安定したクラウドサービスの実現に向けて

～ISO/IEC 20000 の活用～

JIPDEC

2022 年 8 月 10 日

一般財団法人日本情報経済社会推進協会

目 次

はじめに

デジタル化の急速な進展に伴い、私たちの社会は大きく変化しようとしています。デジタル社会の実現に向けては、社会を構成する企業がデジタル技術を駆使して価値を創造し続けるデジタル企業へと変革していくことに加え、これまでの業種・業界ごとの縦割りの構造から、機能ごとの横割りの構造へと産業構造を変革していく必要性が「Society5.0 の実現に向けたデジタル市場基盤整備会議」において示されました。

デジタル社会においては、価値創出の源泉がフィジカル（現実）空間からサイバー空間へと移行します。その空間の中で様々な企業や組織が連携し、社会課題の解決や新たな価値、体験の提供が迅速になされ、安心・安全な社会が実現でき、またデジタルを活用してグローバルで活躍する競争力の高い企業や、カーボンニュートラルをはじめとした世界の持続的発展に貢献する産業が生まれる社会となることが期待されています。

一方、2020 年初頭からの新型コロナウイルスの世界的な拡大により、企業は短期間での顧客の行動変化や「新しい生活様式」への対応を迫られることになりました。その対応の過程では、押印を前提とする商慣習、客先常駐のビジネスモデル、テレワークのインフラやセキュリティ対策の不備等、企業の事業構造変革を阻む様々な問題が一度に表出しました。

今回のコロナ禍によって企業が直面した「新しい環境にあわせて自社のビジネスを迅速に変革していかなければ生き残ることができない」という問題は、2018 年に経済産業省が公表した DX レポートで「2025 年の崖」と表現した事業環境の激変そのものでもありました。DX レポートにおいては、2025 年までにレガシー刷新に計画的に取り組むことの必要性とデジタル技術を前提とした企業経営の変革の方向性を指摘していますが、コロナ禍を踏まえ企業におけるデジタル化の遅れへの対策は待ったなしの状況となっており、2025 年を待つ猶予はなくなったといえます。

DX とデジタル社会の実現に向けた変革を加速すべく、政府は、2018 年 6 月に「政府情報システムにおけるクラウドサービスの利用に係る基本方針」と題し、「クラウド・バイ・デフォルト原則」の優位性を説明するとともに、システム構築時には、様々なメリットを得られるクラウド利用を優先すべきことを推奨してきました。

一方で、クラウドサービスの急速な普及とともに、昨今ではクラウドサービスの停止によって社会公共インフラに多大な影響を与えるような障害も生じており、クラウドサービスを利用する上での懸念事項となっています。

そこで、本書では、この「サービスの停止」、つまりクラウドサービスの提供と利用にかかる「可用性」に関する課題に焦点をあてた具体的な障害事例に対して、IT サービスの国際規格である ISO/IEC 20000 を用いてそのようなトラブルを防止する方法を紹介することを目的に本書を発行いたしました。ISO/IEC 20000-1:2018※を参考に、どのようにサービスの可用性を高め、事業継続性を維持するのか等について解説していきます。

ISO/IEC 20000 は、IT サービスの品質向上のための仕組みを定めた国際規格であり、サービスのセキュリティ、可用性はもとより、安定した運用の強化に役立つ様々な手法が記載されており、クラウドサービスの効果的かつ安全な運用に役立つものです。クラウドサービスと ISO/IEC 20000 の関連を理解いただくとともに、ISO/IEC 20000 を活用して安全で安定したクラウドサービスの構築、運用の参考になることを期待しています。

ISO/IEC 20000 については、「ITSMS ユーザーズガイド―JIS Q 20000 対応（ISO/IEC 20000 対応）―」で解説していますので、併せてご利用ください。

※ ISO/IEC 20000-1:2018 は、その内容を変更することなく日本語化された国内規格である JIS Q 20000-1:2020 が発行されており、本書では JIS Q 20000-1:2020 を引用しています。

1 IaaS に見るクラウドサービスの可用性と障害事例

本章では、インターネット環境で IT インフラストラクチャを提供するクラウドサービスである IaaS（Infrastructure as a Service）の可用性と、その提供と利用における課題について事例を通して考察します。

1.1 クラウドサービス（IaaS）の可用性

オンライン会議ツール、Web メール、SNS 等々、様々なサービスがクラウドサービスとして提供されることが当たり前の時代において、クラウドの向こう側がどのような仕組みになっているのかは、利用者にとってさほど重要なことではないでしょう。

どのような仕組みであれ、利用したいクラウドサービスが、水道や電気のようなインフラ供給と同様に、使いたい時に使えれば良いのです。

一方、クラウドサービスを提供する側にとって、クラウドサービス提供の仕組みを構築することは、ビジネス上での重要な関心事です。クラウドサービスといえども、その仕組みの根源をたどっていけば、オンプレミスのシステムと同様に、物理的なハードウェアとその上に構築されたシステム、すなわち IT インフラストラクチャが存在しています。

近年のクラウドサービスはますます重要度を増しています。銀行、自治体、通信キャリア等々の公的機関で利用されている多くのクラウドサービスが、社会における重要な基盤を支えていることも珍しくありません。企業のオンプレミスによる基幹システムでは、多くの場合、サービスを停止させないというようなミッションクリティカルシステムが要求されます。

クラウドサービスでミッションクリティカルシステムと同等の要件を求められている場合、クラウドサービス提供者は、クラウドサービスが利用できなくなるという要因を事前に検討し、原因となり得るものを取り除いておく必要があります。

特に、“使いたい時に使える”ようにしておくための対策、つまりサービス可用性に対する各種の対策は、クラウドサービス提供側にとって、重要な関心事の一つです。

1.2 可用性の障害事例

本項では、クラウドサービスとしての IaaS（Infrastructure as a Service）における可用性に関する課題について、架空の障害事例（P 社）を通して説明します（「図 付-1 P 社提供のクラウドサービス（IaaS）」を参照）※。

P 社の提供しているクラウドサービス（IaaS）は、可用性、信頼性、セキュリティに配慮した、ミッションクリティカルな顧客向けのソリューションであることを謳っています。可用性に関しては、次のような対策を実施しています。

・IT インフラストラクチャのコンポーネント（物理サーバー、ネットワーク機器 等）の冗長化

・物理サーバー上での死活監視に加えて、ゲスト OS やアプリケーションの監視サービス

・ゲスト OS に異常が発生した際に、他の物理サーバー上にゲスト OS を移転する機能

P 社の顧客である C 社は、生産管理システムを国内の各工場で、オンプレミス環境で運用していました。システム運用に関わる費用の削減と各工場の業務効率改善を目的に、P 社が提供するクラウドサービス（IaaS）に全面的に移行し、各工場のオンプレミスで利用していたハードウェアを撤廃し、クラウド環境下での生産管理システムを稼働させました。その際、P 社のクラウドサービスが上記の対策を行っていることから、生産管理システムを稼働する上で十分と判断

しました。

※本事例の技術的な背景は「付録　1 章における架空の障害事例（P 社）の技術的背景」をご参照ください。

クラウドサービス（IaaS）の障害事例

ある日、クラウドサービスを利用しているＣ社の工場の 1 つから、「自工場の生産管理システムへアクセスができない」と、報告がありました。P 社のインフラ監視チームが調査したところ、クラウドサービス（IaaS）で使用しているディスクへアクセスができていないことが判明しました。

調査を進めるうちに、他の工場でも、クラウド上にある、その工場の生産管理システムへのアクセスが極端に遅くなっているとの報告があがっていることが判明しました。障害状況は時間を追うにつれて深刻になり、最初の報告から数時間後には、全工場からアクセスができなくなり、クラウドサービス（IaaS）が完全にダウンしました。

長時間にわたる調査の結果、原因が判明しました。原因は、冗長化されたディスクの制御部の障害でした。

クラウドサービス（IaaS）の障害の副作用として、顧客であるＣ社では、データ修復が完了するまでの時間、業務が止まってしまいました。また、一部の工場でデータベースの整合性が取れなくなり、サービスの復旧後にバックアップからのリストア作業を余儀なくされました。さらに、リストア作業に想定をはるかに上回る時間を要し、完全復旧が大幅に遅れてしまいました。

クラウドサービス（IaaS）の提供における可用性管理

P 社の提供するクラウドサービス（IaaS）のように、ハードウェアに関しては、全てのコンポーネント（サーバー、ネットワーク、ハードディスク等）で冗長化を採用し、サービスのダウンを防ぐために可用性を高めている場合でも、予期せぬ障害は発生します。十分な対策を講じて、可用性を高めていながら、障害が発生してしまった事例は、近年においても少なくありません。この事例からもわかるように、IT インフラストラクチャのコンポーネントの冗長化を進めておけば万全ということではありません。クラウドサービス（IaaS）の運用管理が必要であることを示唆しており、予期せぬ障害に対する対応を可能とする仕組みを、事前に検討し準備しておく必要があります。そのための活動については、3 章で解説していますのでご参照ください。

コラム：クラウドサービスの利用における留意点～提供者と利用者の責任範囲～

クラウドサービス（IaaS）においては、図 1-1 に示すように、クラウドサービス提供側は、サーバー、ネットワーク、ハードディスクなどの物理基盤と仮想化環境を管理します。一方、クラウドサービス利用側は OS を含めた全てのソフトウェア（ミドルウェア、アプリケーション）を管理します。提供されるクラウドサービスの形態（SaaS、PaaS、IaaS 等）によって違いはありますが、クラウドサービス提供には責任範囲があります。こういった責任範囲を「責任分界点」と呼ぶこともあります。

1 章の事例でいうと、クラウドサービス（IaaS）を提供する P 社は、ハードウェア、仮想化の管理をします。顧客である C 社はクラウドサービス（IaaS）を利用する側ですが、クラウド上で動作する全てのソフトウェアに対する管理を実施しなければなりません。例えば、バックアップデータにアクセスできるようにシステムを正常に戻す作業は P 社の責任範囲ですが、バックアップの取得とリストアは一般には C 社の責任範囲となりますので、日次でバックアップが取られていない工場もあった場合には C 社の責任になります。これらの事項は、通常、サービスレベル合意書（SLA：Service Level Agreement）で定めておく必要があります。

