状態だった。
2023 年	利用者のアカウント情報の一部が、不適切なデータ交換が行われている Web サイトに公開されている、との情報提供があった。
2023 年	開催を予定しているイベントの参加申込者の個人情報が、申し込みフォーム上で閲覧できる状態だった。
2023 年	ウェビナーに参加を申し込んだ人の個人情報が、インターネット上で閲覧可能な状態になっていた。情報には名前やメールアドレス、電話番号、住所、生年月日、年収、金融資産額、口座番号が含まれる。
2023 年	ある利用者がオンデマンド放送にアクセスしてログインしたときに、同時にログインしている別の人がいた場合、その人の個人データの一部が編集可能だった。
2023 年	子会社のクラウド環境の誤設定で、顧客情報が外部からアクセス可能な状態だった。

用語の定義

このガイドブックで使う基本的な用語を定義しておきます。

■クラウドとクラウドサービス

　このガイドブックでは、「クラウド」と「クラウドサービス」を以下のように定義しておきます。

　クラウド：「コンピュータシステムの資源の一部を、インターネット等のネットワーク経由で利用するしくみ」
　クラウドサービス：「クラウドのしくみを使って提供されるサービス」

　クラウドサービスには、コンピュータシステムの資源をどこまで利用するかによってＳａａＳ、ＰａａＳ、ＩａａＳの３種類があります。ＩａａＳとＰａａＳは同じ事業者から提供されていることが多いです。具体的には以下のようなものが提供されています。
①ＩａａＳ＋ＰａａＳ：コンピューティング、ストレージ、データベースなど
②ＳａａＳ：オフィスソフト、顧客管理、会計ソフト、名刺管理、Ｗｅｂ会議など

■設定ミス

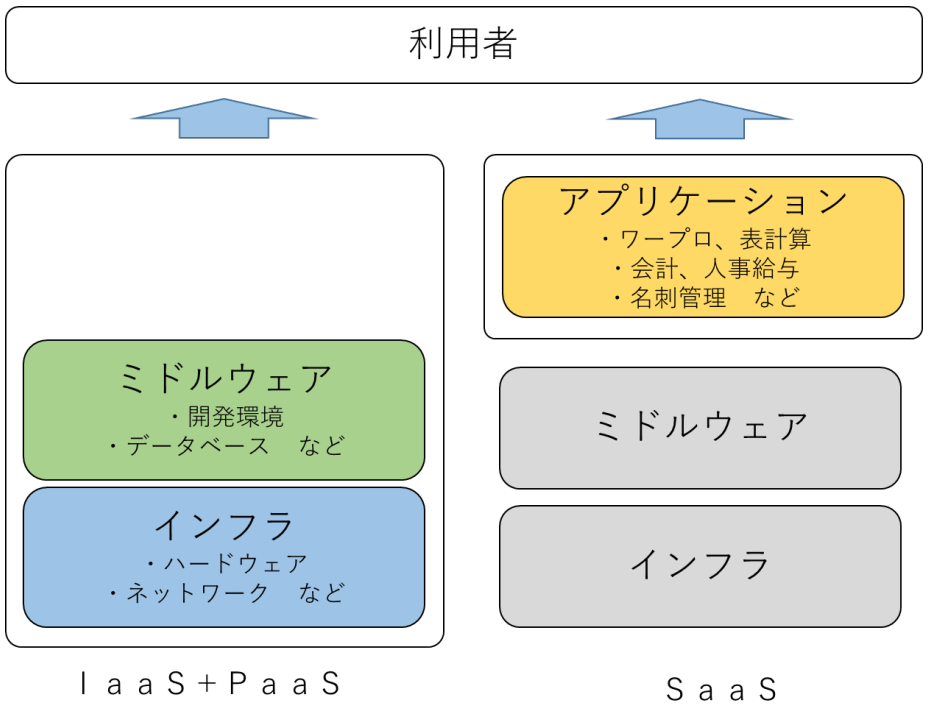
　設定ミスには、クラウドサービスのさまざまな利用条件の設定をする際に、誤った値を設定してしまうこと（誤設定）、何も設定しないこと（未設定）により、不都合な値が有効になっていること、一度設定をした後、環境の変化により設定値を変更しなければならなくなったのに、変更していないこと（未変更）が含まれます。

■デフォルト（またはデフォルト値）

　クラウドに限らず、システムの設定の話の中には、「デフォルト」とか「デフォルト値」という言葉がよく出てきます。デフォルト（default）とは、既定（あらかじめ決められている）という意味です。コンピュータシステムの場合は、出荷時に設定されている値のことを指します。利用者が何も設定をしないと、デフォルト値が有効になっています。
　例えば、海外のソフトなどでは、使用言語のデフォルトが「英語」に設定されていることがあり、利用者は使い始める前に「日本語」に設定を変更したりします。
　また、デフォルト値が設定されていない場合、利用者が初期設定をしないとエラーになったりします。

●クラウドとは

●クラウドサービスの提供形態



＊ＳａａＳは自社のインフラ等を使ってサービスを提供する場合もある

●デフォルト値と初期値の違い

デフォルト値 （default value）	機器やシステム、ソフトウェアに最初から組み込まれた設定値
初期値 （initial value）	機器やソフトウェア、ネットワークサービスなどの使用開始時の設定値。また、初回使用時に行う設定の値。

クラウドの設定項目

具体的に、クラウドの設定項目にはどんな項目があるのかを見てみましょう。

■クラウドの設定項目

クラウドの設定とは、クラウドを利用するための条件を決めることです。設定項目は、サービスの種類ごとに異なりますが、重要な項目は同じです。

設定項目の中で、ミスをすると情報漏洩などの事故につながるものは、ユーザのＩＤやセキュリティの設定です。ＩａａＳ＋ＰａａＳでは、「ＩＤとアクセス管理」「セキュリティ等の集中管理」、ＳａａＳでは、「ユーザの設定」「セキュリティとアクセスの設定」などと呼ばれています。

■ＩａａＳ＋ＰａａＳの設定項目例

インフラやプラットフォームを提供するＩａａＳ・ＰａａＳの設定項目には、以下のようなものがあります。（→Ⅱ.1.1、Ⅱ.1.2）

ＩＤとアクセス管理
ロギングとモニタリング
オブジェクトストレージ
インフラ管理
仮想マシン（ＶＭ、ＶＰＳ）
ネットワーク
セキュリティ等の集中管理
鍵管理
（ＰａａＳが提供する）アプリケーションの設定
データベースの設定
コンテナの設定

■ＳａａＳの設定項目例

業務アプリケーションを提供するのＳａａＳの設定項目には、以下のようなものがあります。

組織の設定
ユーザの設定
　プロファイル、権限、ロールなどの設定
セキュリティとアクセスの設定
　パスワードポリシーやログインポリシーの設定
　共有設定
オブジェクトの設定
アプリケーションの設定
プロセスの自動化の設定　など

コラム：よくある設定ミス

クラウドの設定ミスが起きているのは、日本だけではありません。クラウドを利用している多くの国で起きています。

■米国の専門機関が公表した設定ミスのトップ１０

ＮＳＡ（National Security Agency、米国家安全保障局）とＣＩＳＡ（Cybersecurity & Infrastructure Security Agency、米サイバーセキュリティ・インフラセキュリティ庁）は、2023 年 10 月に、設定ミスのトップ１０を公表しました。

Top Ten Cybersecurity Misconfigurations
（設定ミス・トップ１０）

①Default configurations of software and applications
（ソフトウェアやアプリケーションのデフォルト設定）
②Improper separation of user/administrator privilege
（ユーザ／管理者の権限の不適切な区分）
③Insufficient internal network monitoring
（不十分なネットワーク監視）
④Lack of network segmentation
（ネットワークセグメンテーションの欠如）
⑤Poor patch management
（パッチ管理の不備）
⑥Bypass of system access controls
（システムアクセス制御のバイパス）
⑦Weak or misconfigured multifactor authentication (MFA) methods
（多要素認証の脆弱性や設定ミス）
⑧Insufficient access control lists (ACLs) on network shares and services
（ネットワーク共有やサービスのアクセス制御リストの不備）

この文書は、実際の事例に基づいてまとめられたものであり、大変参考になります。以下のページを参照してください。
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-278a

第2章

設定ミス対策の前提となる考え方

2-1　責任分担の原則

■責任分担

クラウドのセキュリティの確保については、まず、サービスの提供者と利用者とが、責任を分担するという考え方が重要です。このような考え方を「責任共有モデル」と呼びます。責任共有モデルの考え方は現在多くのクラウドサービス事業者に採用されています。

また、ＳａａＳ、ＰａａＳ、ＩａａＳといったクラウドサービスの種類によって責任分担の範囲が異なります。（→Ⅱ.1.2）

■利用規約等の「免責事項」に注意

クラウドサービスにおける責任分担について、「利用規約」や「約款」などに書いてあることがあります。特に、サービスの提供者側が、責任を負えない分野について「免責条項」や「責任制限条項」が記述してあることがよくあります。（→Ⅲ.1.1.1）

これは、サービス提供者が契約どおりにサービスを提供できなかった場合の責任を免除したり、一定範囲に限定したりする条項です。例えば、損害賠償の範囲の制限などです。

この免責条項等は、提供者側が故意に違反したような「信義則に反する」場合などを除けば有効なので、クラウドサービスの契約の時に注意して読んでおく必要があります。

■ＳＩ事業者と設定ミス

日本では、クラウドを使ったシステム開発を、ＳＩ事業者（システム開発事業者）に委託することも多いので、その場合の責任分界にも注意が必要です。（→Ⅱ.1.3）

ＳＩ事業者が入ると責任分担が複雑になるので、契約等でよく確認する必要があります。また、ＳＩ事業者はＩＴのプロではありますが、プロといえどもミスをすることはあります。実際にＳＩ事業者の設定ミスによる事故も起きています。ＳＩ事業者が行った設定であっても、最終的な責任は利用者が負うことになることから、利用者もＳＩ事業者の行った設定に注意しておく必要があります。

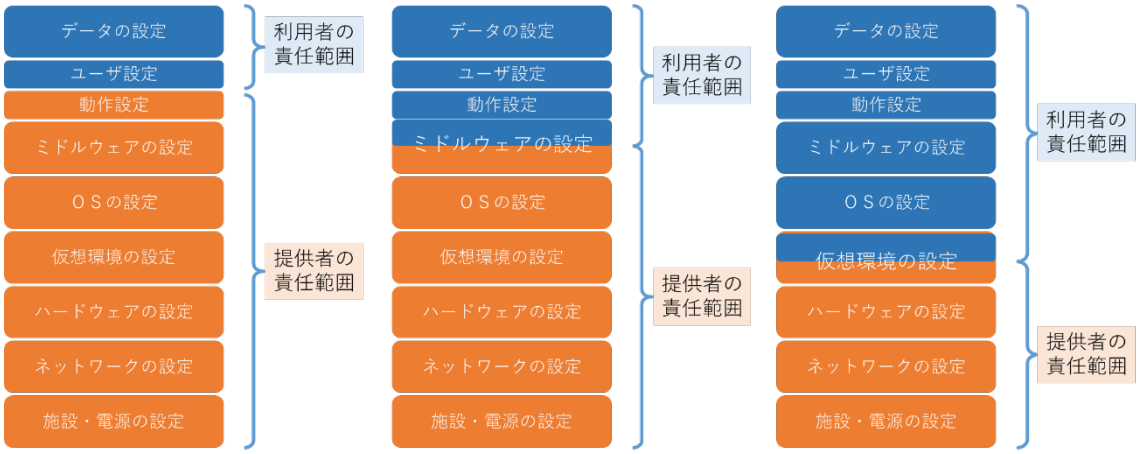
■クラウドサービス間の連携と責任分担

クラウドサービス同士が連携してサービスを提供することも増えてきています。よく使われるのがＡＰＩ（Application Programming Interface）という方式です。（→Ⅱ.1.3）

