クラウドを利用した
システム運用に関するガイダンス

令和５年７月１日

内閣官房国家サイバー統括室

改定履歴

改定年月日	改定箇所	改定内容
2025 年 7 月 1 日	―	・初版決定

目次

1. はじめに

本ガイダンスは、増加するクラウドサービスの選定や利用、サービスを使った環境の構築や運用などを行うに当たり、クラウドサービスの「利用者[1]」（以下「利用者」という。）がクラウドサービスの基本を理解し、クラウドサービスにおけるインシデント（利用者にとって好ましくない事象や出来事）の発生を可能な限り抑制することや、インシデントが発生した際の対応及びステークホルダー（利害関係者）の連携によって事態の解決を図る重要性など、クラウドサービスの安全な運用に重点を置いた利用者向けの基本的なガイダンスの詳細版です。

昨今、個別の動作環境（ハードウェアやソフトウェア）を準備して、自らコントロールする「オンプレミス」のシステムに代わり、クラウドサービスを活用したシステム構築や運用が主流となってきています。確かに、利用者にとってクラウドサービスを利用することは、調達や導入の負荷軽減に寄与しますが、利用者からシステム運用や責任そのものがなくなるわけではありません。クラウドサービスでは、クラウド事業者が提供する動作環境を活用していることから、利用者が制御できない環境や領域が存在するため、利用者の目に見えないところでクラウドサービスの更新や仕様変更が行われます。

そのため、クラウド事業者の作業によってインシデントが発生する場合もあり、利用者はクラウド事業者からWebサイトへの公開等により提供される情報の把握や変更管理などを適切に行う必要があります。インシデントによってはクラウド事業者にもその原因が分からず、約款や利用規約などの取り決めにもない想定外の事態が発生する場合もあります。その場合は、クラウドサービスに係る全てのステークホルダー、関係機関や、サイバーセキュリティコミュニティが協力しながら、事案対応を行う必要があります。

クラウドサービスは約款による契約に基づいて提供されることから、利用者がクラウドサービスを活用し、顧客に対して何らかのサービス等を提供する事業を行っている場合、その顧客から見れば、利用者が当該サービスの提供元となります。このため、クラウド事業者側に起因するインシデントが発生した際、クラウド事業者は基本的には約款や利用規約で定めている範囲で責任を負う一方、それ以外の範囲については、利用者に責任が問われる場合があります。クラウドサービス利用に関して、初期導入の容易さや負荷軽減のメリットがある一方、オンプレミスと同等に利用者の責任は存在することから、システムの運用・維持体制の整備が不可欠であることを認識することが重要です。

我が国では、利用者が様々な情報技術を活用する場面において、自組織のみで対応が完結することは少なく、システムの構築や運用の全体や一部を外部に委託しているのが現状です。そのため、情報システム子会社やシステムインテグレータ（以下「SIer」という。）をはじめとしたステークホルダーを把握して、我が国全体（Cybersecurity for All）で対応することが欠かせません。

「デジタル・トランスフォーメーション」や「クラウド・バイ・デフォルト」が叫ばれている昨今において、クラウドサービスの活用は、事業継続や成長の観点からも欠かすことができません。利用者はクラ

[1] クラウドサービスを利用する事業者のほか、地方公共団体も含む。

ウドサービスの活用を一層推進する一方で、クラウドサービスの構造や責任範囲などについて理解を深めておく必要があります。また、クラウド事業者は、情報の非対称性を踏まえ、情報の公開や提示を実施し、我が国全体でクラウドサービスを安心・安全に使える社会にしていくよう努める必要があります。

2. クラウドサービスの基本理解

2.1. クラウドサービスを利用する背景

以前は、組織が利用するシステムは、自分たちで全てのハードウェアやソフトウェア(OS、ミドルウェアやアプリケーション)などを調達しなければなりませんでした。しかし、それでは初期投資に費用がかかることや、企画や設計からかなりの長い歳月を隔てなければシステム利用、そして事業そのものが開始できませんでした。それでは、変化の激しい現代社会において、大きな遅れをとることになります。そこで注目され、昨今の主流となっているのがクラウドサービスを活用した事業やシステムの展開です。

クラウドサービスと言ってもその形態は様々です。利用者はどのようなクラウドサービスを活用するのか適切に選定する必要があります。NIST SP800-145[2]などでも定義されているように、ハードウェアや仮想化ソフトウェアなどの基盤となる環境を整備しているのが「IaaS(Infrastructure as a Service)」、そしてOSやアプリケーションを制御、支援するミドルウェアまでの環境を整備しているのが「PaaS(Platform as a Service)」、さらにアプリケーションまでの環境を整備しているのが「SaaS(Software as a Service)」です。クラウドサービスは後者になればなるほど、クラウド事業者が提供する範囲が広がり、利用者はより早く活用することが可能です。