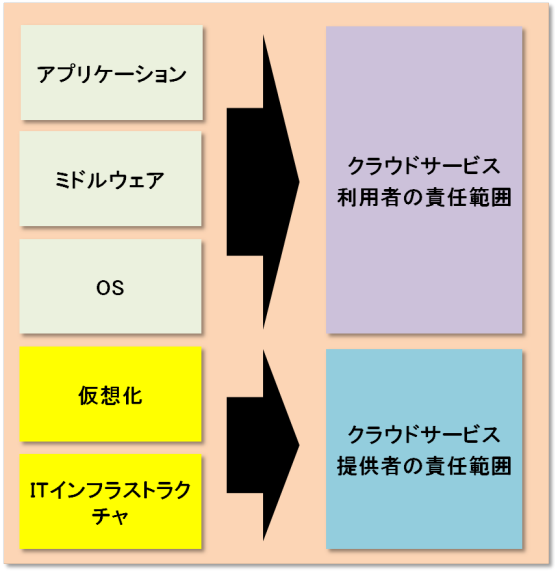


図 1-1 クラウドサービス（IaaS）の責任分界点

2 トラブルを防止するための ISO/IEC 20000 の適用

1 章では、クラウドサービスの可用性と、その提供と利用における課題について事例を通して紹介しました。この章ではそうした課題の解決に役立つ、サービスマネジメントの国際規格である ISO/IEC 20000-1:2018 を紹介します。

2.1 ISO/IEC 20000 とは

現在、多くの企業が、競争力維持・強化のために、デジタルトランスフォーメーション（DX：Digital Transformation）の実現に向けて様々な課題に直面しています。それらの課題としては、次が挙げられます。

（1）DX によりビジネスをどう変えるかといった経営戦略の決定

（2）「2025 年の崖」と呼ばれる、既存システムの老朽化・複雑化・ブラックボックス化

また、これらの課題を克服しようと、新しいデジタル技術やクラウドサービスを運用又は活用し、効率的かつ高可用性の維持のために IT 投資にリソースを振り向けるように取り組んでいます。その矢先に、1.2 に示したような昨今のクラウドサービスにおけるミッションクリティカルシステムの可用性に関する障害の事例は、相当なインパクトを各企業に与えたと考えられます。

サービスマネジメントシステム（SMS：Service Management System）の導入

特に、DX を目指す企業にとっては、顧客からのサービスの要求事項に対してサービスを通じて価値を提供する仕組みである SMS を、経営戦略の方向性に沿って迅速に導入し、DX 活動の推進のためのエンジンとして機能させることが重要です。

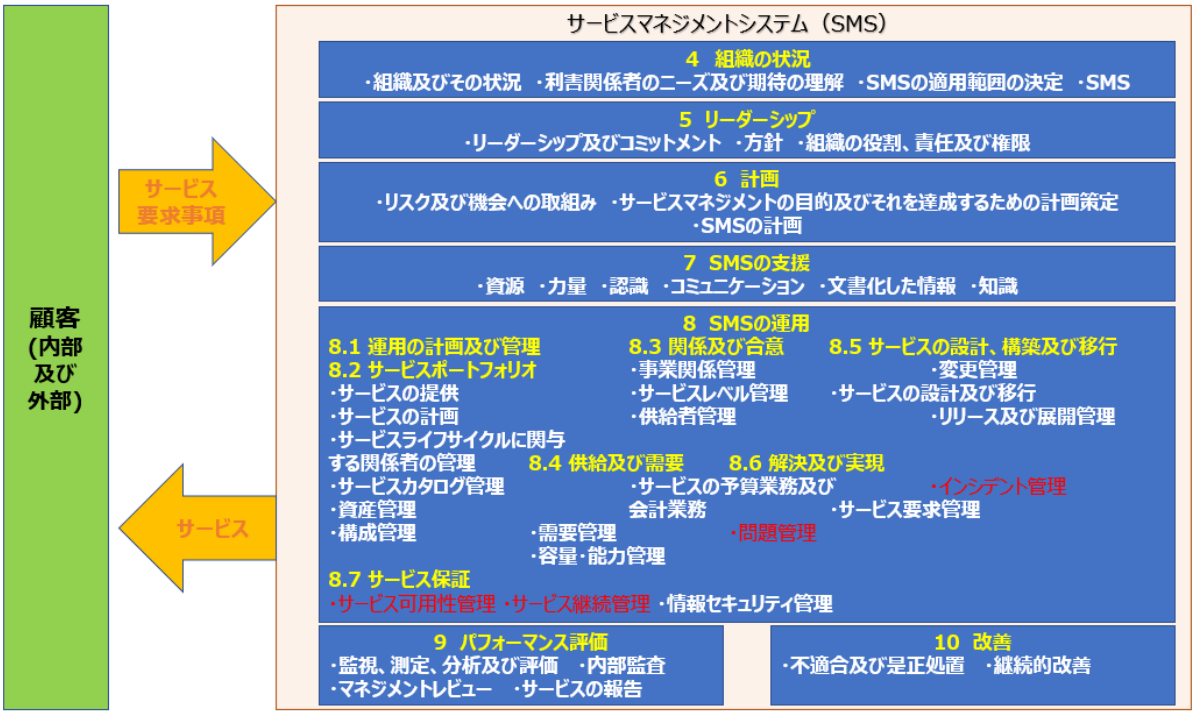
ISO/IEC 20000-1:2018（サービスマネジメントシステム要求事項）は、SMS の導入に役立つ国際規格として、広くグローバルに認知されており、サービス可用性管理を含む、サービス品質の運用・向上に必要な事項が記載されています。そのため、国際的に展開する多くのクラウドサービス事業者にとって、包括的にこれらの課題を解決するのに役立ちます（ISO/IEC 20000 の詳細は、「ITSMS ユーザーズガイド―JIS Q 20000 対応（ISO/IEC 20000 対応）―」をご参照ください）。

また、2020 年 11 月より経済産業省が設けた DX 認定制度（「コラム：DX 認定制度」参照）において、認定を受けるのに必要である次の申請項目を満たすために、この規格を参照することが役立ちます。

（1）企業経営の方向性及び情報処理技術の活用の方向性の決定

（2）企業経営及び情報処理技術の活用の具体的な方策（戦略）の決定、等

ISO/IEC 20000-1:2018 の要求事項は、以下のような構成になっています。本章では、特に SMS 全体の概要及びメリットについて解説します。図 2-1 の赤字で示している項目は、本書の「3 サービス可用性管理、サービス継続管理の重要性」、「4 サービス可用性、サービス継続を支える活動 ～インシデント管理、問題管理～」で説明していますのでご参照ください。

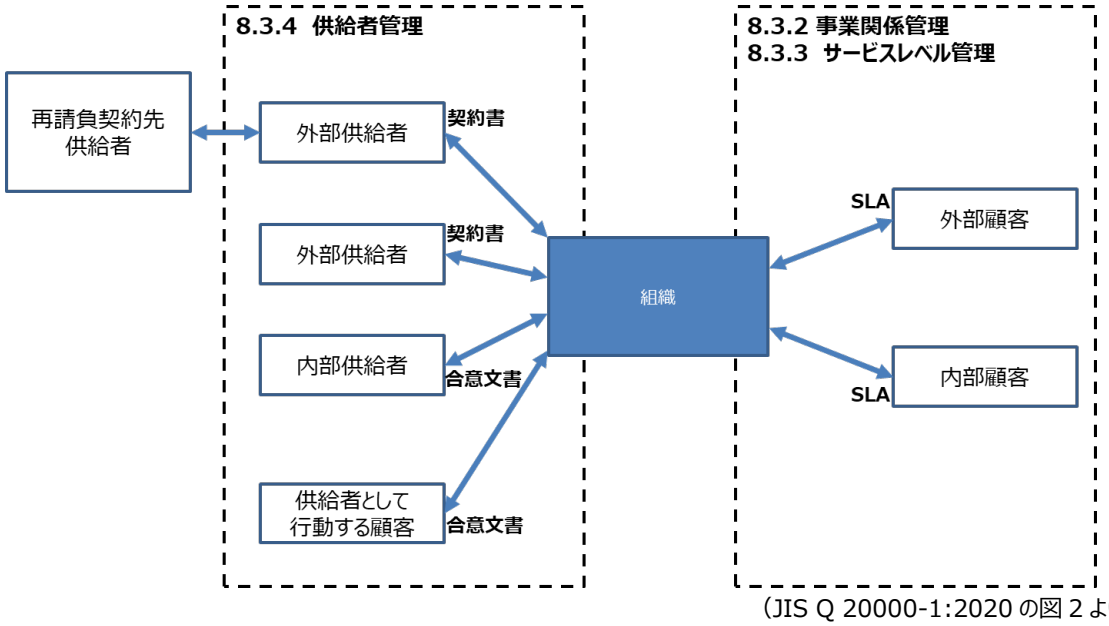


（JIS Q 20000-1:2020 の図 1 より引用）

図 2-1 ISO/IEC 20000-1:2018 の構成

この規格は、SMS 全体にかかる「計画、SMS の運用、パフォーマンス評価、改善」といった（PDCA）と称されるマネジメントシステムの導入について必要な個々のプロセスについて要求するものです。

組織は、自組織で定めた SMS の適用範囲（4 組織の状況）で、提供するサービスに対する顧客や利用者からの要求を明らかにし、要求事項を満たすために不可欠な戦略的及び戦術的パートナ、内部の供給者等を決定します。決定後、これらの関係者間で、ストラテジー（戦略）を共有し、お互いの役割や責任を、契約書や合意文書といった形で締結又は明文化し、顧客に対しては SLA として展開します。



（JIS Q 20000-1:2020 の図 2 より引用）

図 2-2 SMS 適用範囲内のサービスのライフサイクルに関与する関係者間の関係及び合意

特に、SaaS 型のクラウドサービスを提供する事業者（CSP：Cloud Service Provider）にとっては、CSP としての顧客・利用者への SLA に準じたサービスを展開する責任と、1 章の事例で触れた IaaS 型のクラウドサービスを活用する顧客・利用者（CSC：Cloud Service Customer）としての責任も果たす必要があります。さらに、SaaS 型のサービスを提供する際、他事業者が提供するサービス（例：Web メールやリモート会議システム等）を組み入れたサービスを展開する場合もあるでしょう。SaaS 型のサービスを提供する CSP は、このように一連のサプライチェーンの中で、CSC に対して価値のあるサービスを展開する必要があるため、CSP と CSC との間の「共同責任（shared responsibility）」を果たすことが重要です。そのため、CSP は、展開するサービスに対して、関係者を明らかにし、どのような合意を得る又は、得ようとしているのかを SMS の適用範囲として、明確に示すことが必要です。

このことは、1 章の事例のような障害が発生した場合、図 2-3 のような問題及び責任のなすりあい等を予防し、速やかに問題を解決することにもつながります。また、上述した DX 認定制度への申請にも役立つことになります。

（ITSMS ハンドブック運用管理のお手本 ISO/IEC 20000～事例から学ぼう～「総集編」の 8-6-1 より引用）

図 2-3　複雑なプロセスを含むサービス提供においては、障害の原因やそもそも顧客を特定することさえ困難

さらに、「共同責任」を果たすという考え方は、CSP 及び CSC にとっては、サイバーセキュリティを含む情報セキュリティの分野でも取り入れられており、次のような要求事項に対応する際に重要な役割を果たします。