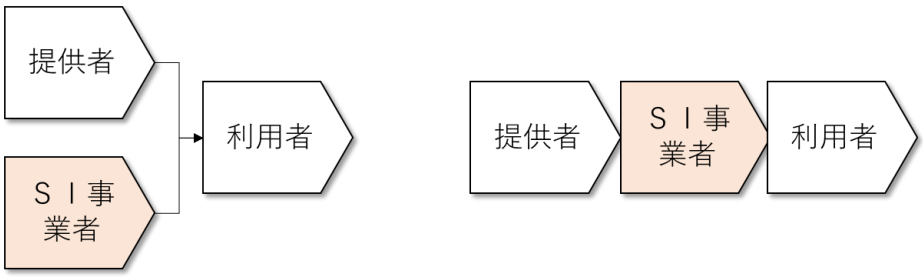
１つの仕事を複数のＳａａＳの機能を連携させてこなすために、機能を提供する側と、機能を利用する側で、情報のやり取りのルール（仕様）を決めたものがＡＰＩです。

クラウドサービス同士の連携の場合は、事業者間の契約に基づく責任分担を確認することが重要になります。

●サービスの種類ごとの責任範囲の違い



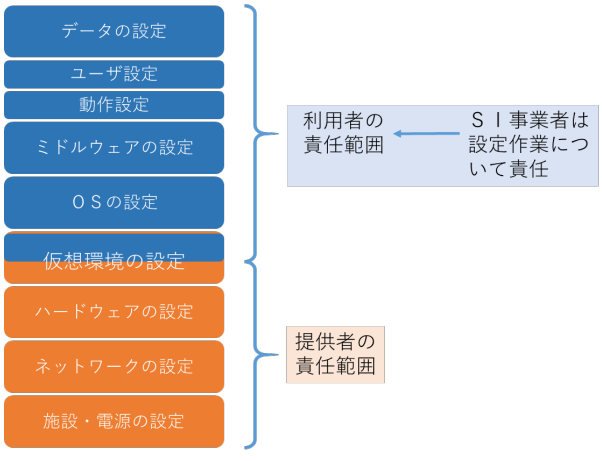
●ＳＩ事業者が関わるパターン



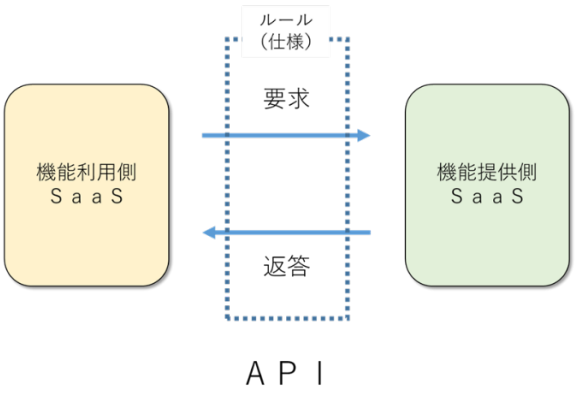
利用者が提供者と契約

ＳＩ事業者が提供者と契約

●ＳＩ事業者が入る場合



●クラウドサービス間連携



2-2　予防と発見

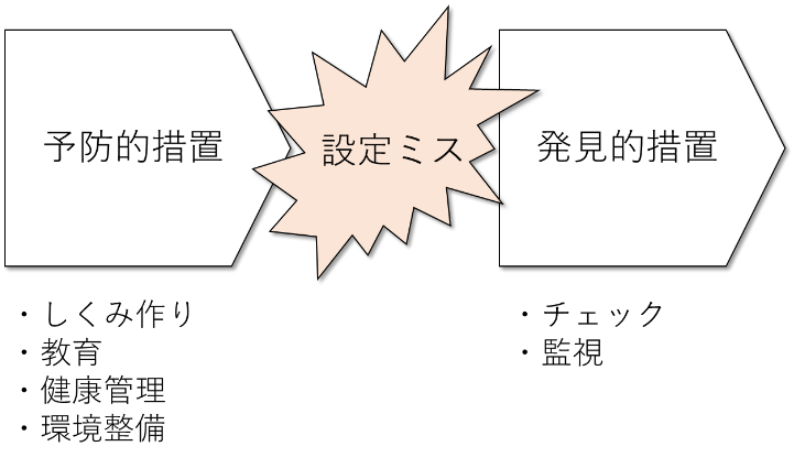
設定ミスは、できれば起きないことが望ましいですが、設定作業の大部分は人間が行っており、そうである以上、ミスは避けられないのも事実です。

■予防的措置と発見的措置

ミスが避けられないものなのであれば、ミスが起こらないようにする「予防」の対策だけでなく、起こってしまったミスを見つける「発見」の対策も必要になります。これらは「予防的措置」と「発見的措置」と呼ばれています。（→III.3.1.2）

設定ミスの場合、ミスをしてから問題が起きるまでに時間があることもあるので、その前にミスを発見して修正できれば被害が発生せずにすみます。そのため「早期発見」を可能とする対策が必要になります。

なお、「後で発見すればいいからミスをしてもかまわない」という考え方はよくありません。重大な事故を引き起こしておいて「人間はミスをするものだから」ではすまされないからです。やはり予防できるにこしたことはないのです。そういう意味では、優先すべきは「予防」ということになります。



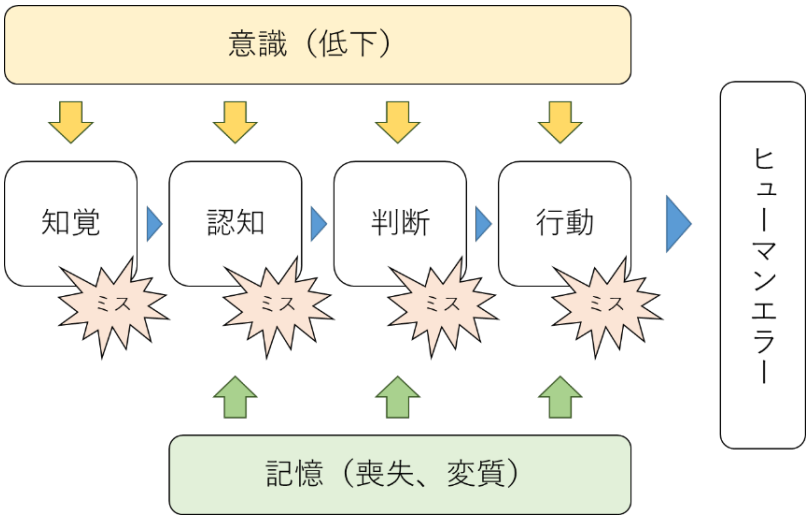
用語解説：ヒューマンエラー

人間の行動による誤りや失敗は「ヒューマンエラー」と呼ばれています。

ヒューマンエラーには、「うっかりミス」、「うっかり忘れ」、「思い違い」などがあります。なお、本ガイドブックの「ミス」には、「意図的にルールに違反する行為」は含めません。

ヒューマンエラーは、人の行動における特性（起因）と、その人を取りまく環境（誘因）によって発生します。

人間の行動は、「知覚」「認知」「判断」「行動」といった流れで行われており、そのすべてのプロセスでミスが起きる可能性があります。そして、これらに影響するのが「意識」と「記憶」です。意識が低下したり、記憶があいまいだったりするとミスが起きやすくなります。



人間を取り巻く環境は、人間のミスを引き起こす「誘因」になります。この「環境」には、心身の状態、作業環境、組織環境などがあります。

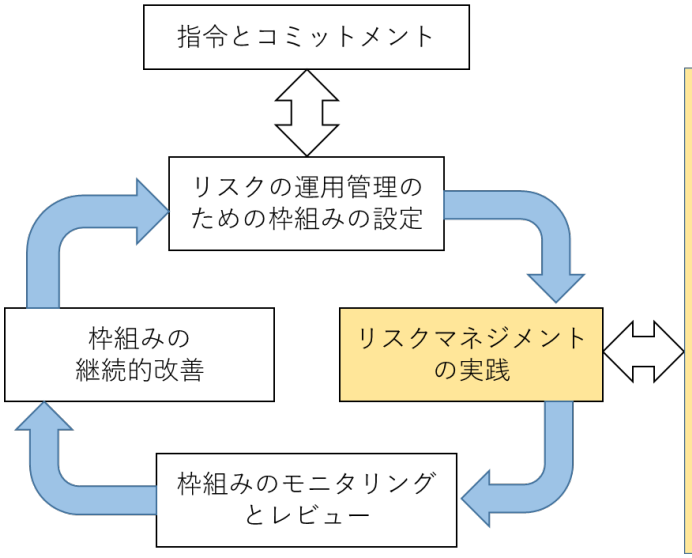
心身の状態	・身体の状態（疲労、睡眠不足、加齢による身体機能の低下など） ・精神の状態（ストレス、緊張感、悩みなど） ・意識の状態（他のことに気を取られている、ぼうっとしているなど）
作業環境	・職場の騒音、照明、振動、悪臭、温湿度など ・使用するハードウェアの状態（パソコン、キーボード、マウス、ディスプレイなど） ・使用するソフトウェアの状態（わかりやすさ、操作性など）
組織環境	・仕事の環境（ルールの複雑さ、負荷、納期の厳しさなど） ・職場の人間関係（上司や同僚との関係など） ・コミュニケーション（指示・命令の適切性、わかりやすさなど）

用語解説：リスクマネジメント

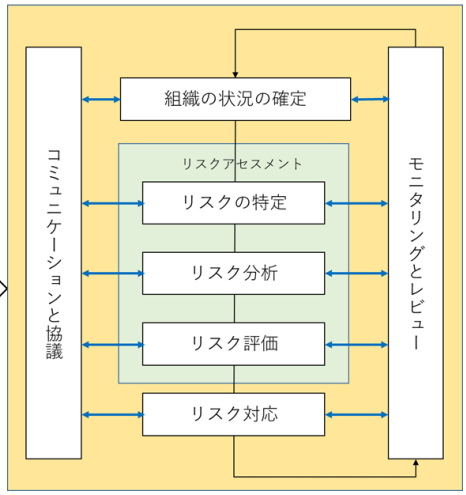
設定ミスも「リスク」であり、そのマネジメントには、一般的な「リスクマネジメント」の考え方が使えます。

■リスクマネジメントサイクル

リスクマネジメントといっても難しい話ではなく、リスクを想定して予防策を打つということです。そのためには、リスクを特定して、分析・評価し、対策を検討するというプロセスが必要になります。また、このリスクマネジメントプロセスを、ライフサイクルという大きな時間軸で見て、サイクルを回していくのが「リスクマネジメントサイクル」です。



リスクマネジメントプロセス



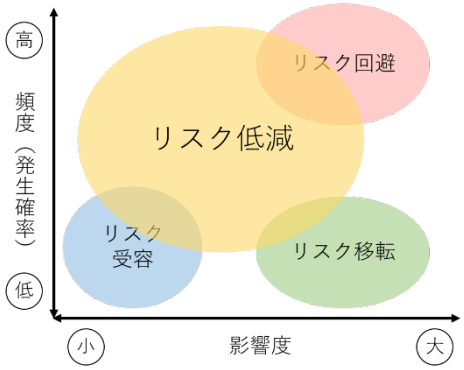
■リスク分析とリスク対策

リスクを分析するには、その発生する頻度（発生確率）と、影響の大きさ（影響度）で分析する「リスクマトリックス」が使われます。

設定ミスの場合、影響度が大きいリスクは、やはり情報漏洩につながるアクセスコントロール等のセキュリティに関わる設定になります。そういうリスクに対しては、対策を優先する必要があります。