利用者は各社が提供しているクラウドサービスがどの分類に当てはまる(又は折衷的に提供している)サービスなのかを理解した上でクラウドサービスを活用し、利用者の責任範囲を明確にする必要があります。

また、これまで 3 つの分類で語られることが多かったクラウドサービスですが、昨今ではさらに細分化されています。例えば、様々な環境で利用可能なアプリケーションの開発ができるCaaS(Container as a Service)や、サーバレスでアプリケーション開発ができるFaaS(Function as a Service)等の形態が存在し、それらを組み合わせてシステムが構築されるようになり、より複雑化しています。

2.2. クラウドサービスのメリット・デメリット(リスク)

クラウドサービスは導入や構築が素早く行え、拡張性が高い一方で、外部の資源を活用しているので、組織のリスク管理そのものに影響し、自組織だけでは完結しがたい状況になります。また、これまで我が国のクラウドサービスは、事業継続性の観点だけではなく、初期導入面のコス

[2] NIST(アメリカ国立標準技術研究所)によるクラウドコンピューティングの定義
https://www.ipa.go.jp/files/000025366.pdf

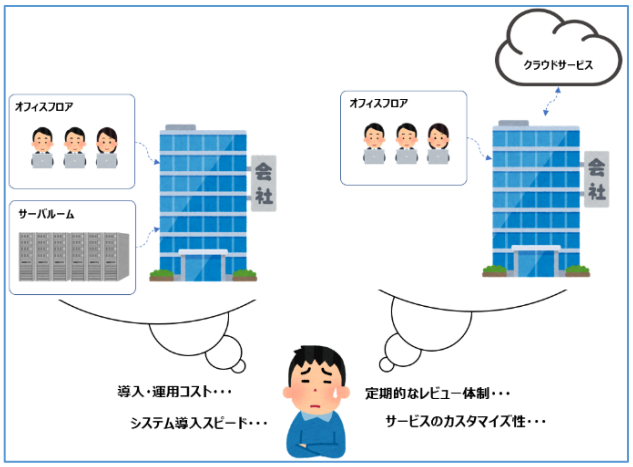
ト低減の視点から価格面が注目され、導入が進んでいる現状にあります。忘れてはならないのは、クラウドサービスであったとしてもシステムを運用し続けているという意識を持つことです。むしろクラウドサービスはクラウド事業者のタイミングで仕様や約款などの変更が行えるため、新たな仕様の確認や、設定の再確認等、運用にはそれ相応のコストがかかります。図１にまとめたメリットやデメリットを理解した上でクラウドサービスを活用しましょう。

メリット	デメリット
・導入や構築が素早く行える ・利用状況に応じた拡張性の高さ ・自組織で調達しない範囲の運用負荷の軽減 （※作業は軽減されても運用責任は残る） ・拡張機能が追加され続ける	・自組織のシステムやサービス意識の低下 ・カスタマイズ性が低い ・ステークホルダーが多く、リスク管理が自組織で完結し難い ・特定のクラウドサービスの専門知識が必要 ・仕様変更や機能拡張のたびにレビューしなければならない

図１ クラウドサービスのメリット・デメリット

コラム：クラウドサービスの必要性

クラウドサービスの特徴として、仕様の変更や機能の追加がしばしば行われます。利用者はそれらの機能を理解し、変更される仕様に対して都度レビューをしなければなりません。進化し続けるクラウドサービスは非常に大きな強みですが、それは利用者の負担とも考えられます。システムの調達や刷新を行う際、本当にクラウドサービスを活用するのが適しているのか、というポイントから検討するのが望ましいと言えます。政府はクラウド・バイ・デフォルトの考え方を提唱しておりますが、まずクラウドサービスを候補として検討するという考え方であり、クラウドサービスだけが選択肢であるものではありません。導入サービスの内容や組織体制によってはクラウドサービスが不向きなこともあり得ますので、オンプレミスの構成も十分に検討するのがよいでしょう。



コラム：セキュリティ担保の取組

利用者環境のセキュリティを実装するには利用者が責任をもって担保するべきものです。脆弱性診断のパッケージツールや SI サービス、ペネトレーションテストの SI サービスなど様々ありますが、ツールやサービスに一任するのではなく、明確な目的と意図をもってそれらのツール等を活用するべきです。

クラウド事業者側も、サービスの設定値やログを監視するツール等を提供しており、クラウドサービス側の仕様変更があった際に設定値の簡易的な確認が行えます。

しかし、どのような対策を講じてもセキュリティインシデントのリスクをゼロにすることはできません。許容できないインシデントリスクに対しては、サイバーリスク保険も選択肢のひとつとして検討することが考えられます。