- ISMS（Information Security Management system）認証
- ISMS クラウドセキュリティ認証
- ISMAP[1]（Information system Security Management and Assessment Program：政府情報システムのためのセキュリティ評価制度）
- DX 認定制度の申請項目「(6)サイバーセキュリティに関する対策の的確な策定及び実施」

SMS 導入のメリット

SMS 導入の最初のメリットとして、ISO/IEC 20000-1:2018 の「8.3 関係及び合意」が挙げられます。このプロセスは、SLA を確立し、顧客や利用者との良好な関係を保つことで、重大な変更のインパクトの議論や SLA に対する修正への合意を得やすくすることや、変更の間の中断やデメリットについても受け入れやすくなるといった利点もあります。

多くの場合、新規開発、変更時には、第三者である供給者（外部供給者）が関わりますので、確立されたビジネ

[1] 参考 URL：ISMAP https://www.ismap.go.jp/csm

ス関係を有しておくことは、必要な変更に合意することをより容易なものにします。

SMS 導入の２つめのメリットとして、ISO/IEC 20000-1:2018 の「7 SMS の支援」を紹介します。

ここでは、SMS のトップマネジメントがパートナや従業者等に対して、「サービスの要求事項を満たし、サービスマネジメントの目的を達成するために、SMS の確立、実施、維持及び継続的改善、並びにサービスの運用に必要な人、技術、情報及び財務に関する資源を決定し、提供」することを要求しています。

特に、新規のサービスをリリースする、又は従来のサービスを継続的に改善するための変更やシステムを更改する際には、常に組織に対してリスクをもたらします。なかでも、ISO/IEC 20000 では、以下の事項が考慮されています。

- ビジネスモデルの変更／改革（トランスフォーメーション）による「メリット/利点」を得るための、変更に十分な時間とリソースを割り当てるストラテジー（戦略）
- サービス事業者と顧客/利用者は、新規又は変更後の新しいビジネスモデルに沿った「やり方」の学習
- またそこに行きつく間、従業員や担当者のモチベーションや顧客・利用者にとってのメリットの実感/可視化

図 2-4 は、SMS のトップマネジメントが期初にサービスの新規開発や更改後に予測されるメリットを従業者や顧客に十分に理解させ開発する場合、期初の従業者や顧客のモチベーションは極めて高い状態にあることを示しています。一方、メリットを可視化する過程においては、好ましくない課題や問題に遭遇し、期待されたメリットの可視化に対して時間がかかりすぎると、モチベーションは急速に減少する傾向があることを示しています。この際、低下するモチベーションの中で、個々の課題を解決し、メリットをプラスに可視化する期間をトップマネジメントにとっての責任期間と呼びます。

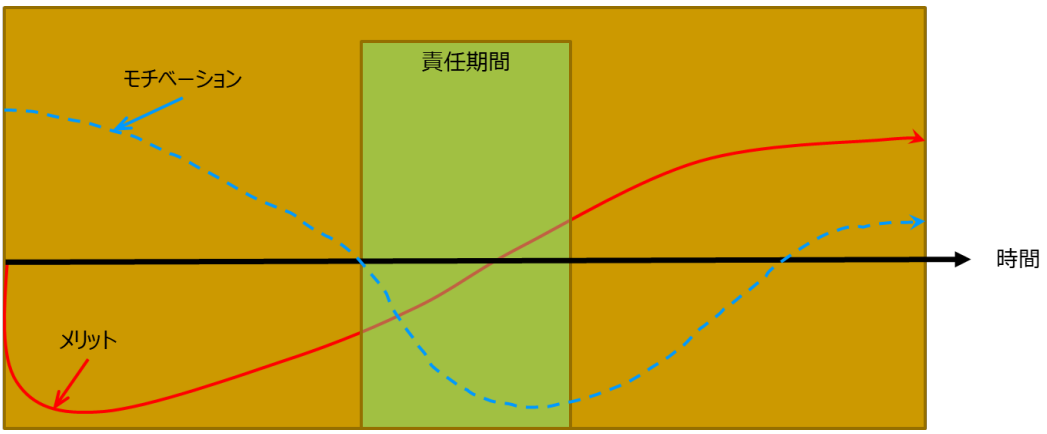


図 2-4　従業者のモチベーションと顧客が感じるメリットとの傾向性

これらの傾向性は、期待されたメリットが、その新規開発や変更に費やしたコストを上回るまで、モチベーションが減少するといわれ、特に新たなサービスを立ち上げる場合、損益分岐点と呼ばれる利益が固定費と変動費を上回る分岐点に至るには複数年かかるといわれており、短時間では目標は達成できず、その間のモチベーションは一層減少していく傾向にあることが知られています。

ISO/IEC 20000-1:2018 の「7 SMS の支援」では、SMS を導入するにあたり戦略を策定する際、トップマネジメントの役割として、SMS 導入期間中のあらゆる問題や起こり得る課題を理解し、優先順位等を調整しながら、担当者やパートナ及びメリットを期待する顧客のモチベーションを維持し、減衰期を乗り越え、うまく運用できるようリソースに関してコミットし、それぞれの要員を励ますことが重要です。しかしながら、うまくいかせるための「特効薬」はなく、必ず遭遇するであろう「問題」に対して、最良の「処方箋」を確認しながら修正していく必要があります。

これらの「処方箋」について、JIPDEC は、数種類のガイドを発行しています [2]。例えば、個々の問題を解決しながら、その壁を乗り越える際に、何かのプロセスを自動化する等、効率化を図るための工夫を施し、期待される可視化されたメリットが得られるまで、減少傾向にあるモチベーションを再び強化し、期初の目標を達成するために必要な要員、技術、情報及び財務に関する資源を決定し、提供し続けること等が挙げられます。

その一方で、SMS において、最悪な状況を作り出してしまう状況とは、「責任期間」中に大きな課題（2025 年の崖問題・サービス停止等）に向かいあうことで、それまでの「方針」を断念し、その間の投資を無駄にし、何が問題であったか、どうすれば回避できたかを理解する間もなく、また別のプロジェクトを立ち上げ、同じような課題を繰り返して採りあげるという「負のスパイラル」に陥ることです。

SMS の導入における 3 番目のメリットは、「ISO/IEC 20000-1:2018」の箇条 8 に示す、多くの密接したプロセスから構成されていることが挙げられます。これらのプロセスは、サービスの品質、実現に何が必要かという点から細分化・グループ化されており、網羅的に整備された規格となっています。

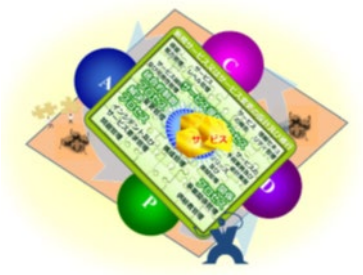
（2020 年開催第 97 回 JIPDEC セミナー「DX 推進エンジンとしての『JIS Q 20000』の活用」の講演資料より引用）

図 2-5　提供サービスのプロセス

これらのプロセスの狙いは、SLA の範囲の中で、組織のビジネスニーズを満たす最良のサービス、すなわち、顧客満足度が高く（高可用性を含む）、費用対効果が高く（DX 化された）、リスクが最小限のサービスを提供することにあります。もちろん、これらのプロセスは、非 IT サービスを提供・運用する際にも同様な利点をもって適用することもできます。

これらのプロセスを効果的に組み合わせ、それぞれの組織における関係者への影響や利害、それらをマネジメントするために定めた戦略を検討し、支援する内外の供給者との関係やパートナシップを構築し、様々な課題に対するリスクを最小化し、サステナブルなサービスの提供が実現できることが最大のメリットと考えます。

[2] 参考 URL：「ITSMS 認証に関するガイド類」https://www.jipdec.or.jp/library/smpo_doc.html#12



本書では、クラウドサービス提供における高可用性の実現を課題として取り上げていますが、これらの課題に対しては、「8.7 サービス保証」の「8.7.1 サービス可用性管理」、「8.7.2 サービス継続管理」のプロセスとサービスの高可用性を阻害する問題やインシデントを解決するためのプロセス「8.6 解決及び実現」のプロセスを組み合わせて、適用することが重要と考えます。

3 章では、サービスの可用性管理、継続性管理の意義や重要性について解説し、4 章において、3 章で示した ISO/IEC 20000-1:2018 の「8.7 サービス保証」と密接な関係のある「8.6 解決及び実現」の各プロセスとの連携（プロセス間の連携）について解説します。また、5 章では、これらのプロセスを実装し、サービス提供を効率的に展開している事例を紹介します。

コラム：DX 認定制度

このコラムでは、DX 認定制度[3]の概要と、ISO/IEC 20000 との関連について説明します。

DX 認定制度とは、DX 推進に伴い、2020 年 11 月より経済産業省が設けた認定制度です。本制度では、国から DX への取組みをしている優良企業として、DX 認定を受けることができます。

本認定制度では、「デジタルトランスフォーメーション（DX）」を以下のように定義しています。

> デジタルトランスフォーメーション（DX）の定義
>
> “企業がビジネス環境の激しい変化に対応し、データとデジタル技術を活用して、顧客や社会のニーズを基に、製品や サービス、ビジネスモデルを変革するとともに、業務そのものや、組織、プロセス、企業文化・風土を変革し、競争上の優位性を確立すること”。

一方、本制度では、DX とは、単に**以下のプロセスを充足することではない**とも警告をしています。

プロセスを電子化して ●データをとって使う ●レガシーを刷新する ●人間を AI におきかえる

従って、経済産業省では、DX の定義に沿って、以下のようなデジタル戦略をもって取り組む優良な事業者を申請に基づき認定する制度としています。

デジタル技術を使って ●つながり方を変えて ●本当にやりたかったことをやる

すなわち、**経営戦略とデジタル戦略は一体化させ、ユーザー視点で新しい価値を提供可能な組織** を評価する制度です。ここで、組織とは全ての事業者のことであり、法人と個人事業者（法人は会社だけではなく、公益法人等も含みます）が対象となります。また、ユーザーとは、ISO/IEC 20000 で定義する「顧客」同様、経営陣・職員・社員・パートナ等の内部顧客を含むユーザーであり、ユーザー視点とは、全ての利用者のことを示しています。

DX 認定の審査では、DX を推進していく準備ができている状態「DX-Ready の状態」であるかを「認定基準」とし、準備が整っていると認められる企業を国が認定します。「認定基準」の内容は、経済産業省が公表した「デジタルガバナンス・コード[4]」に基づいており、コードの各項目に対応する内容を申請書に記載することが求められます。