■4種類のリスク対策

リスク対策には、「回避」、「低減」、「分散(転嫁)」、「受容」の4種類があるとされています。



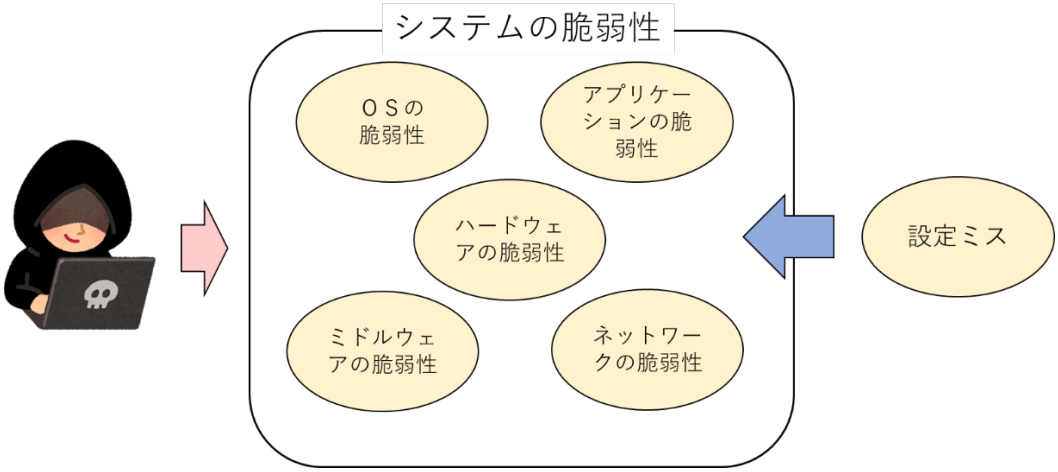
コラム：セキュリティ対策の一環

設定ミス対策は、それだけを単独で考えるのではなく、システムのセキュリティ対策の一環としてとらえる必要があります。

■システムの脆弱性

攻撃の対象にされるのは、提供される製品やサービスに「脆弱性」と呼ばれる弱い部分がある場合もあります。

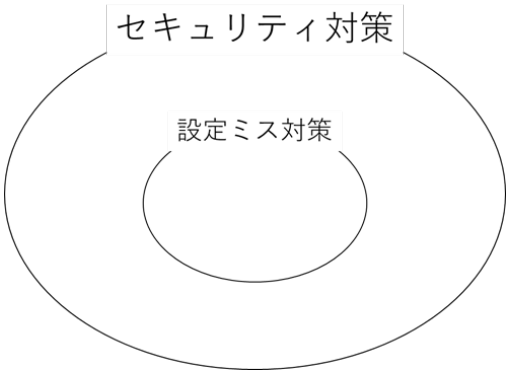
設定ミスは、利用者がシステムに脆弱な部分を作り出してしまうという見方もできます。



■設定ミス対策とセキュリティ対策

設定ミス対策は、システムの弱い部分をなくすというセキュリティ対策全体の中で、一緒に考える方が、企業全体のセキュリティレベルの向上に対して効果的です。

例えば、脆弱性診断サービスというサービスがあります。このサービスを活用して、設定ミスの診断だけではなく、システム全体の脆弱性を診断することにより、より包括的に情報漏洩を防ぐことができます。



第３章

設定ミスの対策

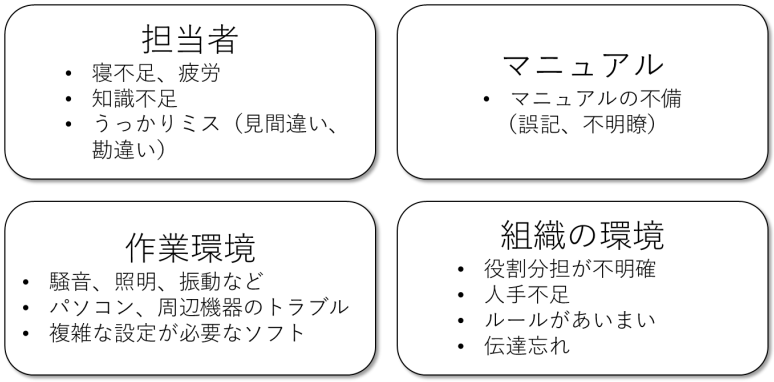
3-1　設定ミス対策の４つの観点

対策の説明に入る前に、設定ミスの原因と対策について整理しておきましょう。

■設定ミスの原因

設定ミスの原因には、前章のヒューマンエラーの箇所でとりあげたものの他にも、さまざまなものがあります。（→ II .2.1）

設定ミスの原因は①担当者、②マニュアル、③作業環境、④組織の環境の４つの観点から整理できます。

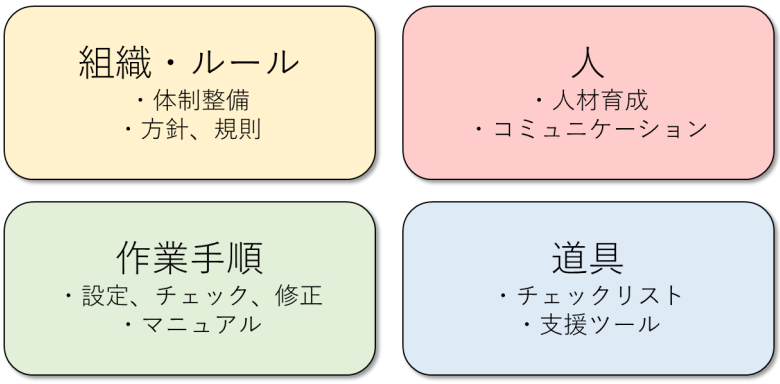


上記に挙げたものの他にも、組織や職場によって、さまざまな原因がありえます。一度、職場で原因分析を実施することをおすすめします。

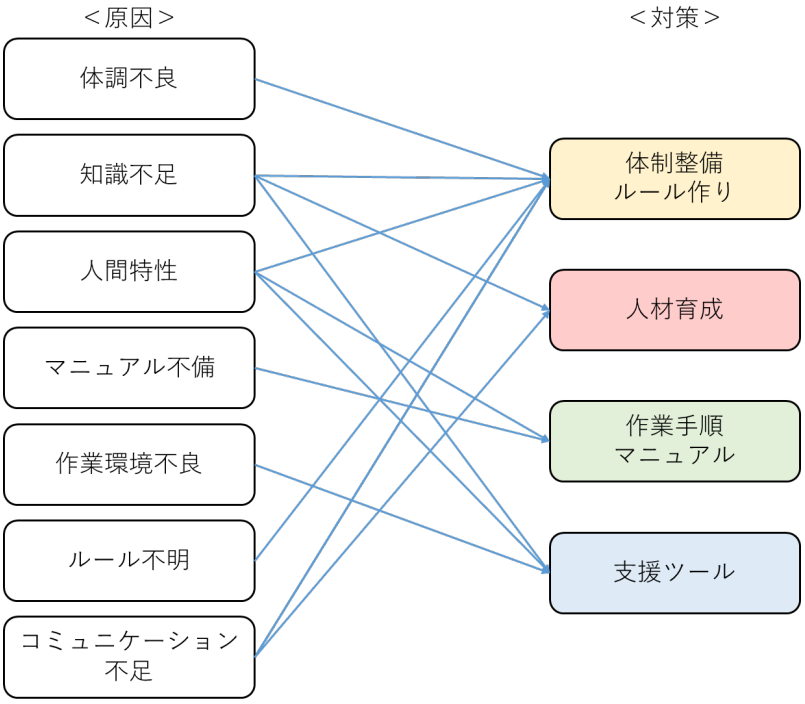
■設定ミスの対策

設定ミスにはさまざまな要因がからんでいるので、１つの対策だけでは解決しないことが多く、総合的な対策が必要になります。逆に１つの対策で、複数の原因を解決できることもあります。（→ II .2.2）

本ガイドブックでは設定ミスの対策について、設定ガイドラインに記載されている対策を、理解しやすいように主に基本的に実施すべき対策からなる①組織・ルール②人③作業手順に加え、①～③を高いセキュリティ水準で実施することが求められる場合に推奨される対策からなる④道具（ツール）の４つの観点から整理しました。



●設定ミスの原因と対策



●ガイドラインにある設定ミス対策の整理

ガイドラインの目次	ガイドブックの目次
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	組織・ルールの対策（設定ルールの策定）
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	組織・ルールの対策（設定ルールの策定）
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	ツールによる対策（支援ツールと診断サービス）
III.1.1.4 【基本】 クラウドに関する人材の組織的育成	人的対策（人材育成）
III.1.2.1 【基本】 技術情報の収集	人的対策（情報収集とコミュニケーション）
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	人的対策（人材育成）
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	人的対策（人材育成）
III.1.4.1 【基本】コミュニケーション	人的対策（情報収集とコミュニケーション）
III.2.1.1 【基本】作業規則の整備	組織・ルールの対策（設定ルールの策定）
III.2.1.2 【基本】作業手順書の整備	作業手順面の対策
III.2.1.3 【基本】ヒューマンエラー対策	作業手順面の対策
III.2.1.4 【基本】作業手順書に係るマネジメント	作業手順面の対策
III.3.1.1 【基本】設定項目の把握と設定	作業手順面の対策
III.3.1.2 【基本】設定項目の管理	作業手順面の対策
III.3.2.1 【基本】変化への適応及び体制整備	組織・ルールの対策（体制の整備）
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	組織・ルールの対策
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	人的対策（情報収集とコミュニケーション）
III.4.2.1 【推奨】支援ツールや外部診断サービス等の活用	ツールによる対策（支援ツールと診断サービス）
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	作業手順面の対策
IV.4.1.1 【推奨】設定項目管理ツールの提供	ツールによる対策（支援ツールと診断サービス）
IV.4.2.1 【推奨】設定項目診断ツールの提供	ツールによる対策（支援ツールと診断サービス）
IV.5.5.1 【推奨】暗号化機能の提供と設定	その他の対策
IV.7.1.1 【推奨】マネージドサービスの提供	その他の対策
ＩａＣの活用	コラム

3-2　組織・ルールの対策（体制の整備）

まず、組織・ルール面の対策のうち、体制の整備から見ていきましょう。

■複数の担当者を

クラウドサービスを利用するにあたっては、まず、責任者や担当者を明確にすることが重要です。中小企業においては役員が責任者になることもあるでしょう。（→III.1.1.1）

また、クラウドの設定を担当する者は複数いることが望ましいです。.1 人でクラウドの設定をするのは危険です。そもそも情報システムを担当する人が１人しかいない組織は「ひとり情シス」と呼ばれ、さまざまな課題を抱えています。

設定ミス対策としては、少なくとも設定をする人と、設定をチェックする人を置くことが必要です。担当者が設定して、責任者がチェックするという方法もあります。

【参考】専門組織（ＣＣｏＥ）を設置している企業もある

セキュリティ部門やコンプライアンス部門を設置している企業も増えています。中には、クラウドの専門組織であるＣＣｏＥ（Cloud Center of Excellence）を設置しているところもあります。

■クラウドサービス提供者との窓口の明確化

体制の整備の中で重要なのが、クラウドサービスを提供する事業者とのコミュニケーションの要となる窓口を明確にすることです。サービス提供者からの情報は、正しい設定をするのに必須です。得られた情報を社内に周知をするのも窓口の役割です。（→III.1.2.1）