3. クラウド事業者や利用者などのステークホルダーの責任等の理解

3.1. クラウドサービス活用におけるステークホルダーの理解

利用者にとっては、クラウド事業者からクラウドサービスを直接調達する場合や、販売者や構築者を介して調達する場合など、クラウドサービスの活用には様々なステークホルダーが存在します。利用者はステークホルダーを把握し、締結された契約の相手方、その契約内容(約款、利用規約等[3])及び契約に基づく責任範囲を把握する必要があります。クラウドサービスにおいては、その利便性から、クラウド上のデータのみを取り扱い、システム運用には関わらない事業者が存在する場合もあります。システム上のステークホルダー(表１)に加え、データを取り扱うステークホルダー(表２)についても把握する必要があります。なお、以下のステークホルダーについてはあくまでも例示であり、サービスによっては全てのステークホルダーが存在しない(利用者とクラウド事業者のみの)場合もあります。例えば、受託開発の場合、受託開発に加えてライセンスを利用する場合、利用規約に同意して利用する場合等、ステークホルダーの構成は様々です[4] 。

表１ システム視点でのステークホルダー例

項目	説明
利用者	クラウドサービスやシステムを利用する組織
販売者	クラウドサービスやシステムを販売する組織
構築者	クラウドサービスを活用してシステムを構築する組織 (利用者の子会社や SIer など)
設置者	クラウド構築者を支援して、実作業や設置を行う組織 (SIer や SIer の委託企業など)
運用者	構築されたシステムの運用を支援する組織 (SIer や SIer の委託企業など)
クラウド事業者	クラウドサービスを提供している組織 ※組織によっては日本国内には販売拠点や一時的なサポートを行う体制しかない場合があり、最終的なサポートの判断や解決策の提供などは、国外の拠点から行う場合もあるため、ステークホルダーはクラウド事業者の国内外の体制の確認を行うとともに、クラウド事業者は体制について開示する必要があります。
顧客	利用者がクラウドサービスを利用してシステムを構築し、何らかのサービス等を提供する対象者

さらに、昨今はシステム視点だけではなく、「データ」の視点も欠かすことができません。そもそもクラウドサービスを活用している時点で、オンプレミス型とは異なり、既にクラウド事業者がデータを保管しています。

---

[3] 約款、利用規約、利用条件等があり、取引条件を記載した文書を指す。

[4] 自治体の SNS 利用と個人情報へのアクセス
https://cio.go.jp/sites/default/files/uploads/documents/dp2021_04.pdf

クラウドサービスを利用し、利用者自身が作成した文書や資料であれば「保有者」であり、データの主体と言えます。また多重下請け構造に鑑みると、保有者が作成した文書や資料などについて、必ずしもシステムには依存せずに、クラウドサービス外においても、販売者、構築者、設置者、運用者がデータを保存している場合があります。データの保存者も保有者のデータの所在を明確にしておくなど、適切にデータを守らなければなりません。またクラウド事業者は保有者のデータを保管する者として、データの棄損や消失などがないよう保管しておく必要があります。なお、データの使用者や加工者は、保有者との利用契約等に基づいて(許諾を得る場合を含む。)、使用や加工を行います。

クラウドサービスに限られた話ではなく、昨今のシステム活用に当たっては、このようにデータ視点でのステークホルダーの理解も欠かすことができません。

表 2 データ視点でのステークホルダー例

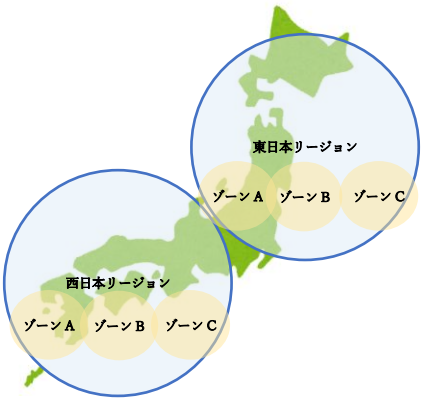
項目	説明
保有者	クラウドサービスに保存するデータを保有している者(独自にデータを作成した者等)
保存者	保有者のデータを保存している者(所有者の業務や作業などの委託事業者)
保管者	保有者のデータを保管している者(クラウド事業者)
使用者	保有者のデータを利用する者(情報収集者や所有者の許諾を得て利用する者)
加工者	保有者のデータを編集・修正する者