申請書の項目は以下のとおりです。

(1) 企業経営の方向性及び情報処理技術の活用の方向性の決定

(2) 企業経営及び情報処理技術の活用の具体的な方策（戦略）の決定

(2) ① 戦略を効果的に進めるための体制の提示

(2) ② 最新の情報処理技術を活用するための環境整備の具体的方策の提示

(3) 戦略の達成状況に係る指標の決定

(4) 実務執行総括責任者による効果的な戦略の推進等を図るために必要な情報発信

(5) 実務執行総括責任者が主導的な役割を果たすことによる、事業者が利用する情報処理システムにおける課題の把握

(6) サイバーセキュリティに関する対策の的確な策定及び実施

申請項目全般を通じて、ISO/IEC 20000-1:2018 との関連性が強く、(6)サイバーセキュリティに関する対策の的確な策定及び実施に関しては、ISO/IEC 27001（情報セキュリティマネジメントシステム－要求事項）や ISO/IEC 27017（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）が役立つと考えられます。

[3] DX 認定制度（情報処理の促進に関する法律第三十一条に基づく認定制度）：
https://www.meti.go.jp/policy/it_policy/investment/dx-nintei/dx-nintei.html

[4] デジタルガバナンス・コード（経済産業省）https://www.meti.go.jp/shingikai/mono_info_service/dgs5/pdf/20201109_01.pdf

3 サービス可用性管理、サービス継続管理の重要性

前章では、1 章に示したクラウドサービスの提供と利用における可用性に関する課題の解決に役立つ ISO/IEC 20000-1:2018 の概要及び導入のメリットについて解説しました。この章では、ISO/IEC 20000-1:2018 の中で記載されている、サービスを止めることなく利用可能な状態に保つために必要な、サービス可用性管理とサービス継続管理の重要性について説明します。

3.1 サービス可用性管理

サービス可用性とは、「あらかじめ合意された時点又は期間にわたって、要求された機能を実行するサービス又はサービスコンポーネントの能力」と定義されています。

サービスの可用性は一般的に、顧客と合意したサービス提供時間における、顧客がサービスを利用できた時間の割合で表されます。

$$\text{可用性（\%）} = \frac{\text{（合意済みのサービス提供時間 − 停止時間）}}{\text{合意済みのサービス提供時間}} \times 100 \quad \text{（\%）}$$

つまり、サービス可用性管理は、顧客や利用者が必要としている時に、合意された機能を確実に提供するための管理活動です。

ISO/IEC 20000-1:2018 ではサービス可用性管理について、以下のような活動が求められています。これらのサービス可用性管理の要求事項を満たすことで、顧客と合意したサービス可用性に関するコミットメントが満たされることを確実にすること、及び非可用性を最小限にすることが可能となります。

ISO/IEC 20000-1:2018 で求められているサービス可用性管理の主な活動は以下の通りです。

- サービス可用性のリスク（サービスの中断や品質低下等を引き起こす可能性のある脅威等に関するリスク）を評価し、文書化する必要があります。つまり、サービス可用性の観点でリスクアセスメントを実施し、その記録を確実に残すことが求められています。
- サービス可用性の要求事項（顧客と合意したサービス提供時間内で、提供しなければならない機能等）及び目標（サービス可用性の要求事項を満たしていることを示す指標、例えば稼働率 99.99%等）を決定し、文書化し、維持する必要があります。サービス可用性の要求事項と目標は、サービス可用性を設計する上で重要なインプットとなり、多くの場合、SLA やサービスカタログ等で明確化されます。
- サービス可用性は監視し、結果を記録し、計画外の非可用性（可用性目標の未達）が発生した場合は、調査し、必要な処置をとる必要があります。ここで言う「計画外の非可用性」は、インシデントとして取り扱われることが一般的であり、インシデント管理や問題管理と連携し処置が講じられます。

なお、サービス可用性管理と後述のサービス継続管理は、どちらもサービスが利用可能な状態を保つという目的があ

ることから、サービス継続管理の解説の中で、その関係や違いについて解説します。

3.2 サービス継続管理

サービス継続とは、「サービスを中断なしに、又は合意した可用性を一貫して提供する能力」と定義されています。つまり、サービス継続管理は、「サービスを停止させない」、「サービス品質を低下させない」、「万一、不測の事態が発生した場合にも、いかに即座に合意されたレベルまで復旧できるか」を実現するための能力を管理することを目的とした活動です。

以下のような ISO/IEC 20000-1:2018 で求められているサービス継続管理の要求事項を満たすことで、顧客へのサービス提供を継続するための合意されたコミットメントが、予見可能な状況において確実に満たされることが可能となります。

ISO/IEC 20000-1:2018 で求められているサービス継続管理の主な活動は以下の通りです。

- サービス継続のリスク（サービスの復旧を阻害する可能性のある脅威に関するリスク）を評価し、文書化する必要があります。つまり、サービス継続の観点でリスクアセスメントを実施し、その記録を確実に残すことが求められています。
- サービス継続の要求事項（目標復旧時間や目標復旧ポイント、レベル等）を決定する必要があります。サービス継続の要求事項は、サービス継続計画の中で、文書化されます。
- サービス継続計画を作成する必要があります。サービス継続計画では、次の表に示す項目を明確にする必要があります。

項目	解説
サービス継続の発動の基準及び責任	以下のように、“いつ、誰が、どのような状況の時にサービス継続計画を発動するのか”を定める必要があります。 ➢ 判断のプロセス、指針、基準 ➢ 発動通知方法 ➢ 発動責任者　等
重大なサービスの停止の場合に実施する手順	以下のような被害状況の確認方法やサービスの復旧方法等の具体的な手順を準備する必要があります。 ➢ サービスへの影響（被害状況や範囲）を可能な限り速やかに、且つ正確に把握するための手順 ➢ エスカレーションの基準と連絡先 ➢ 縮退運転か代替サイトへの切り替えかの判断 ➢ サービスへの影響、復旧見込みの顧客への報告 ➢ 復旧手順（操作方法、機器搬入やデータの移行、運用要員や保守要員の手配　等）　等
サービス継続計画が発動された	サービス継続計画が発動された場合に、サービスの縮小や縮退運転等の

場合のサービス可用性の目標	可能性を考慮し、サービス可用性の要求事項を満たすレベルを定めます。
サービス復旧の要求事項	サービスの目標復旧時間や目標復旧ポイント、復旧の優先順位等を定めます。
平常業務の状態に復帰するための手順	例えば、バックアップ環境や DR（Disaster Recovery）環境から切り戻すための判断基準や責任者、具体的な手順を準備する必要があります。

- 有事の際は、サービス継続の発動基準に従い、サービス継続計画に基づき速やかにサービス継続活動を遂行する必要があります。また、サービス継続計画を作成する際は、非常時対応におけるリスク（セキュリティレベルの低下、DR 環境へ切り替えることによる重要業務以外への影響等）に対しても十分な配慮が必要です。
- サービス継続計画は、あらかじめ定めた条件（タイミングや頻度）でサービス継続の要求事項に照らして試験されなければなりません。この試験は、サービス継続計画の実効性の評価、検証のほか、「サービス継続管理の組織への定着の促進」や「重大インシデント発生時の状況の模擬体験による、要員の判断力や対応能力の向上」という目的があります。

試験では、以下のような項目を考慮することが望まれます。

  - 試験におけるリスクを最小化する
  - 試験参加者は、あらゆる階層から選定する
  - 必要以上に広範囲に渡る試験の実施を目標とせず、要員への過度の負担を回避する
  - 重要性やリスクの高いサービスやシステムに関する試験を優先する
  - 過去に実施していない試験項目を優先する
  - 前回失敗した試験項目を再実行する　等

- サービス継続計画及び連絡先の一覧は、通常のサービス提供領域へのアクセスが妨げられた場合でも利用可能とする必要があります。ここで、“通常のサービス提供領域へのアクセスが妨げられた場合”について、物理的（ビルへの立ち入り制限等）、論理的（ネットワーク経由での接続不可等）アクセスが同時に妨げられるような、最悪の事態を想定し、備えておくことが効果的です。

今や、サービスは事業を成功させるための重要な要素となり、サービスの停止は直接的に事業の停止を意味することもあります。24 時間 365 日動き続ける事業の世界では、あらゆる状況下においてサービス継続とサービス可用性の管理は常に意識されなければなりません。

サービス可用性の管理は主に日常的に起こり得る可能性が高い障害（機器障害等）に着目しており、サービス継続管理は効果的な対策が直接実施できないもの（例えば地震、テロ等）やサービス全体にわたり大きな障害が発生しうる問題等に着目しています。つまり、サービスが利用可能であることに対して、可用性の管理は日常的な管理を行い、サービス継続管理は重大なサービス障害や災害等の発生時の管理を行うと考えると良いでしょう。

3.3 クラウドサービス（IaaS）の提供におけるサービス可用性管理とサービス継続管理

本項では、1 章で紹介したクラウドサービス（IaaS）の障害事例をもとにサービス可用性管理とサービス継続管理について、解説します。

障害によって発生するコストに関する考え方に、ダウンタイムコストがあります。このダウンタイムコストは、サービスを提供する P 社及び顧客である C 社ともに発生するコストです。ダウンタイムコストは、ダウンしている時間に関する、直接的及び間接的なコストの総和になります。直接的なコストは、クラウド上で稼働しているアプリケーションが、何時間か、あるいは何日か止まってしまった場合の、ビジネスが受ける損失と考えれば理解しやすいでしょう。一方、間接的なコストは、機会損失あるいは評判といった要素を含むコストです。この間接的なコストにはサービスがダウンすることによる顧客満足度の低下、競合他社と比較しての評判、株価といったものが含まれ、場合によっては直接的なコストの数倍から数十倍に達する可能性も指摘されています。そして、このダウンタイムコストはサービス可用性管理において有効性の測定基準の 1 つとなり得ます。

P 社が提供しているクラウドサービス（IaaS）の可用性のレベルは、利害関係者（顧客である C 社等）からのビジネス要求で決定されます。サービスに対する可用性の要求は測定可能な数値で表され、サービスを提供する側（P 社）とサービスを利用する側（C 社）との合意文書（SLA）により文書化されます。SLA ではサービス可用性に関する項目を含むことは必須とされていて、測定可能な数値として本書の 3.1 で紹介した稼働率等で示されることが一般的です。

では、P 社はサービスの可用性について、どの程度のものをあらかじめ用意しておくことが妥当だったのでしょうか？クラウドサービス（IaaS）を提供する IT 環境の設計・構築において、可用性の観点から考慮すべき項目には、コンポーネントの冗長化はもとより、次のようなものが考えられます。

- 監視ツール、監視システムの構築
- バックアップ/リカバリーの対策
- SPOF（Single Point of Failure：単一障害点）の検出と排除あるいは対策
- 大規模障害発生時のサービス復旧の対策