■協力企業への委託

自社だけでは、人数やクラウドの専門知識が不足しているという場合に、外部の企業に協力してもらうというのも選択肢の.1 つです。クラウドサービスの運用自体をまかせることもあります。

■導入時から運用時まで

クラウド関連の業務を担当する体制は、導入時だけではなく、運用開始後も必要です。（→III.3.2.1）

クラウドサービスの内容が変更になったり、新しいクラウドサービスを導入するなど、クラウドの環境は日々変化しています。

●「ひとり情シス」の問題

問題	設定ミスの懸念
業務量をこなせない	業務量が多すぎて、設定作業が進まない。残業が続くと、疲労から設定ミスも起きやすくなる。
ミスに気がつかない	設定をチェックしてくれる人がいないため、ミスが発見されずに残ってしまう。
トラブルの対応が遅い	設定ミスによる情報漏洩が発生しても、なかなか対応できずに、さらに被害が拡大する
ノウハウが属人化する	システムのことがわかるのが.1 人なので、その人が退職すると誰もシステムの設定を変更できなくなる。

●ＣＣｏＥ（Cloud Center of Excellence）の役割

役割	説明
クラウド導入の企画	組織にとって最適なクラウドサービスを選択し、導入の計画を立案する。
クラウド活用の環境やルールの整備	クラウドサービスを利用できるように環境の構築を行う。利用のルールも策定する。
クラウドのセキュリティ対策	セキュリティポリシーに基づき、監視ツールの導入など、セキュリティ対策を実施する。
クラウドに関する情報収集と共有	クラウドの技術情報やトラブル情報などを収集し、社内に共有する。

●窓口の明確化も重要

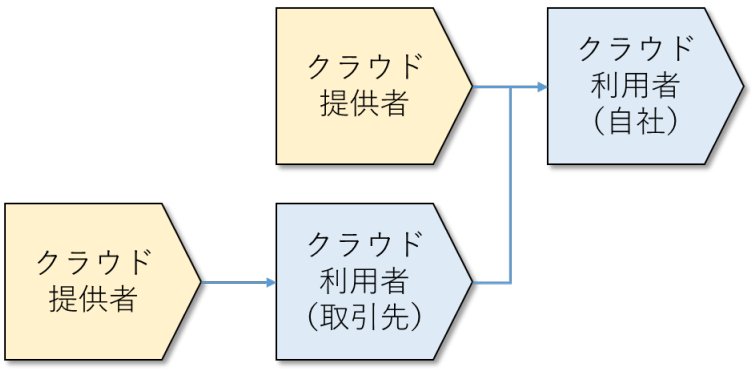
コラム：サプライチェーンリスク

■取引先の設定ミスによる情報漏洩

近年、取引先や関連企業でのクラウドの設定ミスを原因とする情報漏洩等の事故が起きています。また、クラウドサービスの運用を委託した企業での設定ミスの事故なども起きています。

■サプライチェーンを意識したセキュリティ対策を

セキュリティ対策の体制を構築する上では、サプライチェーン上の関連企業も巻き込んだ検討が必要になっています。



体制という観点からは、自社で利用しているクラウドサービスだけでなく、関連企業の利用しているクラウドサービスについても目を配る必要があります。

■ツールやセキュリティポリシーの共有

すでに、グループ企業や関連企業とセキュリティ対策や支援ツールを共有している例もあります。

具体的には、セキュリティポリシーや利用方針を子会社や関連企業と共有したり、セキュリティ対策ツールを共通化する取り組みが見られます。

コラム：「シャドーＩＴ」

■シャドーＩＴとは

企業や組織において、管理部門の許可なく使われている情報システムやサービスは、「シャドーＩＴ」と呼ばれています。隠れて使われているＩＴという意味です。

会社に隠れて、こっそりファイル共有サービスを使って、社外の人と情報交換をしているというようなケースです。

■シャドーＩＴのリスク

「シャドーＩＴ」としてクラウドサービスが使われる場合には、使う個人がセキュリティに関する設定を行っています。これは、個人の知識不足からミスをする危険があります。

実際に、個人でファイル共有サービスを利用して、設定ミスによる情報漏洩を起こしたという事例があります。

このような事例は、特にテレワークの普及により増えています。

■事業部門によるクラウドサービス利用

企業においては、事業部門の判断で、情報システム部に許可されていないクラウドサービスを導入する例もあります。これも一種のシャドーＩＴと言えます。

事業部門でクラウドサービスを導入することを許可している企業においては、その事業部門で利用のルールを定めるという対策が必要になります。（→III.1.1.2）

■シャドーＩＴの対策

シャドーＩＴを取り締まるというのは難しいですが、まずはルールを決めて周知するところからになります。

最近では、シャドーＩＴを検知するサービスなども登場しています。

3-3　組織・ルールの対策（設定ルールの策定）

クラウドの設定のルールを決めずに、個人の判断に依存している状況では、設定ミスが起きやすくなります。ルールには方針や規則などがあります。

■セキュリティポリシー

クラウドの設定に限らず、セキュリティ全般に関する方針を定めたものが「セキュリティポリシー」です。（→III.1.1.1）

セキュリティポリシーの作成は、社内に存在する情報資産を洗い出し、重要度に応じてラベル付けをすることろから始まります。そして、それぞれの情報資産の管理の方針を決めます。セキュリティポリシーは、「基本方針」、「対策基準」、「実施手順」の３つで構成されることが一般的です。

■クラウドサービス利用方針

クラウドサービスを利用する際に基本となる方針を定めたものが「クラウドサービス利用方針」です（→III.1.1.1）。利用方針はセキュリティポリシーと整合性をもって作成する必要があります。

通常は全社方針として作成されることが多いですが、事業部門ごとにクラウドサービス利用するような場合は、事業部門ごとの方針も必要になります。（→III.1.1.2）

利用方針では、責任者を明確にしたり、個人での利用を禁止したりします。特に重要なのは、①ユーザアカウントの管理、②アクセス管理、③情報公開のルールです。（→III.3.1.1）

その他、定期診断等の監査方針などについても定めます。

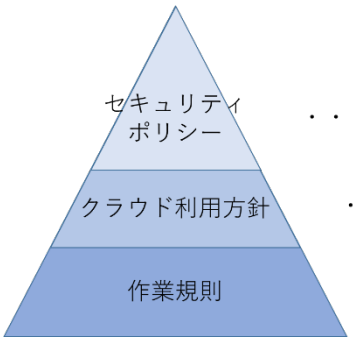
■作業規則

利用方針ができたら、次はルールの具体化です。利用方針に基づいて、クラウドの設定をするための「作業規則」を決めておくとミスが減ります。作業規則は、個人の判断に頼らず、誰でも正しく作業できるようにするためのものです。（→III.2.1.1）

■ルールの文書化

「セキュリティポリシー」や「クラウドサービス利用方針」などの方針を定めたら、それを文書化して周知することが必要です。（→III.1.1.1、III.1.1.2）

●方針と規則



・・・セキュリティ全般の方針

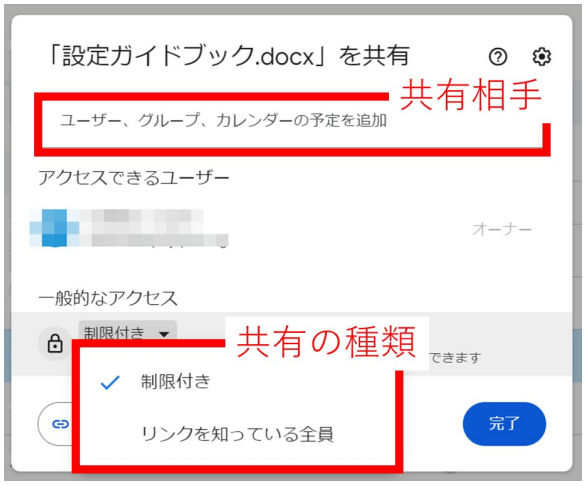
・・・クラウドを利用する際の基本方針

・・・具体的な作業のルール

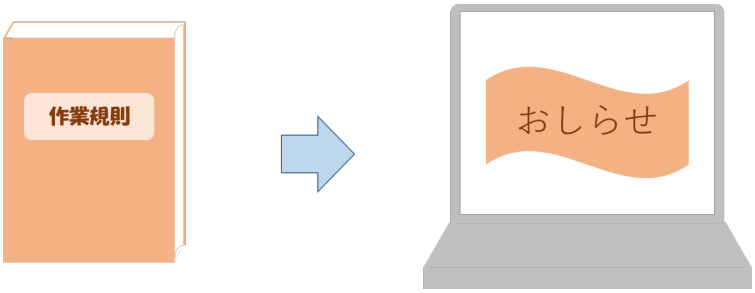
●重要な設定ルール

ユーザ アカウント の管理	アクセス管理	情報公開
・パスワードの厳格化 ・多要素認証の採用など	・データへのアクセス	・公開、非公開

●情報公開の設定の例



●文書化と周知



デフォルト値に注意

■デフォルト値とは

クラウドに限らず、システムでは、最初から「既定値」（デフォルト値）が設定されていることが多いです。利用者が特に何も設定しないと、システムではその値が使われることになります。

設定のルールを決める際に、このデフォルト値の扱いについても意識する必要があります。（→III.2.1.2）

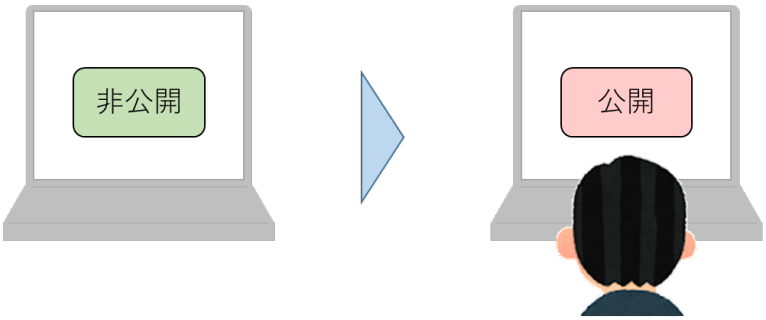
■デフォルト値が安全とは限らない

というのは、デフォルト値が安全な値でない場合があるからです。国内でもクラウドサービスを何も設定しないで使ったら、デフォルト値が有効のままで、情報が漏洩してしまったという事例があります。

■デフォルト値を変更するのにも注意が必要

また、逆にデフォルト値が安全だったのに、利用者の都合で変更したために、危険な値になるというパターンもあります。例えば、情報公開のデフォルト値は「非公開」だったのに、システムの開発期間中に、チームメンバーで情報を共有するために「公開」に変更して、運用が始まった後もそれを戻さなかったという例があります。