コラム：データセンターとリージョンについて

データセンターは、サーバやネットワーク等の装置を設置・運用することに特化した施設のことです。災害時に設備に極力支障が出ないよう耐震・免震構造となっており、24 時間 365 日安定した電力供給、安定した通信が行えるよう設計されています。クラウドサービスはハードウェアを意識せずに利用できますが、実体となるハードウェアはどこかのデータセンターで稼働しています。

日本国内で利用できるクラウドサービスを提供しているデータセンターは、必ずしも日本国内にあるわけではなく、データセンター内のデータ取扱について、国内法以外の法令及び規制が適用される場合があります。データセンターが設置されている国が、法制度や実施体制が十分でない、法の執行が不透明である、権力が独裁的である、国際的な取決めを遵守しないなどのリスクの高い国である場合、データセンター内のデータが法執行機関の命令により強制的に開示される等が考えられます。情報の開示が懸念される場合は、機関等の管理する暗号鍵で暗号化するなどの措置の検討や、クラウド事業者へデータ保護の措置等についての確認を行うようにしましょう[5]。特にマルチクラウド等を活用してシステムを運用する場合には、各クラウドサービスにおいてデータ保護の措置を検討する必要があります。

リージョン(region)とは地域、領域といった意味の英語で、クラウドの分野では地理的・ネットワーク的に独立したエリアのことを意味します。東日本リージョン、北米リージョンというように、クラウドサービスがどのリージョンで運用されているのかを表すのに使用されます。激甚災害等に備えるには、複数のリージョンで運用されるサービスを選択する必要があります。リージョン内をロケーションごとに分割したエリアのことをゾーンと呼びます。なお、クラウド事業者によってリージョンやゾーンの用語の定義や範囲に違いがあることにご留意ください。

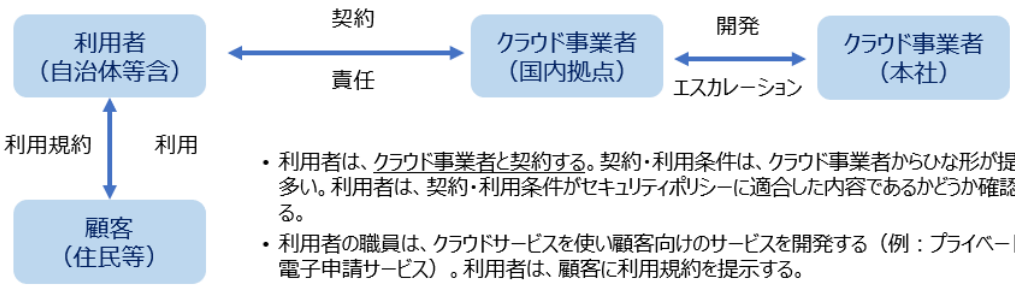


[5] 政府機関等の対策基準策定のためのガイドライン(令和５年度版)
https://www.nisc.go.jp/policy/group/general/kijun.html
遵守事項 4.2.1(1)(a)(ア) 「クラウドサービス利用判断基準」について

コラム：クラウドサービスのステークホルダー例

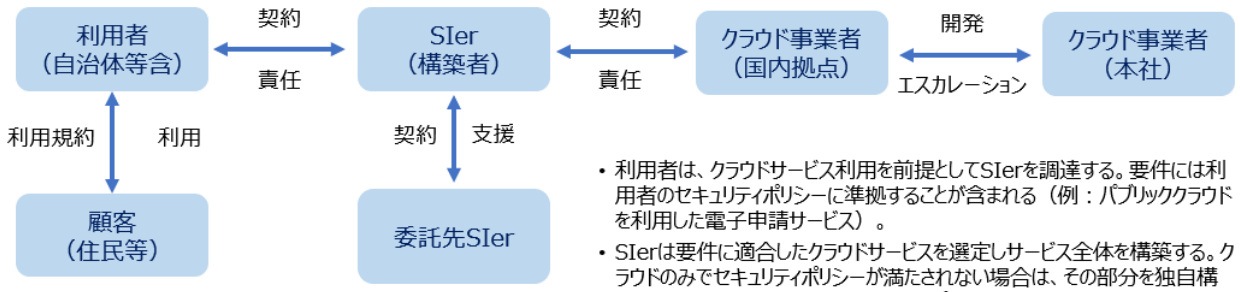
以下にクラウドサービスにおけるステークホルダーの例を示します。クラウド事業者やSIer（構築者）はそれぞれの間における契約や利用規約に基づき事業を行っています。利用者は関連する事業者等がどのような契約関係にあるのかに留意する必要があり、また顧客に対して提供するサービス自体の説明責任は利用者が負うものであることを認識する必要があります。