これらの項目からもわかるように、IT インフラストラクチャのコンポーネントの冗長化を進めておけば万全ということではありません。クラウドサービス（IaaS）の運用管理が必要であることを示唆しており、予期せぬ障害に対する対応を可能とする仕組みを、事前に検討し準備しておく必要があります。そのために、本書の 3.2 で紹介したサービス継続管理が役立ちます。サービス継続管理で提唱するリスクアスメント活動を通じ「予期せぬ障害の範囲を可能な限り狭める」、「復旧活動を阻害する脅威を事前に備える」ことが可能となる他、障害発生時にとるべき対応（サービス継続計画）の訓練を確実に実施しておくことで、障害発生時の混乱を抑え、要員が適切に行動できるよう備えることができます。この事前の準備は、P 社及び C 社ともに実施しておくべきことであり、特に 1 章で紹介したクラウドサービス（IaaS）の障害事例では、C 社がリストア作業に想定を上回る時間を要してしまったことが紹介されています。この事例もサービス継続管理を適切に実施していれば十分に防ぐことができた事例ではないでしょうか。

前述のように、予期せぬ障害や障害発生時の対応について、サービスのリスクを明確にし、効率的に管理し、継続的に改善していくための事項をまとめた国際規格が、ISO/IEC 20000-1:2018 です。ISO/IEC 20000-1:2018 は、サービスマネジメントシステム（SMS）に関する国際規格で、サービスマネジメントのベストプラクティスをもとに制定されています。包括的なベストプラクティスは、可用性管理活動の参考になるだけでなく、インシデント管理、問題管理といったクラウドサービス（IaaS）の運用の仕組みを構築する上での参考になります。

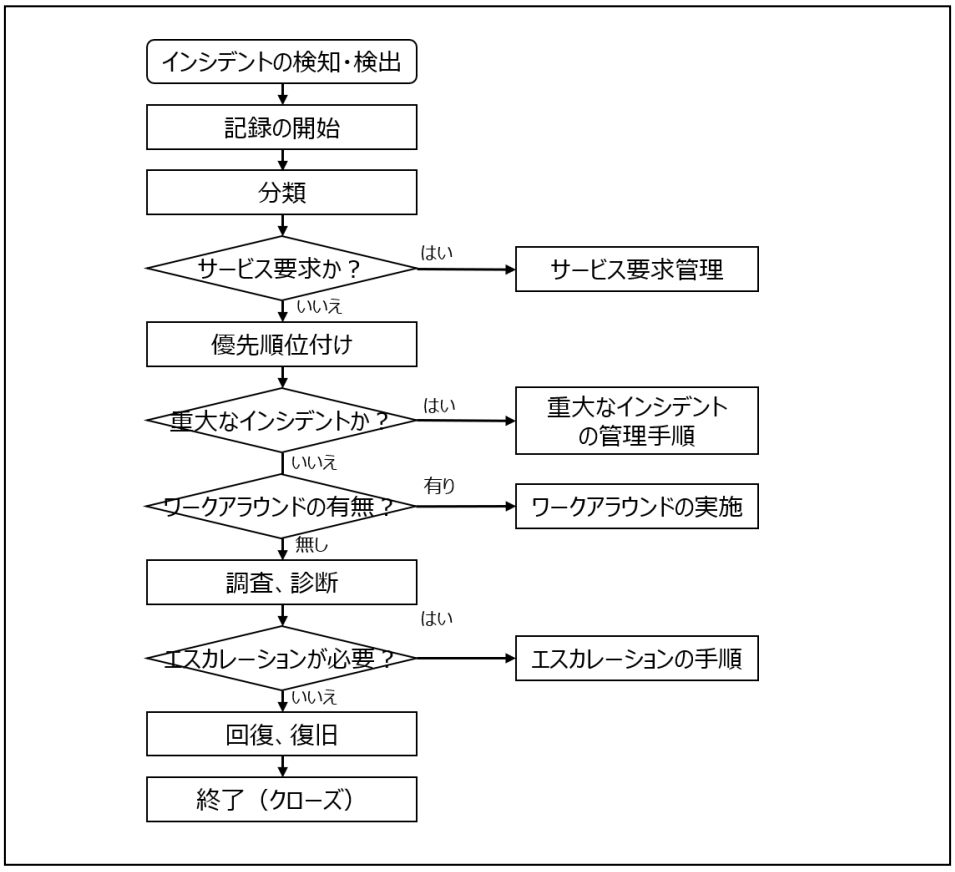
4 サービス可用性、サービス継続を支える活動 ～インシデント管理、問題管理～

前章では、サービス可用性管理及びサービス継続管理の重要性について解説しました。この章では、サービス可用性及びサービス継続を支える関連活動である、インシデント管理及び問題管理の役割と関係について解説します。

4.1 インシデント管理とは

インシデントとは、「サービスに対する計画外の中断、サービスの品質の低下、又は顧客若しくは利用者へのサービスにまだ影響していない事象」のことです。ここで、「顧客若しくは利用者へのサービスにまだ影響していない事象」の例としては、冗長化しているディスクの 1 つに起きた障害があります。

インシデント管理は、通常のサービス運用を可能な限り迅速に回復させ、事業へのマイナスの影響を最小限に抑え、合意したレベルのサービス品質を維持することを目的としています。そのため、インシデント管理では、あらかじめ定められたフローに従って、インシデントが処理されます（図 4-1 参照）。



（JIPDEC「ITSMS ユーザーズガイド-JIS Q 20000-1:2020 (ISO/IEC 20000-1:2018)対応-」の図 8-7 をもとに作成）

図 4-1 インシデント管理フロー

ISO/IEC 20000-1:2018 は、重大なインシデントを特定し、重大なインシデントのための管理手順に従って管理することを要求しています。「重大なインシデント」とは、事業への影響度が最上位に分類されるインシデントで、深刻なサービス中断の原因になる場合があります。したがって、より短時間で緊急の手順に従って処理される必要があります。

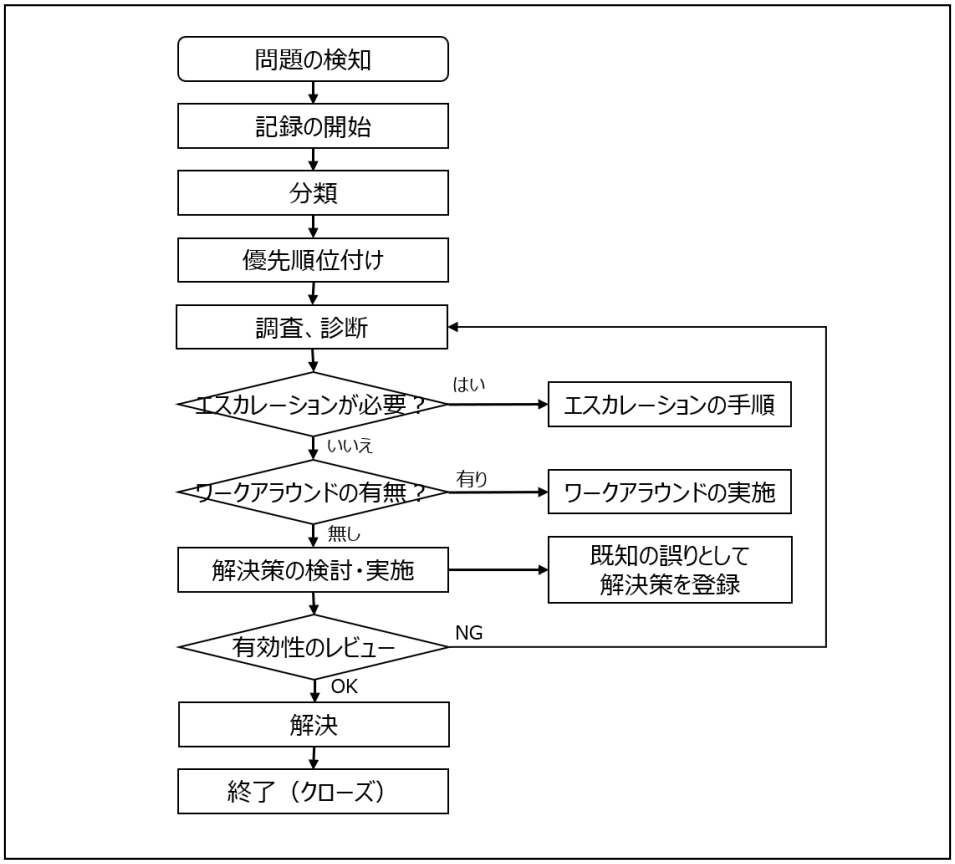
インシデント管理フローの中にある「ワークアラウンド」とは、完全に解決することができないインシデントや問題の影響を低減又は排除することです。例えば、障害が発生したサービスの構成要素を再起動することです。インシデント管理で

は、サービスをより早く回復することが優先されますので、既にワークアラウンドがある場合、これを実施することで一時的にでもサービスを回復させることができます。「ワークアラウンドの有無」とは、問題管理において登録された既知の誤りを検索してワークアラウンドが見つかった場合に、インシデント管理でワークアラウンドを適用するという意味です。「4.2 問題管理とは」も併せてご参照ください。

4.2 問題管理とは

問題とは、「一つ以上の実際に起きた又は潜在的なインシデントの原因」のことです。

問題管理は、インシデントや問題が事業に対する中断を最小限に抑えることと、インシデントを引き起こした根本原因の検知と、恒久的な解決を提供し、更に、再発を防ぐ予防までを目的としています。そのため、問題管理では、あらかじめ定められたフローに従って、問題が処理されます（図 4-2 参照）。



（JIPDEC「ITSMS ユーザーズガイド-JIS Q 20000-1:2020 (ISO/IEC 20000-1:2018)対応-」の図 8-8 より引用）

図 4-2 問題管理フロー

問題管理でも、ワークアラウンドが既に存在する場合、問題が完全に解決するまでそのままにしておくのではなく、サービスを一時的に回復させるためにワークアラウンドを実施することが必要です。

問題を解決するためには、根本原因、あるいはサービスへの影響を低減若しくは除去する方法であるワークアラウンドを特定する必要があります。そして、この根本原因とワークアラウンドが判明している問題を、「既知の誤り」として登録しておく必要があります。それは、さらなるインシデントや問題が発生した場合に、より早くサービスを回復できるようにするた

めでもあり、素早く診断及び解決できるようにするためでもあります。

問題管理には、リアクティブな側面とプロアクティブな側面があります。リアクティブな問題管理では、1 つ以上のインシデントの発生に対応して問題を解決します。プロアクティブな問題管理では、同じようなインシデントが再び発生する前に、問題を解決します。

4.3 サービス可用性管理とインシデント管理及び問題管理

サービス可用性管理では、サービスの可用性を監視し、計画外の非可用性を認識した際に、調査・分析し、可能な限り早くサービスを回復させます。

サービスの可用性は、サービスの障害発生の頻度と障害発生後の復旧の速さによって決まります。これらは、それぞれ平均故障間隔（MTBF：Mean Time Between Failure）、平均サービス回復時間（MTRS：Mean Time to Restore Service）で表すことができます。したがって、サービスは、高い MTBF を実現するように設計・構築され、運用されます。そして、サービスが停止した場合には、サービスをできる限り早く復旧できるように、つまり MTRS を最小化するように対処します。