このようにデフォルト値を変更する場合にも注意が必要であり、明確なルールを決めておく必要があります。（→III.1.1.1）



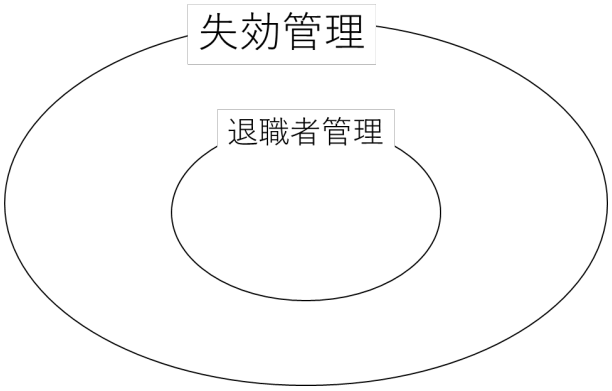
＜デフォルト値＞　　＜自分で設定した値＞

なお、海外のサービスは、日本とデフォルト値が異なることがあるので、注意が必要です。（→III.3.3.1）

コラム：退職者の管理

■失効管理の一環

クラウドの設定に関連して忘れがちなのが、退職者等の管理です。これは人事異動も含んだ「失効管理」の一環です。（→Ⅲ.1.1.1）



■退職者への対応

退職者が出たときには、その人が持っていたアカウントを削除したり、権限を他の人に引き継いだりという作業が発生します。すなわち、設定の削除や変更が必要になります。

これを忘れると、退職者が現役時代の権限を使って機密情報にアクセスすることが可能となってしまいます。

■残された人が困ること

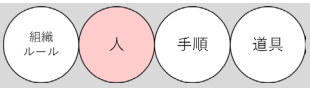
逆に、残された人が困る事態も発生します。退職者が利用していたシステムやＩＤがわからないことにより、業務が滞るかもしれません。その人がシステム管理者だった場合は、システムが使えなくなる可能性もあります。

■退職者から申請はこない　－　人事部と情報シスの連携を

都合の悪いことに、退職者が自分から設定の変更や削除を申請するということが少ないのが現状です。人事部門と情報システム部門が連携して対処する必要があります。

クラウドサービスの利用についても、退職や人事異動の際の手続きやルールについてもきちんと決めておく必要があります。

3-4　人的対策（人材育成）



クラウドの設定には一定のスキルが必要です。したがって設定ミスを防止するには、クラウドについてのスキルを習得させる人材育成も重要になります。

■サービス提供者の研修の活用

クラウドサービス提供者からセミナーや研修等が提供されていることが多いので、それらを活用しましょう。（→III.1.1.4、III.1.3.1、III.1.3.2）

集合研修だけでなく、オンラインによる研修が提供されているサービスもあります。

■クラウド研修の種類

現在、サービス提供者などからクラウドに関するさまざまな研修が提供されています。

①クラウドについての入門的な研修

クラウドの基本的な概念から学ぶ研修です。

②クラウド技術についての研修

クラウドで使われているさまざまな技術について学ぶ研修です。

③クラウドにおけるセキュリティについての研修

クラウドのセキュリティで注意すべき点やセキュリティ対策を学ぶ研修です。

④資格取得のための研修

クラウドサービスに関する資格取得のための研修です。

■社内での研修の企画

社内の多くの人がクラウドの設定にたずさわるような場合は、自社で研修を企画して実施することも有効です。（→III.1.3.1）

同じ情報を共有することにより、組織全体のリテラシーの向上が見込めます。

【参考】コンサルティングサービスの活用

クラウドサービス提供者によっては、コンサルティングサービスを提供しているところもあります。有料のサービスが多いですが、わからないことを個別に相談できるというメリットがあります。

■継続的な教育を

クラウドサービスも常に進化していますので、勉強を続ける必要があります。研修等は1回で終わらせるのでなく、継続的に実施していく必要があります。（→III.1.3.2）

●研修への参加

セミナー

オンライン研修

●クラウド研修の種類

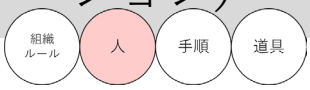
研修の種類	概要
クラウドについての入門的な研修	・クラウドの概念、種類、しくみ ・クラウドのメリット、デメリット
クラウド技術についての研修	・クラウドのアーキテクチャ ・ネットワーク、データベース　など
クラウドにおけるセキュリティについての研修	・セキュリティ事故の原因と対策 ・セキュリティ対策支援ツール　など
資格取得のための研修	・サービス提供者ごとの資格取得研修

●さまざな教育機会

社内研修

コンサルティングサービス

3-5　人的対策（情報収集とコミュニケーション）



情報の不足による設定ミスを避けるためには、意識して情報収集に取り組む必要があります。また、情報を共有するためのコミュニケーションも重要です。

■収集すべき情報

クラウドの設定に関して収集すべき情報には、①クラウドサービス提供者からの情報（→III.1.2.1）、②クラウドの技術情報（→III.1.2.1）、③設定ミスよる情報漏洩等の事例、④政府からの情報などがあります。

情報源については巻末の参考文献も参照してください。

■組織としての取組み

クラウドに関する情報収集は、個人で行うより、組織としてノウハウを蓄積して共有する方が効果的です。（→III.4.1.1）

可能であれば、専門の部署で情報収集を行い、全社に周知しましょう。（→III.1.2.1）

■コミュニケーションの充実

コミュニケーションの不足による設定ミスを起こさないため、以下のような関係者とのコミュニケーションの充実が求められます。（→III.1.4.1）

① クラウドサービス提供者とのコミュニケーション（→III.3.3.1）
② 社内のコミュニケーション（→III.3.2.1）
③ 協力企業、取引先等とのコミュニケーション

その他、同じクラウドサービスの利用者の間で、「ユーザコミュニティ」が形成されている場合は、そのコミュニティにおける情報交換も有益です。（→III.1.4.1）

クラウドサービスに関係する人が増えると、コミュニケーションは急速に複雑化します。関係者が多い場合は、特に理解しやすい情報共有が求められます。

【参考】言語の違いにも注意

海外で開発されたシステムの場合、マニュアル等が日本語に翻訳されていなかったり、翻訳の際にミスがあったりすることがあります。実際に、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もありますので、わかりにくい場合にはクラウドサービス事業者や代理店などの担当者に確認する、原文をチェックする等の注意が必要です。

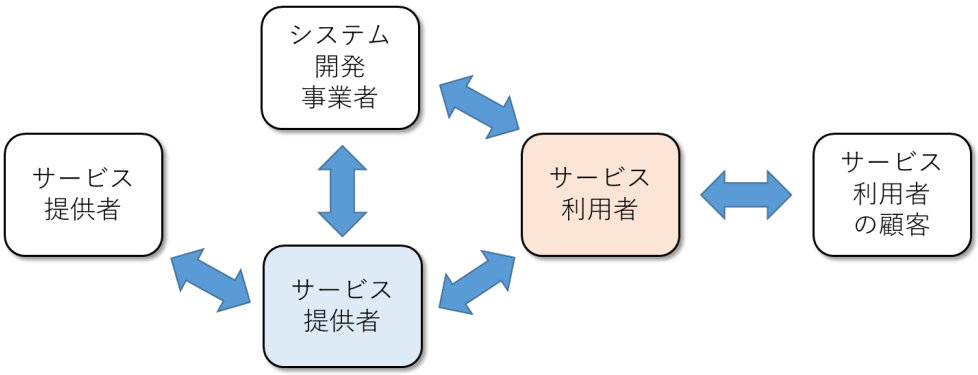
●収集すべき情報の例

情報の種類	説明
クラウドサービス提供者からの情報	利用するクラウドサービスに関する情報。特に設定の変更を伴うような情報は重要。
クラウドの技術情報	クラウドサービスのしくみを理解するための基礎的な技術情報。常に最新の情報が必要。
設定ミスによる事故の情報	設定ミスによる情報漏洩等の事故の情報。自社の事例だけでなく、他社の事例も参考となる。
政府からの情報	総務省、ＮＩＳＣ、ＩＰＡなどからの情報システムのセキュリティに関する情報。ガイドライン等や緊急周知など。

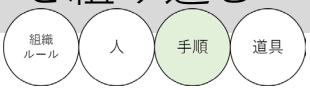
●関係者とのコミュニケーション

相手	コミュニケーションの内容
クラウドサービス提供者とのコミュニケーション	サービス内容について理解に齟齬がないようにしておく。疑問を解決するための問い合わせなどの日常のコミュニケーションも重要。
社内のコミュニケーション	複数の部門で設定を行っている場合、社内で情報を共有する。同じ設定ミスを繰り返さないように、教訓を共有する。
協力企業、取引先等とのコミュニケーション	取引先のシステムと連携していることも多いため、互いのシステムについて情報を共有する。協力企業の作業状況についても把握する。

●複雑化するコミュニケーション



3-6　作業手順面の対策　－　チェックを組み込む



次に、クラウドの設定では、どういう作業手順なら設定ミスが少なくなるかを考えましょう。

■設定項目の洗い出し　－　抜け漏れをなくす

クラウドの設定にあたっては、抜け漏れが無いように、事前に設定が必要な項目を洗い出し、どの値に設定するかを決めます。その際、利用方針や作業規則との整合性に留意します。

■作業マニュアルの整備

作業手順を決めたら、作業マニュアル（手順書）を作成します（→III.2.1.2）。参考になるのは、クラウドサービス提供者が提供しているマニュアルです。

なお、ＣＩＳ（Center of Internet Security）という米国の団体が各サービスの推奨設定を記した「ＣＩＳベンチマーク」という文書も参考になります。

■マニュアルもレビューする

マニュアルの設定値の記述に間違いがあると、設定ミスに直結します。マニュアルを作成したらレビューが必要です。また、クラウドの環境の変化に対応するため、作業マニュアルも定期的な見直しが必要になります。（→III.2.1.4）

■慎重で確実な設定を　－　マニュアルは必ず見る

設定ミスは、設定時に起きるので慎重かつ確実に行いましょう。人は慣れてくるとマニュアルを見ずに作業するようになりますが、記憶に頼って作業をするというのはミスのもとです。作業環境や心身の状態にも留意する必要があります。

■チェックが重要　－　可能なら事前チェックも

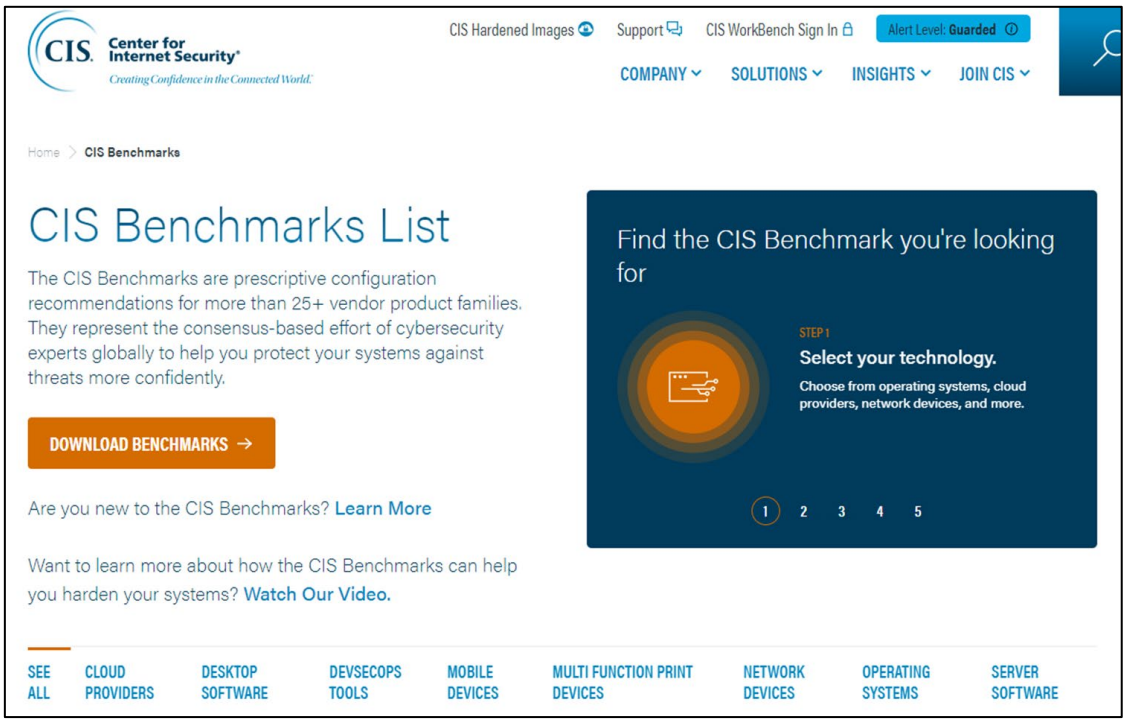
人間のミスを０にすること困難なので、設定をチェックすることが重要です。それも複数の目で行うことが望ましいです（→III.2.1.3）。担当者によるセルフチェックだけでなく、別の人もチェックする「ダブルチェック」が理想的です。