利用者がクラウドサービス契約者



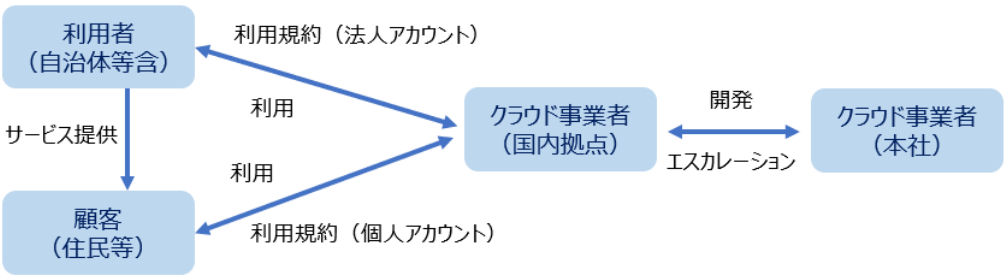
- 利用者は、クラウド事業者と契約する。契約・利用条件は、クラウド事業者からひな形が提供される場合が多い。利用者は、契約・利用条件がセキュリティポリシーに適合した内容であるかどうか確認したのち契約する。
- 利用者の職員は、クラウドサービスを使い顧客向けのサービスを開発する（例：プライベートクラウドを使った電子申請サービス）。利用者は、顧客に利用規約を提示する。

SIerがクラウドサービス契約者



- 利用者は、クラウドサービス利用を前提としてSIerを調達する。要件には利用者のセキュリティポリシーに準拠することが含まれる（例：パブリッククラウドを利用した電子申請サービス）。
- SIerは要件に適合したクラウドサービスを選定しサービス全体を構築する。クラウドのみでセキュリティポリシーが満たされない場合は、その部分を独自構築する（例：データの保存場所をオンプレに作る等）。
- SIerは、クラウド事業者と契約し、利用規約等の変更について監視を怠らないようにする。

利用者、顧客がクラウドサービス契約者



- 利用者は、クラウドサービスの利用規約に同意し、法人アカウントを開設する（約款による利用）。利用者は、利用規約がセキュリティポリシーに合致するか確認したのち利用する。
- 顧客は、クラウドサービスの利用規約に同意し、個人アカウントを開設する（約款による利用）。
- 利用者は、クラウドサービスを利用して、サービスを顧客に提供する（例：メールマガジン配信、チャットによる問合せ対応）。
- 利用者は、クラウドサービスの利用規約の変更を監視し、セキュリティポリシーに合致しなくなった場合は、利用を停止する。

3.2. クラウド事業者における「責任共有モデル」

クラウドサービスを活用する際、「責任共有モデル(Shared Responsibility Model)」の理解が大前提となります。これは、利用者とクラウド事業者が、責任分界点を定めるだけではなく、運用責任を共有し合っているという考え方です。図 2 は基本的な責任共有モデルの考え方ですが、各クラウド事業者やサービスによって責任共有モデルの考え方が異なる場合があります。

しかし、どのようなクラウドサービスでも、組織としての活用の目的や指針、設定や接続する端末の安全性の確保、さらには管理する(又は生み出される)データなどの取扱は、概ね利用者側の責任です。また、先に述べたとおりクラウドサービスの活用に当たっては多数のステークホルダーが存在し、一般的に利用者側に責任がある領域も外部へ委託している場合や外部からの支援を受けている場合があります[6]。そのため、責任共有モデルは構築者や設置者などのステークホルダーを踏まえた上で理解する必要があります。