サービスが停止した場合、事業に与える影響を最小限に抑え、できる限り迅速にサービスを回復させるために、サービス停止の要因となっているインシデントの継続時間と影響を最小限に抑えることが必要です。このとき、インシデントによるサービスの総停止時間を、インシデントのライフサイクルの各段階に分解し対応付け、インシデント管理及び問題管理と連携して調査・分析することが有効です（図 4-3 参照）。

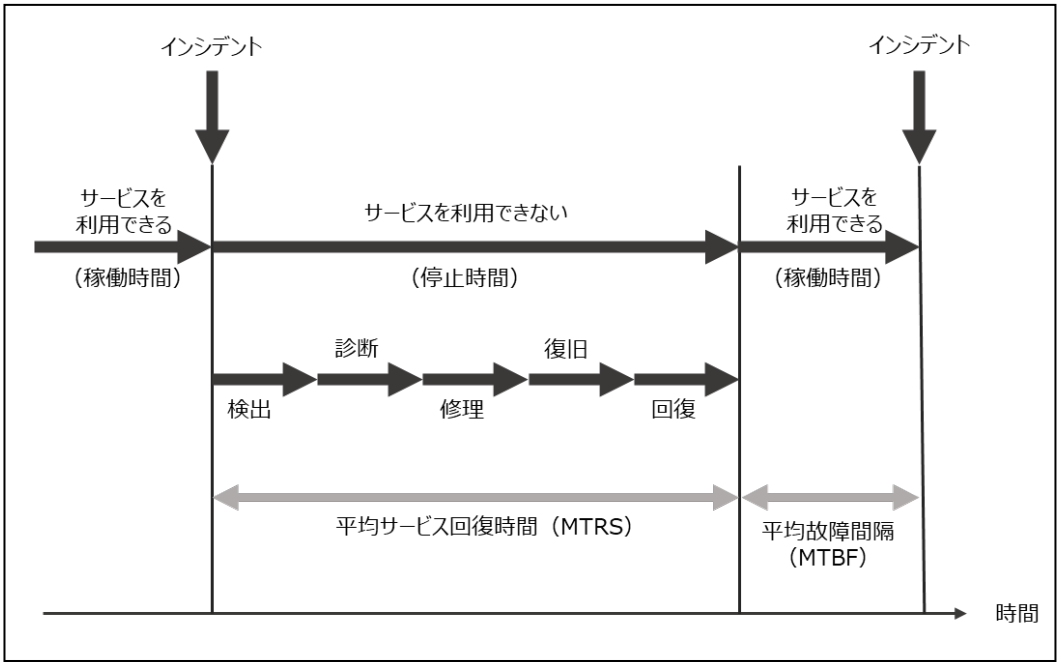


図 4-3 インシデントのライフサイクル分析

サービス可用性におけるインシデントのライフサイクルの各段階の説明は以下の通りです。

①インシデントの検出：サービス提供者がインシデントを認識した段階

②インシデントの診断：根本原因を特定するための診断が終了した段階

③インシデントの修理：障害が修理又は修正された段階

④インシデントの復旧：コンポーネントの復旧が完了した段階

⑤インシデントの回復：通常のサービス提供が再開された段階

サービス可用性管理にも、リアクティブな側面とプロアクティブな側面があります。リアクティブなサービス可用性管理では、実際に非可用性を認識している状態なので、関連する全てのサービスとコンポーネントの可用性をモニタリングし、認識した非可用性を調査し、是正措置を取ります。プロアクティブなサービス可用性管理では、新規又は変更されるサービスが、合意されたレベルの可用性を提供できるように計画を立案し、設計すること、サービス継続管理と連携してリスクアセスメント及びリスク管理を行うこと、そして可用性を継続的にレビューし、必要に応じて改善することです。

インシデント管理や問題管理は、リアクティブなサービス可用性管理の一環として連携して機能するだけでなく、プロアクティブなサービス可用性管理にも貢献しています。プロアクティブな問題管理によって、インシデントの再発を防止することができるため、MTBF を高く維持することができます。さらに、サービスの回復に利用できるワークアラウンドを通じて、より迅速にインシデントを解決することができるので、MTRS を低減することができます。

サービスは、障害が発生しないことが理想ですが、実際にはそれは不可能です。サービスは、様々な外的・内的要因によって障害が発生する、「脆弱（fragile）」なものです。例え、「堅固（robust）」なサービスを設計・開発したとしても、想定外の障害には対処できないことが多々あります。

そこで、そのような想定外の障害が発生しても、柔軟に対応し、被害を限定的に抑えるようにコントロールすることで、安全かつ安定した状態を維持することができるような「回復力のある（resilient）」サービスであることが求められます。

サービス可用性管理が、その目的を達成し、常に安定的にサービスを提供し続けるためには、障害が発生することを前提にして、インシデント管理や問題管理と密に連携して対処することが重要です。さらに、イベントやインシデントを含む障害の自動検出や自動エラー復旧を支援するツールを活用することも有効です。

4.4 サービス継続管理とインシデント管理及び問題管理

サービス継続管理では、事業を支えるサービスに深刻な影響を与えるイベントである災害が発生しサービスが停止した際に、サービス継続計画に基づき、サービスへのリスクを受容可能なレベルまで軽減するとともに、合意した時間内にサービスを復旧します。

サービス継続計画が発動されるのは、サービスの中断や事業に対するリスクが通常の対応、つまりインシデント管理や重大なインシデント管理手順で対処できない場合です。それほど重大でないイベントはインシデント管理で処理されます。そして、重大であってもそれほど深刻な影響を与えることはないインシデントは重大なインシデント管理手順の一環として処理されます（図 4-4 参照）。そのため、事前に、インシデント、重大なインシデント、及び災害によるサービス停止の違いを明確に定義し、関係者間で合意しておく必要があります。

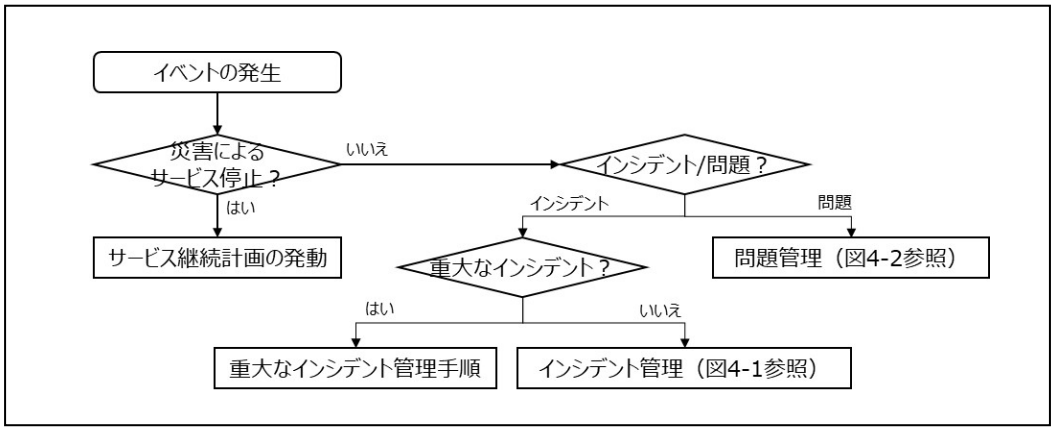


図 4-4　サービス継続管理とインシデント管理及び問題管理

　また、インシデントや重大なインシデントの原因が深刻な影響を与える災害を誘発する可能性があります。したがって、インシデント管理及びプロアクティブな問題管理でインシデントや重大なインシデントの発生を未然に防ぐことは、サービス継続の観点からも重要です。

5 実践事例と導入効果の紹介 ～株式会社ＴＫＣ～

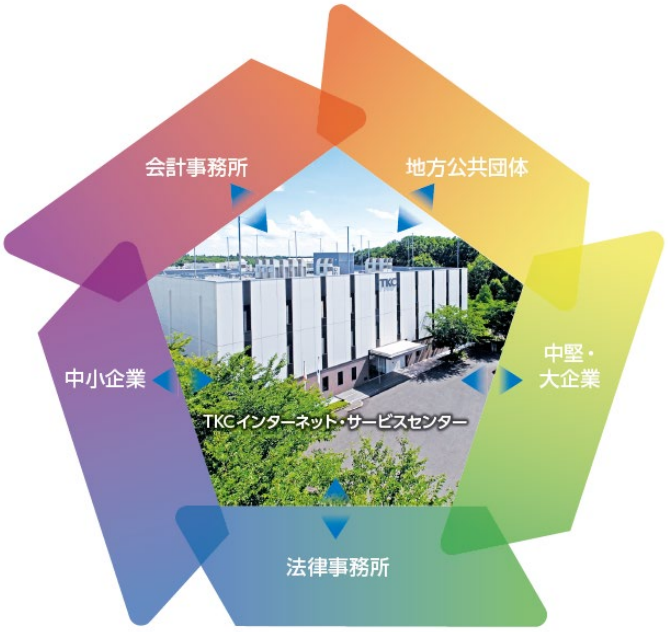
本章では、税務と会計に特化され大小様々な企業様や地方公共団体向けのクラウドサービスを提供されている株式会社 TKC 様に、SMS 導入の目的、実際に得られた効果、SMS をクラウドサービスへ適用するためのポイントについてご紹介頂きました。

5.1 会社説明、サービス説明

（1）当社は、会社定款（第２条）に次の二つの事業目的を掲げ、昭和 41 年に創業しました。以来、一貫して会計事務所と地方公共団体（市町村等）に専門特化した情報サービスを提供し、情報産業界において独自の地位を築いてきました。

1　会計事務所の職域防衛と運命打開のため受託する計算センターの経営

2　地方公共団体の行政効率向上のため受託する計算センターの経営



（2）平成 15 年、「お客さまが安心して利用できる当社専用のデータセンターが必要」と考え、自社のデータセンターを建設しました。

当社のお客さまの社会的な役割や業務を考え、単に「便利」なだけでなく、24 時間 365 日、安全にサービスを提供し、万が一のトラブルにも迅速、的確に対応できるよう、自社のデータセンターを建設し、お客さまの業務知識を有する自社の正社員がサービスの運用管理を担っています。

当社のデータセンターでは、当社のお客さまである会計事務所とその関与先企業、地方公共団体、中堅・大企業等に自社で開発したクラウドサービスを提供しております。

5.2 ＳＭＳ導入の目的（期待していた効果）

（1） SMS の継続的改善プロセスを通して、当社クラウドサービスのシステム事故やトラブル発生時の早期復旧、未然防止できる運用体制の基盤構築を目指して SMS を導入しました。

（2）また、お客さまが安全、安心、便利に当社クラウドサービスをご利用いただけるよう、サービスの変更管理プロセス、問題管理プロセス等の各プロセス管理活動の強化を図り、クラウドサービスの可用性と継続性の向上を目指して SMS を導入しました。