通常は設定後にチェックしますが、可能であれば事後だけでなく事前にもチェックするのが効果的です。設定すると、すぐにシステムに反映されて、チェック前に問題が起きることもあるからです。例えば、設定項目を記入したシートを事前にレビューします。

■定期的・継続的なチェックを

クラウドの環境は常に変化しているので、一度設定したら終わりではありません。環境の変化に対応するためには、定期的・継続的なチェックも必要です。（→III.3.2.1、III.4.3.1）

●ＣＩＳベンチマークが参考になる



https://www.cisecurity.org/cis-benchmarks

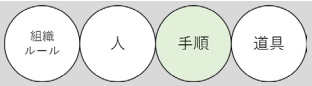
●作業マニュアルを必ず見る

慣れてきた
時が危ない

●できれば事前チェックを

設定項目の洗い出し → 事前チェック → 設定 → 事後チェック → 管理・運用

作業プロセスの自動化



■人間の作業を減らす

人間による設定作業の場合、ミスの発生は避けられないものです。そこで、設定作業を自動化してミスの発生を減らそうという考え方があります。

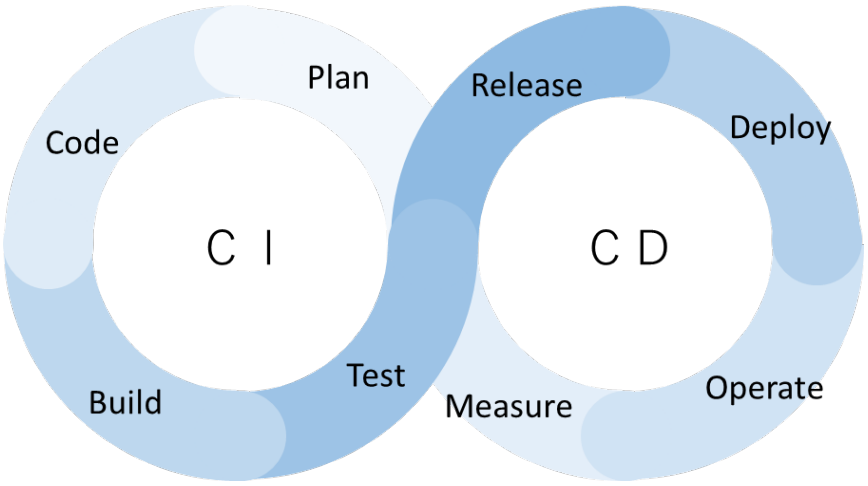
■ＣＩとＣＤ

アプリケーションの開発においては、ＣＩ（Continuous Integration）やＣＤ（Continuous Delivery）と呼ばれる自動化技術が普及しつつあります。（→III.2.1.3）

ＣＩやＣＤを組み合わせて使うと、開発したアプリケーションを変更する際に、自動でテストからリリースまで行うことができます。

ＣＩは、コード（プログラム）を変更するたびに共有の環境に統合して管理するしくみです。そこではプログラムを実行可能な形式に変換するビルド（コンパイル）やプログラムのテストが自動で行われます。

ＣＤでは、ＣＤの成功後、セキュリティや性能を含めた総合的なテストが行われ、本番環境へのデプロイ（配備と設定）や利用者への提供が自動的に行われます。



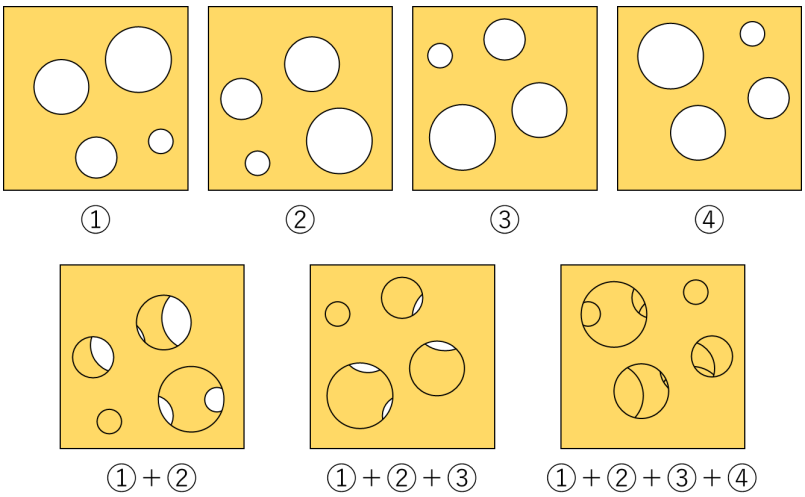
ＣＩとＣＤの組み合わせ

将来的にはこうした自動化技術の普及により、人間による作業が減り、設定ミスも減ることが期待されます。

コラム：多段階チェック

■複数のチェックの組み合わせ

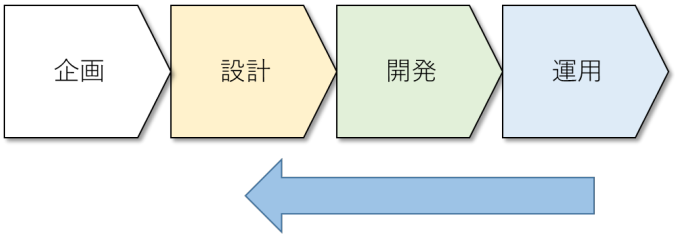
複数のチェックの組み合わせは、よくチーズの絵で説明されていて、「スイスチーズモデル」と呼ばれています。1 枚のチーズだけでは（ミスが）穴をすりぬけてしまいますが、2 枚、3 枚と重ねていくと、穴がなくなりなります。



なお、チェックを複数にした結果、1 つ 1 つのチェックがおろそかになっては意味がありません。人によるチェックだけでなく、機械によるチェックを組み合わせるのも手です。

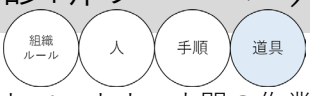
■「シフトレフト」　－　ＩａａＳ・ＰａａＳの場合

複数チェックの例として、システム開発における「シフトレフト」という考え方があります。システム開発では、各工程で設定ミスのチェックを行うことが有効であり、それも早い工程でのチェックが効果的です。チェックの重点を工程図の左の方にもっていくという意味で「シフトレフト」と呼ばれています。



ＩａａＳ・ＰａａＳを利用してシステムの開発を行う場合には、この考え方が使えます。

3-7　ツールによる対策（支援ツールと診断サービス）



クラウドの設定作業を支援してくれるツールやサービスも提供されています。人間の作業にミスはつきものなので、機械でチェックするツールを導入することは、検討の価値があります。

■設定支援ツールの活用

設定支援ツールは人間が見落としたミスを機械が発見してくれることも多く、作業の効率化や負担軽減にも役立ちます。

■２種類の支援ツール

クラウドの設定を支援するツールには、２つの種類があります。（→III.4.2.1）

①設定管理ツール

現在のクラウドの構成を可視化してくれるツールです。構成管理ツールとも呼ばれます。

②設定診断ツール

設定に問題がないかを診断してくれるツールです。

設定支援ツールは、単独のツールではなく、セキュリティツールの一部であることも多いです。例えば、脆弱性診断、ログ監視、ファイアウォールといったさまざまなセキュリティツールに、設定ミスをチェックする機能が含まれていることがあります。

■設定支援ツールの提供者

設定支援ツールは、クラウドサービスを提供する事業者だけでなく、サードベンダー（第三者）も提供しています。

■ガードレール機能

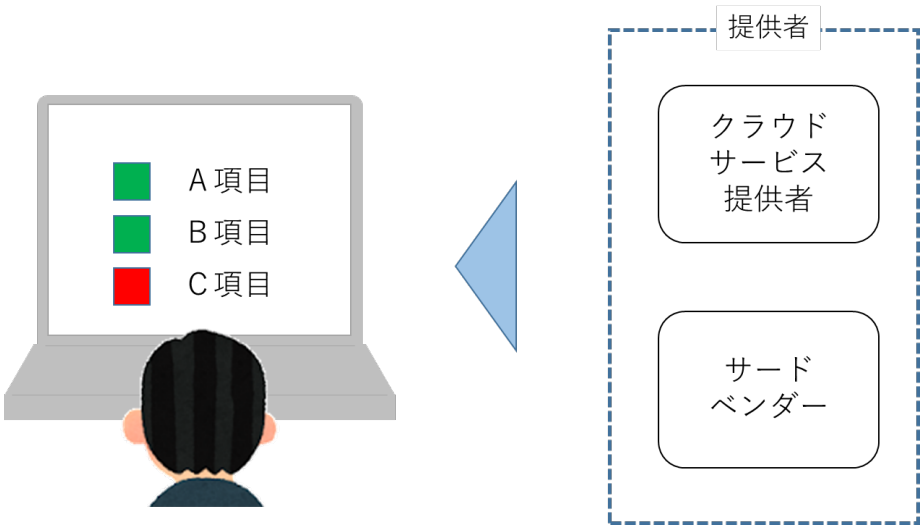
クラウドサービス（ＩａａＳ・ＰａａＳ）の中には、設定値が正常な範囲からはみ出さないようにする「ガードレール機能」を持ったものもあります。設定値が範囲からはみ出すと、範囲内に戻してくれる「自動修復機能」を持ったサービスもあります。

■診断サービスの活用

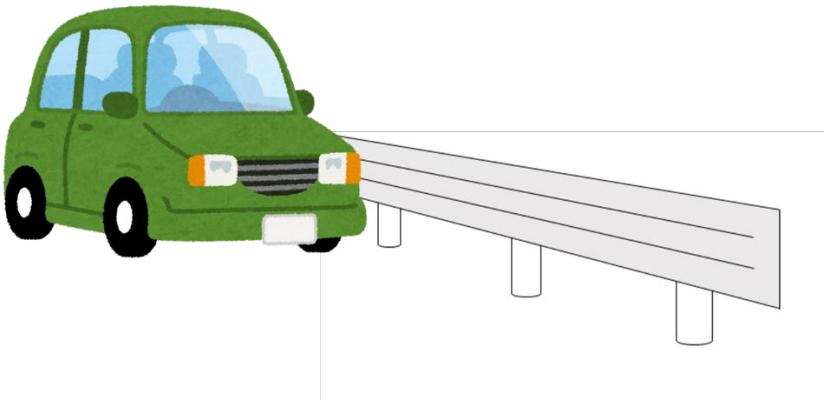
ツールを使ってクラウドの設定に問題がないかを診断してくれるサービスも提供されています（→III.4.2.1）。このサービスを利用することで、自社で行う設定のチェックをアウトソーシングすることができます。