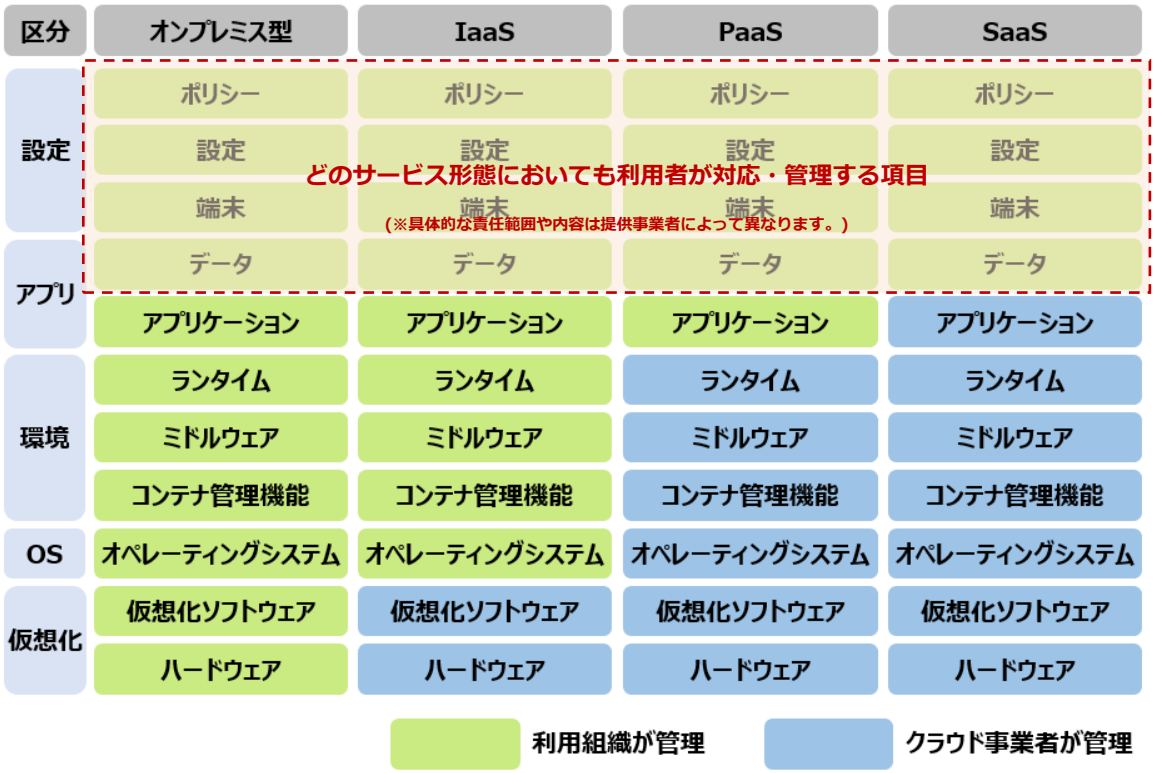


図 2 クラウドサービスの責任共有モデル(例)

[6] 近年のクラウドサービスでは、マネージド・サービスという運用を自動化するサービスが広がってきていますが、運用の責任は利用者側にあることを認識する必要があります。

コラム：クラウドサービスの類型

クラウドの基礎概念解説のため、サービスの分布や責任共有モデルを IaaS、PaaS、SaaS の類型で示しましたが、多くの組織では単一の類型でクラウドサービスを利用することは非常に稀です。IT のサービスは様々な要素の組み合わせであり、例えばデータベースは PaaS、Web サーバは IaaS、認証の仕組みは SaaS、といったように外から見たら一つのサービスでも、中身は複数の要素が組み合わさっており、サービスのニーズに合わせてこうした組合せを行う”設計”が重要となります。また、場合によっては複数のクラウドサービスを連携させて自社のサービスとして組み込むことも一般的です。

クラウド事業者によっては設計のデザインパターンや設計原則などの資料を公開しており、ベストプラクティスを学ぶことでより良いサービスを使うことができます。

複数社のクラウドサービスを組み合わせた構成を SIer が構築する場合などにおいても、利用者は利用サービスに関連する事業者ごとに責任範囲の明確化と理解が求められます。

クラウドサービスを安全に利用していくためには、責任範囲を区別する責任分界点の明確化、インシデント発生時の対応等をあらかじめ検討する必要があります。こうした背景を踏まえ、米国 NSA[7]は 2020 年 1 月にクラウドサービスの脅威・脆弱性と責任共有モデルを示し、「設定」「アプリケーション/データ」「環境」「オペレーティングシステム」「仮想化」といた大枠の区分で表記をしています。しかし昨今、クラウドサービスはより複雑な構造となっており、各クラウドサービスの領域そのものも不明瞭にもなってきています。

図 2 のとおり、クラウドサービスを利用する場合においても、オンプレミス型同様に様々な運用や管理が求められており、ここでは「ポリシー」「設定」「端末」「データ」の４つに細分化して、利用者側の必要な対応について概説します。

まず、それぞれの組織には、粒度や量は異なっても組織の指針やルールなどが存在します。それらの現存する指針やルール(顧客サービスの方針やセキュリティポリシー等)と照らし合わせた上で、組織としてクラウドサービスをどのように構築し、活用するのか、組織としての「ポリシー(組織的な指針)」は事前に確認、検討を行い、(状況によっては)変更し、見直しをしながら運用します。またそのポリシーを踏まえた上で、システム自体のポリシー(製品やサービスの基本となる指針)も決定、設定し、運用し続ける必要があります。