5.3 実際に得られた成果（全般）

（1）SMS 導入以前より、データセンターの IT 機器更新作業に関する変更管理手続き、インシデント管理・問題管

理の運用を実施してきました。各管理業務は実業務の中でおのおのが連携して運用されていましたが、明確に体系化されたものはありませんでした。

そこで、SMS の規格要求事項に照らし合わせ、各管理業務の役割、責任の所在、管理業務間の相互関係を整理し明文化しました。また、SMS の活動を推進するための各会議体についても開催目的、主催者、参加者、開催頻度を見直し整理しました。

その結果、プロセス活動の役割と責任者、プロセス間の連携が明確になり、管理業務を標準化することができました。また、各プロセス管理に KPI（重要業績評価指標）を設定、評価することで活動の有効性を可視化することができ、サービス品質の改善効果を実感できるようになりました。

（2）その一例として、変更管理、リリース管理における変更・リリースの種類とその対応は SMS の規格要求事項で定めてられています。

当社のデータセンターでは、IT 機器更新作業はクラウドサービスの中断事故に直結するため“重大な変更”と定義しています。そのため、このような重大な変更を行う際は、更新作業の企画、設計、作業計画、有効性評価の各工程でレビューを実施し、SMS 管理責任者の承認後、次工程へ進む仕組みとしています。

企画、設計、作業計画の各レビューでは、計画の妥当性、想定されるリスクの抽出と対策を検討しています。企画のレビューでは、実施目的、想定されるリスクの検討はもとより、最高責任者、現場監督者、各担当者の選任と役割を決定します。また、作業計画のレビューでは、変更作業を失敗した時の切り戻しの判断ポイントと切り戻し手順を準備している、切り戻し時間を含めたスケジュールを組んでいるといった基本項目が設定されていることを確認します。

上記の工程を標準化し実績を積み重ねてきたことで、サービス中断に直結するような変更作業も安全かつ確実に遂行できる体制基盤となったことを実感しています。

5.4 実際に SMS を導入、運用してみた感想（クラウドサービスとの親和性）

（1）SMSの導入にあたっては非効率、無理、無駄を排除し、シンプルかつ強力なプロセスを構築することを活動指針の一つとしていました。

当社データセンターでは ISMS を認証取得していたため、マネジメントシステムにおける PDCA のフレームワークや文書管理、情報セキュリティ管理等の管理プロセスは統合して運用しました。また、SMS の規格要求事項にある文書や記録書類は、ISMS で発行済みのものを一部改訂し双方の規格に対応できるような形式にしました。さらに、各会議体の出席者、議題、使用する資料、開催頻度、共通用語の定義の見直し等にも取り組みました。

SMS 導入前は、認証規格が増えることで各責任者、運用担当者に大きな負荷がかかるのではないかと予想していました。しかし、従前の活動や管理文書等を統合し、かつ整理できたことで SMS を比較的スムーズに導入することができ、導入後も運用担当者等への負担は増えることなく運用できています。

一方で ISO/IEC 27000 シリーズとの統合化は道半ばです。これからも継続的な改善に取り組み、よりシンプルかつ強力なプロセス構築を目指していきます。

（2）SMS は、IT サービスの品質管理に関する国際規格です。IT サービスの品質管理には、情報セキュリティだけでなく、サービスの可用性と継続性に関する要素も多く含まれています。クラウドサービスを提供する当社データセンタ

ーにおけるお客さまからのニーズは、万全な情報セキュリティ体制とクラウドサービスを常時利用できることです。

当社データセンターは、これまでの情報セキュリティ体制の強化に加え、クラウドサービスの可用性のさらなる向上を目指すために SMS を導入しました。また、SMS の規格要求事項に適合した運用体制を整備したことで、業務の可視化と標準化を実現することができました。導入後は PDCA のマネジメントサイクルの実践を通して、クラウドサービスの品質向上に向けた継続的な活動がさらに活発になりました。

5.5 SMS をクラウドサービスへ適用するためのポイント

（1） 適用組織の決定

SMS は、IT の運用・保守に焦点を当てた IT サービスの品質管理に関する国際規格です。当社は、自社で開発したソフトウェアを自社のデータセンターからクラウドサービスとしてお客さまに提供しています。また、クラウドサービスをお客さまにご利用いただくためのサポートも行っています。このように当社のクラウドサービスには、開発部門、営業部門、クラウドサービスの運用・保守部門といった複数の部門が関わっています。

SMS を導入するにあたり、適用組織を全部門にする方法もありましたが、当初の導入目的から鑑みて、データセンターでクラウドサービスの運用・保守業務を担当する部門としました。開発部門と営業部門は内部供給者と位置付けています。

これによって適用する業務範囲、適用組織が提供するサービス等を明確にすることができ、フレームワークを固めることができました。

（2）各プロセス管理の役割と目標設定

SMS における実行は、各プロセス管理の活動になります。各プロセスは、単体で活動するのではなく、相互に連携しています。各プロセス管理の活動を活発かつ計画通りに遂行するために、管理責任者を設け、担当する役割を明確にしました。また、各プロセス管理には KPI を設定し活動の成果、有効性を評価できる仕組みを構築しました。

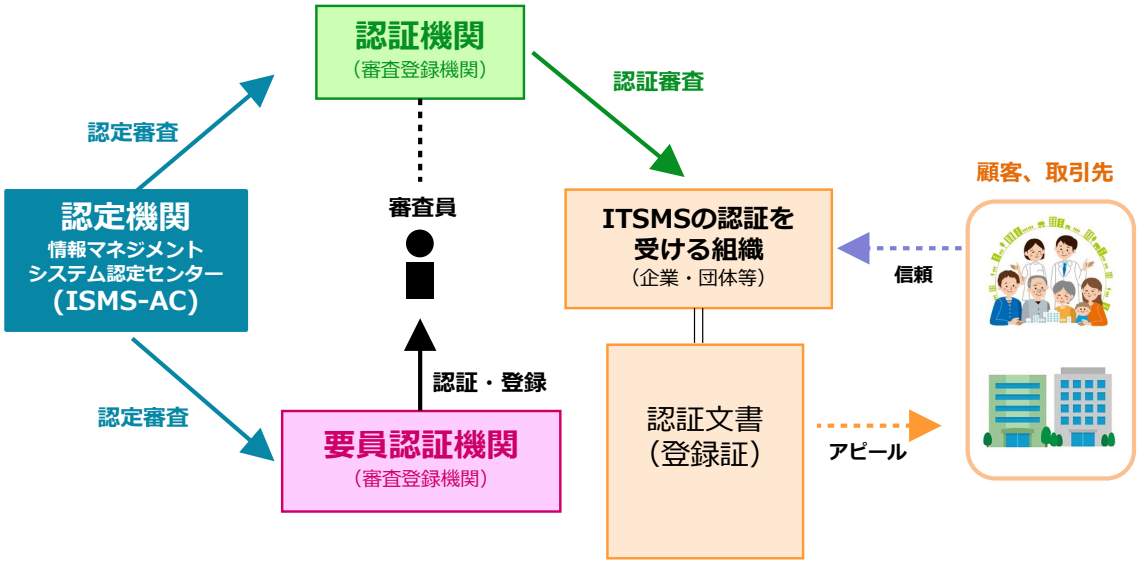
クラウドサービスの提供に必要な容量や資源のモニタリング、キャパシティ計画の立案、新規 IT 機器導入における変更作業の企画・実行・評価、構成管理の更新等、IT サービスのライフサイクル全体を各プロセス責任者が担当し連携することで、より強固な体制基盤を構築できていると感じています。

6 サービスの信頼性を示すには ～ITSMS 適合性評価制度～

本書で紹介したように、ISO/IEC 20000 に沿ってクラウドサービスのような IT サービスのマネジメントシステム（ITSMS[5]）を導入することによって、サービスの見える化、品質向上に向けた継続的な取組みを実施することができます。また、サービスを利用する組織においても、ISO/IEC 20000 に基づいてサービスの見える化を図ることができます。

さらに、ISO/IEC 20000 に基づく第三者認証を受けることによって、対外的にも IT サービスの信頼性をアピールすることができます。

JIPDEC 情報マネジメントシステム認定センター※は、ISO/IEC 20000 に基づく第三者認証の国際的な仕組みである、IT サービスマネジメントシステム適合性評価制度（以下、ITSMS 制度という）を 2007 年 4 月から開始しました。この制度は、認証を公正に運用するために定められている国際的な枠組みに従って運用されています。この仕組みは図で示すと次のようになり、「認証機関」、「認定機関」、「要員認証機関」から構成されています。



認証機関	第三者機関として組織の ITSMS を審査します。これを「認証審査」といいます。
認定機関	認証機関が適切に認証審査を実施できることを審査し、確認します。これを、「認定審査」といいます。
要員認証機関	認証審査に関する能力をもつ審査員を認証、登録します。

詳細は、認定機関である(一社)情報マネジメントシステム認定センター（ISMS-AC）の Web ページをご参照ください。

また、ITSMS 認証に関するユーザーズガイド等は、JIPDEC の Web ページで公開していますので、ご参照ください。

※ 2018 年 4 月に認定業務を行う「一般社団法人情報マネジメントシステム認定センター（ISMS-AC）」となりました。

[5] JIS Q 20000-1:2020（情報技術－サービスマネジメント－ 第 1 部：サービスマネジメントシステム要求事項）は、(IT)サービスのマネジメントシステム規格であり、(IT)SMS と呼ばれています。この規格内では SMS という表現で統一されているため、本書では規格に沿って SMS と表記していますが、制度名称は規格の名称にも記載されている通り、明示的に ITSMS としています。

コラム：認定機関が ITSMS 認証機関を認定する意義

認定機関である情報マネジメントシステム認定センター（ISMS-AC）は、認証機関が適切に審査を実施できる体制・能力をもっているかを、国際規格（ISO/IEC 20000-6）※に照らして審査し、適合していると認められる機関を認定して、「認定シンボル」の使用を許可しています。そのため、認定を受けた ITSMS 認証機関は、適切な ITSMS 認証審査を実施することのできる、信頼のおける認証機関であることを意味します。要員認証機関についても同様です。

認定シンボル（右）と認証機関マーク（左）が並んだ表示例

認定シンボルと認証機関のマークが 2 つ並んでいることは、その認証機関が国際規格に従った適切な審査を実施していることを、認定機関である ISMS-AC が保証していることを示します。

※ ISO/IEC 20000-6 情報技術－サービスマネジメント－第 6 部：サービスマネジメントシステムの審査及び認証を行う機関に対する要求事項

おわりに

企業の情報システム部門によるシステム構築では RAS という指標が使われていました。RAS は、Reliability（信頼性）、Availability（可用性）、Serviceability（保守性）の頭文字を意味していて、コンピュータデバイス、コンピュータシステム等の評価指標として利用されてきました。