設定の診断サービスも、単独で提供されるより、システムの診断サービスの一部として提供されることが多いです。

●設定診断ツールのイメージ

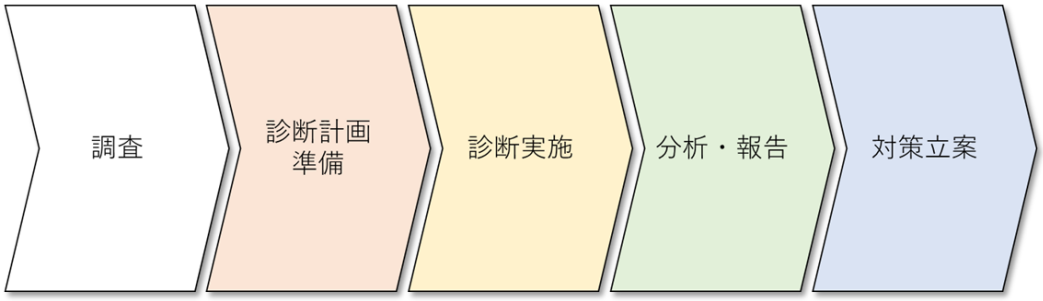


●ガードレール機能



設定値がルールを逸脱しないようにする機能をもったサービスもある

●診断サービスの活用



診断サービス活用のプロセス

3-8　ツールによる対策（CASB、CSPM、SSPM）

■３種類の支援ツール

クラウドの設定ミスを減らすのに有効なツールには、以下の３つものがあります。（→Ⅲ.4.2.1）

①ＣＡＳＢ（Cloud Access Security Broker）
②ＣＳＰＭ（Cloud Security Posture Management）
③ＳＳＰＭ（SaaS Security Posture Management）

■ＣＡＳＢ

ＣＡＳＢ（キャスビーと読みます）は、クラウドサービスの利用状況を可視化して、定期的にチェックしてくれるツールです。アプリケーションやデータへのアクセスを監視したり、セキュリティポリシーに照らして、リスクを検出する機能もあります。

■ＣＳＰＭ

ＣＳＰＭは、クラウドサービスのうち、ＩａａＳ（インフラを提供するサービス）の監査ツールです。クラウドの設定を自動的にチェックし、設定ミスやコンプライアンス違反等のリスクを特定してくれます。また、より安全な利用方法を提示してくれます。

Amazon Web Services (AWS)、Microsoft Azure、Google Cloud などのサービスが対象です。

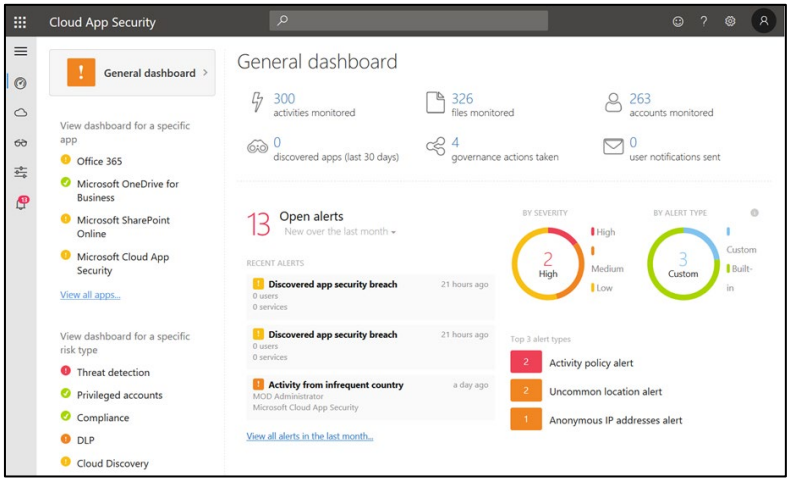
ＣＳＰＭが監査する設定項目は、ＮＩＳＴ（National Institute of Standards and Technology、米国国立標準技術研究所）やＣＩＳ（Center for Internet Security）などの米国の組織が提供する標準的なセキュリティのフレームワークに準拠しているのが特徴です。

■ＳＳＰＭ

ＳＳＰＭは、クラウドサービスのうち、ＳａａＳ（アプリケーションを提供するサービス）の監査ツールです。各アプリケーションの設定やコンプライアンス状況を管理して、脅威を検出することができます。

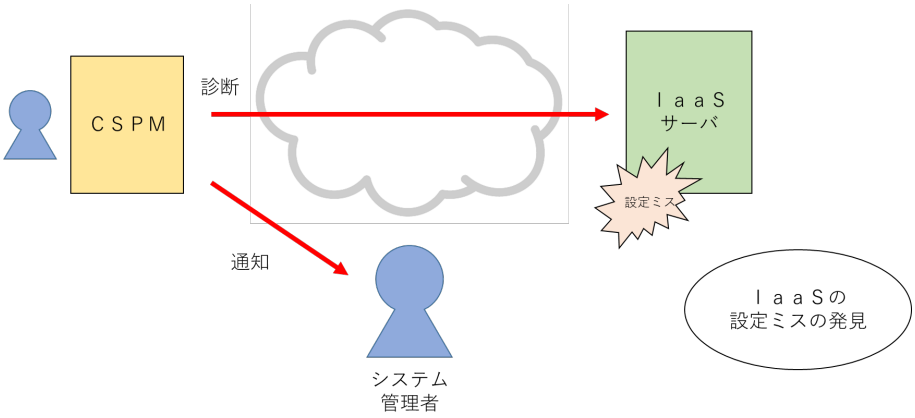
現在、ＳＳＰＭは、グローバルなＳａａＳ（Microsoft 365 や BOX、Salesforce など）には対応していますが、日本のＳａａＳには対応していないこともあります。

●ＣＡＳＢ

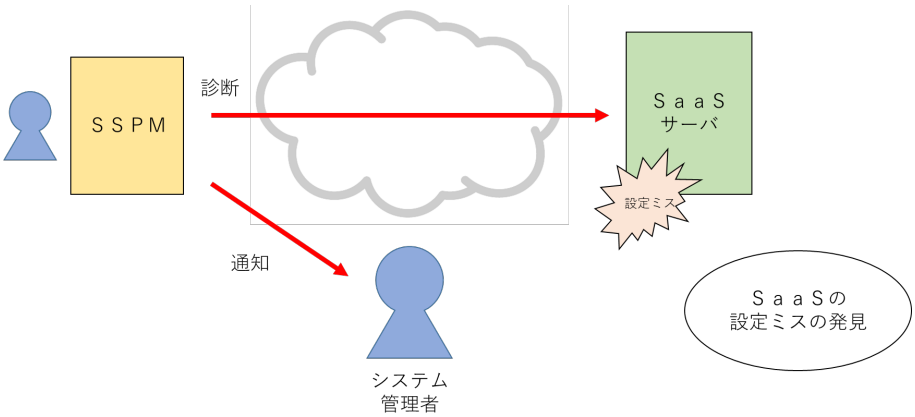


https://chrisonsecurity.net/20.19/08/.14/microsoft-cloud-app-security-5-reasons-to-start-using-it/

●ＣＳＰＭ



●ＳＳＰＭ



3-9　その他の対策

設定ミスに関連する対策としては、設定ミスにより情報漏洩が起きてしまったときの対策や、設定そのものをなくす対策などもあります。

■暗号化

暗号化は設定ミスを減らす対策ではなく、設定ミスによる情報漏洩が起きたときのための対策です。情報が盗まれても暗号化してあれば、そのままでは読むことができません。

もっとも、攻撃者側の技術も向上しているため、暗号化してあれば絶対に安全ということはありません。最近では、将来の技術向上により解読できるようになることを期待して、暗号化されているデータを盗む攻撃者もいます。

それでも、解読されるまでの時間稼ぎになり、犯人を捕まえられる可能性もあるので、暗号化は有効な対策です。特に重要な情報に対しては、暗号化する必要があります。(→Ⅲ.3.3.1)

なお、アクセス経路が乗っ取られた場合など、データベースにあるデータの暗号化だけでは足りない場合もあります。

■データのバックアップ

データのバックアップも設定ミスの防止策ではありません。ファイル共有の設定ミスにより、ファイルが破壊（削除、改ざん等）されたときに備える対策です。

データのバックアップがないと、ファイルを復元することが困難になります。

なお、データのバックアップは、設定ミスによるファイル破壊の対策だけでなく、ランサムウェア攻撃によるデータの暗号化の対策にもなります。

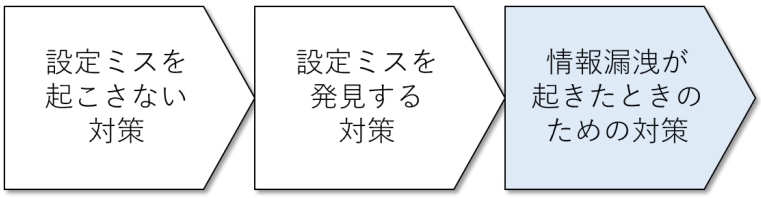
■マネージドサービス

設定ミスのリスクを軽減する対策だけでなく、設定ミスのリスクを移転する対策もあります。「マネージドサービス」の活用がその例です（→Ⅲ.4.1.1）。マネージドサービスは、主にＩａａＳ・ＰａａＳの運用をまかせるサービスです。

このサービスを活用すると、クラウドの設定は、利用者でなくマネージドサービスの提供者が行うことになります。これにより、設定ミスのリスクが移転されることになります。もっとも、設定ミスのリスクは移転できても、クラウドサービスを利用する責任や委託元としての責任は残ることには注意が必要です。

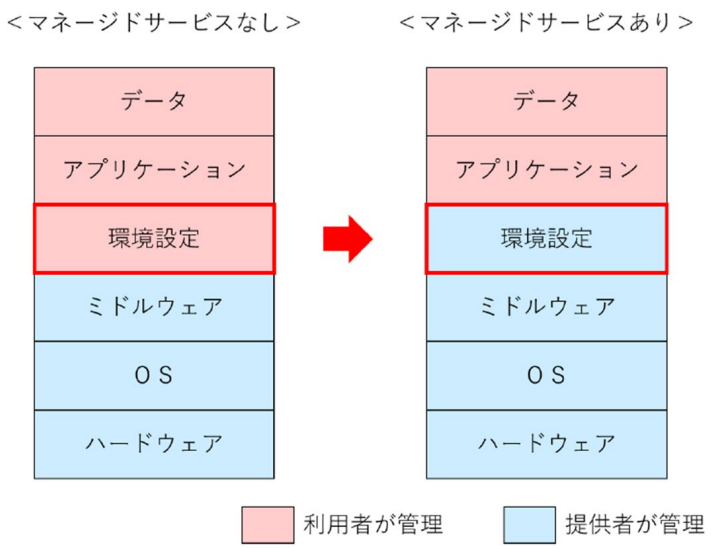
マネージドサービスは、クラウドサービスを提供する事業者だけでなく、サードベンダー（第三者）によって提供されることもあります。この場合のマネージドサービスは、クラウドサービスの運用のアウトソーシングという見方もできます。

●暗号化の意義



●バックアップの意義

●マネージドサービスによるリスクの移転



●アウトソーシング型マネージドサービスのメニューの例

導入段階	運用段階
企画支援	運用
導入支援	セキュリティ管理

コラム：新しい課題

クラウドの技術も進歩していて、設定に関しても新しい課題が生まれています。

■マルチクラウド

複数のＩａａＳを使う「マルチクラウド」という方式も増えつつあります。

マルチクラウドの環境では、システムが複雑化し、セキュリティ対策も難しくなります。これにより、設定漏れや設定ミスなどのリスクが高まります。

マルチクラウドの場合、それぞれのサービス仕様を正確に把握して、セキュリティの設定を適切に行うのは困難です。

対策としては、マルチクラウドを一元的に管理するＣＳＰＭ（支援ツール）や、マルチクラウドを対象とした支援サービスが登場していますので、検討するといいでしょう。

■コンテナ

「コンテナ」という技術も普及してきています。コンテナとは、アプリケーションの実行に必要なものをまとめたものです。最初からクラウド環境でシステムを構築する際には、コンテナがよく使われます。