また、利用者の責任範囲として、セキュリティの基本となるアクセス管理やアカウント管理、システムの詳細設定など、活用する上でのシステム上の「設定」も欠かすことができません。この設定をシステム活用当時から対応しておかないと、いわゆる「設定不備」によるインシデントが発生します(クラウド事業者の仕様変更があった場合も同様です。)。なお、クラウド事業者は、導入や運用の様々な段階においても、情報の非対称性を深く考慮し、利用者だけではなく、販売者・構築者・設置者・運用者に対して、設定に関する情報を丁寧に開示し、説明する必要があります。

さらに、クラウドサービスに接続する端末のマルウェア感染などのインシデントが発生しないように、又はシステム側に波及しないように、アクセスする端末のセキュリティ対策も行う必要があります。なお、テレワークを実施している組織においては、物理的な端末の盗難等のリスクも含め、テレワーク未実施の組織よりも厳格なセキュリティ上の配慮が必要です。

組織に元々あるデータやシステムによって生み出されたデータは、保管場所としてはクラウド事業者側にありますが、データそのものは保有者の情報資産であり、運用や活用の責任は保有者(≒利用者)にあります。昨今、バックアップの重要性が高まっており、重要な情報資産であればあるほど、マルチクラウドやオフラインでのバックアップなどを検討し、事業継続のためのデータ管理を考える必要があります。その一方で、クラウド事業者においては、利用者が設定、運

[7] アメリカ国家安全保障局(National Security Agency)

用しているデータに対するアクセスコントロールや権限、手段、機能等が変わることのないように考慮した上で仕様変更を行い、データを安心・安全に活用できる環境整備を行います。もし、クラウド事業者による仕様変更によって、データや利用者全体に悪影響が及ぼすことが判明した場合は、即座に応急処置や緩和策などの提示を行い、利用者に対応を促す必要があります。

3.3. 責任共有モデルを踏まえた販売者、構築者、設置者、運用者の責任と役割

特に我が国の場合は、クラウド事業者と利用者の間に様々なステークホルダーが存在します。また「責任共有モデル」の箇所で述べたようなポリシーからデータまでの領域についても、利用者の管理領域であったとしても利用者だけで対応が完結せず、それぞれのステークホルダーからの支援を受けている場合があります。そのため、再委託先や再々委託先などを含めた全てのステークホルダーを把握し、普段の業務やインシデント時の業務、責任範囲などについて、事前及び継続的に協議を行い、組織間の運用の落とし穴にならないよう、体制を整えておく必要があります。例えば、特に重要なシステムについては再委託や再々委託を認めないようにするなど、ステークホルダーをあらかじめ限定的にしておくことも、利用者としては検討する必要があります。

また、クラウド事業者としては IaaS や PaaS のサービスを販売者や構築者などに提供し、その組織が SaaS として利用者にクラウドサービスを提供している場合があります。この場合は特にクラウド事業者や販売者、構築者などにおいても事前の協議を行い、クラウドサービスを提供する事業者として対応や責任の範囲の明確化を行い、インシデント発生時には円滑に対応できる体制の確保が必要です。利用者は活用するクラウドサービスの構造について理解に努めることが大切です。

さらに、クラウド事業者のデータセンターが海外にある場合などは、上記のステークホルダーの責任と役割だけでなく、当該国の法令や政府機関の対応等にも細心の注意を払う必要があります。

3.4. ステークホルダーとの契約形態等の理解

クラウドサービスを利用するに当たって、ステークホルダーによって契約の形態、締結対象、組織数なども異なります。

例えば、IaaS を提供しているクラウド事業者のサービスを用いて、構築者が SaaS を構築し、販売者が対象の SaaS を販売しているとします。この場合、クラウド事業者と構築者はクラウドサービス利用のために契約を締結し、構築者は販売者との販売店としての契約を締結し、販売者と利用者は購入や利用に関する契約を締結しています。

表面上、利用者は販売者としか契約を締結していないように見えるかもしれませんが、当該契約が、販売者と構築者及び構築者とクラウド事業者のそれぞれの契約を踏まえた内容になって

いる場合や、利用者が、構築者又はクラウド事業者との間にて別途契約を締結することが前提条件になっている場合、クラウド事業者が公表している約款等への同意が必要とされている場合などがあります。そのため、どの組織とどのような契約を締結していることになるのか、販売者以外の組織とはどのような関係が構築されるのかといった契約状況を把握する必要があります。なお、契約は利用者、事業者ともに対等な立場で同意のもと締結されるものです。利用者は、自組織が一方的に不利な契約内容とならないよう、十分に留意する必要があります。クラウド事業者においても、サービス利用約款や利用規約の策定や更新の際、利用者に不利な内容にならないようにしなければなりません。