クラウドサービスを提供する組織において不可欠なのは、セキュリティ対策、安定したサービス提供です。サービスを止めない、止まらないサービスを目指すためには、サービス提供における可用性に取り組むこと、すなわち、サービスに影響を与えうるリスクの監視と対策を取り続けることが重要となります。

ISO/IEC 20000-1:2018 におけるサービス可用性、サービス継続の考え方が、オンプレミス、クラウド、ハイブリッド（オンプレミス＋クラウド）の混在する環境での安定したサービス提供の一助となれば幸いです。

また、補足となりますが、クラウドサービス提供者だけでなく、1 章で紹介した事例のＣ社のようなクラウドサービス利用者や DX を推進する事業者においても、クラウドサービスが停止した際の事業に与える影響を経営者が認識するために、また DX 認定制度への申請への手助けとして、ISO/IEC 20000-1:2018（特に「8.3 関係及び合意」の事業関係管理、サービスレベル管理、供給者管理等）を役立てて頂ければと思います。

株式会社 TKC 様には、ご多忙な中、SMS の貴重な実践事例を寄稿していただきましたことに、深く御礼を申し上げます。

ITSMS 技術専門部会委員には、各章の分担を執筆いただき、多くの時間を委員会活動に費やしていただきました。この場を借りて、御礼を申し上げます。

最後に、本書の企画段階から全面的にサポートいただいた JIPDEC 事務局には、記して御礼を申し上げます。

一般財団法人日本情報経済社会推進協会
ITSMS 専門部会　主査　塩田　貞夫

付録　1 章における架空の障害事例（P 社）の技術的背景

クラウドサービス（IaaS）の可用性

P 社は IaaS のクラウドサービス提供者です。P 社のデータセンターに設置されているサーバー群は、供給電源の二重化、N+1 空調システム等々、電源喪失時の UPS 群などサーバーの設置環境としては申し分ないものです。

P 社の提供しているクラウドサービス（IaaS）では、仮想化技術を用いて、OS、ストレージ、ネットワークを仮想化しています。高パフォーマンスの IT インフラストラクチャに加えて、可用性、信頼性、セキュリティに配慮した、ミッションクリティカルな顧客向けのソリューションであることを謳っています。可用性に注目すると、次のような対策がなされています。

IT インフラストラクチャのコンポーネント（物理サーバー、ストレージサブシステム、ネットワーク機器等）では、各々が冗長化され、可用性の対策がとられています。物理サーバー上では、死活監視に加えて、ゲスト OS やアプリケーションの監視サービスを提供しています。ゲスト OS に異常が発生し、必要な場合には、他の物理サーバー上にゲスト OS を移転する“ライブマイグレーション”機能を備えています。

ストレージサブシステムでは、データアクセスにおける高可用性を実現しています。物理サーバーとディスクへのアクセスを管理するストレージサブシステム制御装置は、冗長化されたデュアル構成となっています。物理サーバーとストレージサブシステム制御装置の間では、ファイバーチャネルによる SAN（Storage Area Network）環境が冗長構成で構築されています。こうした構成にすることにより、物理サーバーとストレージサブシステム間では、複数の接続（マルチパス）を介したアクセスが実現されています。仮に、いずれかのパスで障害が発生した場合でも、他のパスが利用されることでディスクへのアクセスを可能にしています（図　付-1 参照）。

ディスクは RAID（Redundant Array of Independent Disk）で構成されています。

RAID は、ハードディスクを複数台組み合わせることにより、データ分散をして仮想的なディスクを構成し、可用性、対障害性を高める技法です。P 社の提供するストレージサブシステムでは RAID1（ミラーリング）を採用しています。RAID1 では、2 台 1 組のハードディスクを利用します。RAID1 では、常に同じ内容を 2 台のハードディスクが保持することになります。データを 2 つのハードディスクへ書きこむことで、万が一、一方のハードディスクが故障をしても、残ったハードディスクを利用してデータの書き込み/読み出しが可能です。

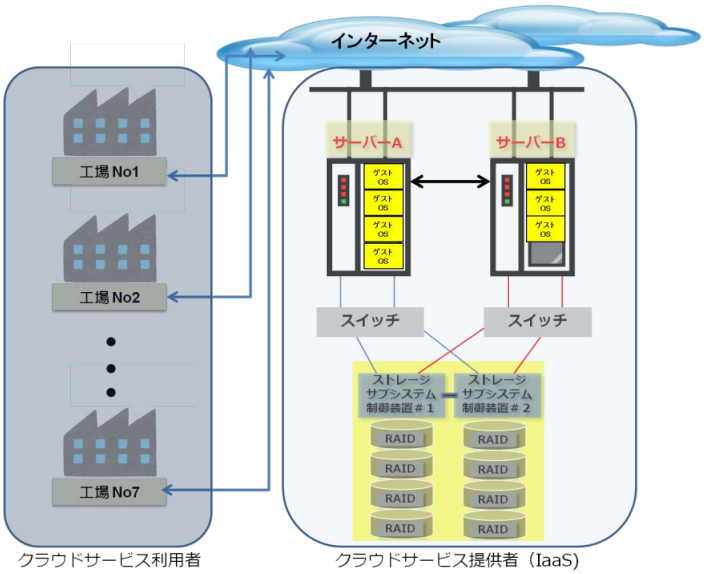


図　付-1　P 社提供のクラウドサービス（IaaS）

クラウドサービス（IaaS）の障害事例

ある日、クラウドサービスを利用している工場の一つから、「自工場　の生産管理システム（ゲスト OS）へアクセスができない」と、報告がありました。P 社のインフラ監視チームが調査したところ、ストレージサブシステム制御装置＃1 の管理下にあるディスクへアクセスできていないことが判明しました。

IaaS のストレージサブシステムは、ディスクへのアクセスパスを複数持ったマルチパス構成であり、ディスクは RAID1 を採用しています。ゲスト OS からディスクへのアクセスができなくなることは、想定外の事象でした。

調査を進めるうちに、他の工場でも、クラウド上にある、その工場の生産管理システムへのアクセスが極端に遅くなっているとの報告があがっていることが判明しました。障害状況は時間を追うにつれて深刻になり、最初の報告から数時間後には、全工場からアクセスできなくなり、サービスの全停止に陥りました。

長時間にわたる調査の結果、原因が判明しました。障害の引き金は、RAID1 を構成している 2 台 1 組のハードディスクの 1 台が故障したことにより引き起こされた、ハードディスク制御部のファームウェアのバグによるものでした。

本来であれば、RAID1 を構成しているハードディスクは故障を検知すれば、RAID1 から切り離されて、残ったディスクで処理を継続することができます。

ハードディスクを管理・制御しているストレージサブシステム制御装置＃1 は、物理サーバーとの間にあるスイッチ経路制御、冗長化されたストレージサブシステム制御装置間のプロトコルなどを機能として備えています。単なるハードディスク管理するための制御装置ではなく、複雑な処理をしている一つのシステムなのです。

ハードディスクのファームウェアのバグにより、ストレージサブシステム制御装置＃1 とハードディスクの間で切り離すことが難しくなり、異常なトラフィックを繰り返し生じた結果、アプリケーションの停止とクラウドサービス（IaaS）全体に重大な影響を及ぼしました。

また、障害の副作用として、一部の工場のゲスト OS では、データベースの整合性が取れなくなりました。サービスの復旧後にバックアップからのリストアを余儀なくされました。日次でバックアップが採られていない工場もあり、修復に時間を取られてしまい、日常的な運用に課題を残すことになりました。

＜1 章に戻る＞

コラム：ストレージサブシステム、RAID、ファームウェア

ストレージサブシステム（Storage Subsystem）

ストレージサブシステムは、コンピュータシステムの一部でありながら、ストレージに関連する部分が 1 つのシステムとしての構造を持っています。ストレージサブシステムに含まれるものとして、ハードディスク、ホスト(サーバー)へのアダプタ、ハードディスクへの制御装置、ストレージに関連した制御ソフトウェアなどがあります。

ストレージサブシステムの基本的な接続形態としては、DAS(Direct Attached Storage)、NAS(Network Attached Storage)、SAN(Storage Area Network)が知られています。

主要なストレージベンダーにおいては、ファイバーチャネル（FC）と SAN を接続することが一般的です。また、規模やコストに合わせ、ユーザー企業やスタートアップの企業等は、iSCSI と NAS を接続するストレージサブシステムを構成することがよく知られています。

コラム：RAID（Redundant Arrays of Inexpensive Disks）

RAID とは、2 台以上のハードディスクを仮想的に 1 つのドライブであるように認識させる技術のことです。RAID には RAID0、RAID 1 、RAID2、RAID3、RAID4、RAID 5 のレベルがあります。他にも RAID6、RAID50、RAID10 といった RAID が存在しますが、これらは RAID レベルの組み合わせ技術を表しています。例えば、RAID6 は RAID5 にパリティを追加したものであり、RAID10 は、RAID1+RAID0 を組み合わせたものです。

データを複数のハードディスクに分散して書き込む機能を備えた RAID なら、データ処理にかかる時間を短縮することもできます。大容量のデータを取り扱うことが多い場合、データ転送の速度を向上できるのは大きなメリットといえます。また、RAID を構成することで、1 台のハードディスクが故障してもデータが失われないという耐障害性を高めることができます。

ファームウェア（firmware）

ファームウェアとは、ハードウェアとソフトウェアの中間に位置するソフトウェアとイメージすれば判りやすいでしょう。世の中に設置されている数多くのインテリジェントな電子機器にはファームウェアが搭載されていることがあります。

ファームウェアはハードウェアを直接制御します。例えば、コンピュータ、ディスクドライブ、ルーターやブリッジなどのネットワーク機器、ノート PC などにはもちろん内蔵されていますし、最近では、多くの家電製品にも搭載されています。

コンピュータ上のソフトウェアである OS やアプリケーションソフトと異なり、ファームウェアは、通常は ROM(Read Only Memory)やフラッシュメモリーなどの IC(Integrated Circuit)内に格納されています。ファームウェアは頻繁に内容を変更するものではありませんが、機器のハードウェアのバグフィックスや改善などを、ファームウェアのパッチあるいはバージョンアップによって行います。

ＩＴＳＭＳ専門部会

（順不同・敬称略）

氏名	会社・機関名
【主査】 塩田　貞夫	洛ＩＴサービス・マネジメント株式会社
黒崎　寛之	株式会社ヒルアビット
岡田　雄一郎	コニカミノルタ株式会社
駒瀬　彰彦	株式会社アズジェント
中村　良和	日本マネジメントシステム認証機関協議会 （BSI グループジャパン株式会社）
オブザーバ	
星　昌宏	一般社団法人情報マネジメントシステム認定センター

〒106-0032 東京都港区六本木１丁目９番９号 六本木ファーストビル
一般財団法人 日本情報経済社会推進協会
URL https://www.jipdec.or.jp/