コンテナの設定ミスを狙った攻撃も確認されています。ＮＩＳＴ（米国国立標準技術研究所）は、「コンテナセキュリティガイド」を公開しており、ＩＰＡ（情報処理推進機構）から日本語訳も出ています。また、コンテナセキュリティ対策用のツールも登場しています。

■生成ＡＩクラウドサービス

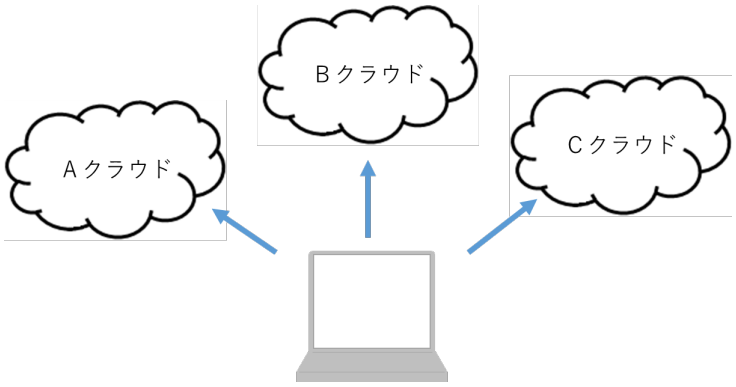
今、ＳａａＳ（アプリケーションのサービス）の分野で、一番の話題は生成ＡＩを始めとするＡＩ（人工知能）を使ったクラウドサービスでしょう。

生成ＡＩのサービスにおいても気をつけるべき設定項目があります。チャットボットなどのサービスでは、何も設定しないと、利用者が入力した情報が、ＡＩの機械学習に使われることがあります。デフォルト（既定値）が「学習あり」になっているのです。入力情報には、文章だけでなく、画像や音声も含まれます。

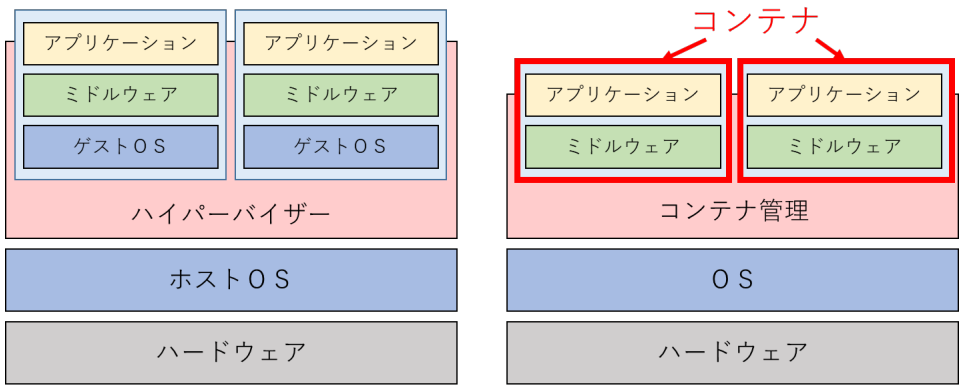
ＡＩが学習した入力情報が他の利用者の出力結果にまぎれこむことによる情報漏洩が懸念されています。

生成ＡＩサービスを利用する場合は、デフォルトの値を確認し、問題がある場合は、入力情報がＡＩの学習に利用されないように設定する必要があります。

●マルチクラウド　－　複数のクラウドの利用

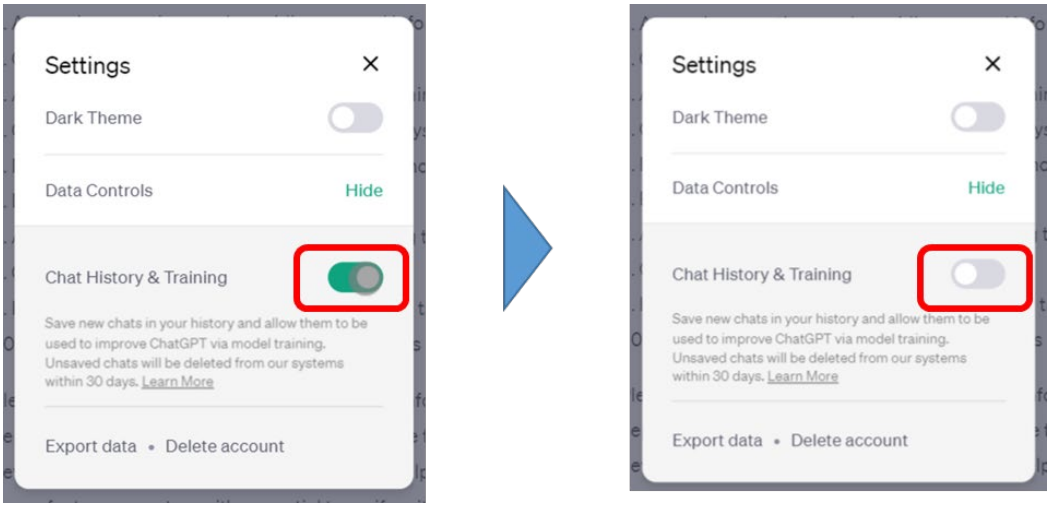


●コンテナ



一般的な仮想化　　コンテナによる仮想化

●生成ＡＩの設定変更の例



コラム：設定のコード化

■設定の見える化　－　事前チェックを可能とする技術

近年、クラウドの設定をプログラムのコードとして記述する技術が開発されています。これを使うと、クラウドの設定を可視化（見える化）することができます。設定が可視化されるということは、事前のチェックが可能になり、コンピュータでチェックすることもできるようになるというメリットがあります。チェック用のプログラムもすでに存在しています。

また、高品質のコードを再利用して、複数のクラウドの品質を向上させることもできます。

■ＩａＣ（Infrastructure as Code）

ＩａＣはＩａａＳの設定をコード化する技術です。

```
"UserData" : {
    "Fn::Base64" : {
        "Fn::Join" : [ ",", [
            { "Ref" : "MyValue" },
            { "Ref" : "MyName" },
            "Hello World" ] ]
    }
}
```

ＪＳＯＮによる記述

```
UserData:
  Fn::Base64: !Sub |
     Ref: MyValue
     Ref: MyName
     Hello World
```

ＹＡＭＬによる記述

https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/quickref-general.html

図のようにＩａｃはプログラミング言語で記述されています。ＩａＣを使いこなすためには、少し勉強が必要かもしれませんが、挑戦してみてください。

■ＰａＣ（Policy as Code）

最近では、ＰａＣという技術も開発されてきています。ＰａＣは、ソフトウェア開発やシステムの管理において、セキュリティポリシーや運用ルールなどをコード形式で定義して管理するものです。具体的には、クラウド環境やシステムに対するアクセス制御、リソースの利用ルール、セキュリティ要件などをコードで定義します。

参考資料

■チェックリスト

■参考文献

■チェックリスト

□リスク分析を行いましたか（2）

組織・ルール

□責任者・担当者は明確になりましたか（3-2）
□（複数の）人を配置しましたか／チェックする人はいますか（3-2）
□方針とルールを策定しましたか（3-3）

（設定ガイドライン上の基本対策）

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
クラウドサービス利用において、ガバナンスの確保やルール形成、人材育成への取組などの組織的方針を明確にする。

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
クラウドシステムの仕様変更や機能追加等により、デフォルトの設定値が変更されるなどの変化に準備し対応する。

Ⅲ．３．３　その他のリスクへの対応
課金管理や日本国以外の法律が適用されるリスクなど様々なリスク対応について明確にし、対応方針を文書化する。

人

□人材育成の計画をたてましたか（3-4）
□情報収集や関係者とのコミュニケーションを行っていますか（3-5）

（設定ガイドライン上の基本対策）

Ⅲ．１．２　技術情報の収集
各種設定値の変更等の技術情報を日頃から収集し、リスク分析対策立案のサイクルを組織的に確立する。

Ⅲ．１．３　人材育成
クラウドサービスの設定におけるリテラシーの向上や動作環境設定における技術力の向上を確実にする。

Ⅲ．１．４　コミュニケーション
組織として利害関係者との窓口の明確化、定期的な情報交換を行うと共に、コミュニケーションのルートと方法を確立する。

Ⅲ．４．１　ノウハウの蓄積
設定方法について組織のノウハウとして蓄積するため、マニュアル化、ツール導入などを行う。

作業手順

□作業規則や作業マニュアルを作成しましたか（3-6）

（設定ガイドライン上の基本対策）

Ⅲ．２．１　作業規則やマニュアルの整備

クラウドシステムの設定について作業規則及び作業手順を整備し、定期的に見直す。併せてヒューマンエラー対策を組み込む。

Ⅲ．３．１　クラウドセキュリティに係る設定項目の確認

自社で利用するクラウドサービスの設定項目を理解し、予防的措置と発見的措置を実施できる体制を構築する。

ツール

□支援ツールの導入を検討しましたか（3-7, 3-8）

（設定ガイドライン上の推奨対策）

Ⅲ．４．２　支援ツール等の活用

複雑化する設定項目の管理について設定不備の検出ツールや監視ツールなどの支援ツールを活用する。

Ⅲ．４．３　定期的な設定値のチェックと対応

設定項目について定期的なチェックを行うとともに、内部監査や外部診断などを行う。

※括弧内の数字は本ガイドブックの章・節の番号を、対策項目の見出しの数字は各類型に対応する設定ガイドライン上の対策の項番を示すものです。

※詳細なチェックリストについては、設定ガイドラインの「ANNEX 対策一覧」を活用してください。

■参考文献

①クラウドのベストプラクティス（→III.1.2.1）
NIST SP-800 シリーズ
CIS Controls
CIS Benchmarks

②出版物
松本照吾 他「ＡＷＳではじめるクラウドセキュリティ」、2023 年
一川誠「ヒューマンエラーの心理学 」、20.19 年、筑摩書房（ちくま新書）
吉原靖彦「図解よくわかるこれからのヒューマンエラー対策」、2023 年、 同文館出版
森田浩平「基礎から学ぶコンテナセキュリティ」、2023 年、技術評論社

③オンラインドキュメント
ＮＩＳＣ（内閣サイバーセキュリティセンター）「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）」
https://www.nisc.go.jp/policy/group/infra/cloud_guidance.html
総務省「テレワークセキュリティガイドライン第５版」と設定解説資料
https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/
経済産業省「クラウドセキュリティガイドライン活用ガイドブック」
https://www.meti.go.jp/policy/netsecurity/downloadfiles/cloudseckatsuyou20.13fy.pdf
ＩＰＡ「中小企業のためのクラウドサービス安全利用の手引き」
https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000072.150.pdf
東京都産業労働局「中小企業向けサイバーセキュリティ対策の極意」
https://www.cybersecurity.metro.tokyo.lg.jp/security/guidebook/369/index.html
"NSA and CISA Red and Blue Teams Share Top Ten Cybersecurity Misconfigurations"
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-278a
ENISA(European Union Agency for Cybersecurity), "Cybersecurity guide for SMEs"
https://www.enisa.europa.eu/publications/cybersecurity-guide-for-smes
NCSC(National Cyber Security Centre), .10 Steps to Cyber Security
https://www.ncsc.gov.uk/files/NCSC%2010%20Steps%20To%20Cyber%20Security%20NCSC.pdf