契約時に特に確認すべきポイントは、平常時の支援内容、インシデント発生時の支援内容、データの取扱（バックアップや破棄などを含む。）に関する内容、そして損害賠償などに関する内容です。クラウドサービスを使うということは、自組織だけでリスク管理や対応が行えるわけではありません。インシデントが発生した時点で利用者が契約内容や約款を見直しても遅いため、必ず契約時に確認をしなければなりません。また、クラウド事業者の約款変更は定期又は不定期に更新されるため、継続的な確認体制も欠かすことができません。

なお、2020 年に施行された改正民法の規定を踏まえ、利用者はまずクラウド事業者と行う取引が「定型取引」に該当するものなのかを確認し、サービス利用約款や利用規約等に定型約款の規定が適用されるのか否かを確認する必要があります。いずれの契約形態であっても、契約締結後、利用約款等の変更が利用者にとって利益になる場合も、不利益になる場合もあります。想定される事態に適切に対処するために契約内容について法務部門等と相談していただくことが望まれます。

クラウド事業者においても、提供するクラウドサービスが不特定多数との取引を目的とした定型取引としての性質を有するのであれば、サービス利用約款が定型約款に該当する可能性があることを忘れてはなりません。

コラム：契約の類型について

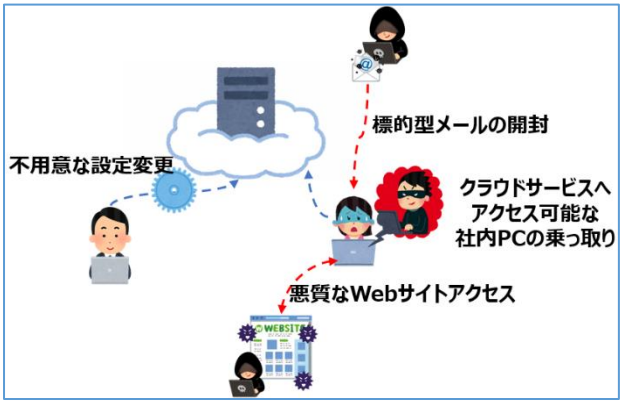
クラウドサービスを利用する際の契約形態は、多数の利用者と同一内容の契約を結ぶことが多いため、利用規約、利用条件、利用契約等の取引条件を記載した文書(以下「利用規約[8]」という。)が用意されていることがほとんどです。利用規約にはクラウドサービスの形態によって民法上の定型約款に該当するものと該当しないものとがあります。定型約款に該当する場合は不当条項規制や変更手続の規定が適用されますが、定型約款に該当しない場合は利用規約が契約に組み入れられているかどうかによって異なります。

また、クラウドサービスは手軽に利用できるものも多く、利用規約の内容について利用者が把握していないケースも見受けられますが、サービスの利用を開始したり、支払いの登録をしたりした段階で利用者は利用規約に同意したと認められる場合があります。

トラブルが発生した際のクラウド事業者とのやりとりには利用規約が土俵となります。クラウドサービスの利用の際には情報システム部門だけでなく、法務部門とも連携して内容について理解するようにしましょう。

コラム：サイバー攻撃の侵入口

セキュリティ対策が強固なクラウドサービスを実現しても、利用者の操作(設定、メール開封、Web サイト訪問など)次第では攻撃者が侵入できる可能性が高まります。特に設定については、既定の設定がどのような動作なのか、といった観点も踏まえて設計を行う必要があります。メール開封や Web サイト訪問については、無害化するソリューションの活用が対策例として考えられます。



サイバー攻撃を可能にしてしまう例

[8] 利用規約には、以下の合意書やポリシーが含まれる場合があります。
- 「クラウドサービスレベル合意書 (Cloud SLA)」
- 「利用ポリシー (Acceptable User Policy)」
- 「セキュリティポリシー (Security Policy)」
- 「データ保護ポリシー (Data Protection Policy)」
- 「事業継続ポリシー (Business Continuity Policy)」
- 「アップグレードポリシー (Upgrade Policy)」
- 「終了ポリシー (Termination Policy)」

4. クラウド利用(環境構築、運用など)の注意点

クラウドサービスをはじめ様々な環境や技術の活用はあくまでも手段の 1 つに過ぎないため、まずは組織としてクラウドサービスをなぜ利用するのか、目標や目的、情報技術を活用する理由を明確にします。その上で最もふさわしいクラウドサービスを選定します。

4.1. 構築時の注意点

＜選定・設計＞

4.1.1. どのような形式のクラウドサービスを活用するのか

まず利用者は、自組織の現状把握が欠かせません。特に既存のシステムや環境が、構築者や設置者などへ依存している場合は、支援を受けている構築者や設置者などと協議を行い、クラウドサービスを活用できる現状であるのか、移行するためにはどのような作業が生じるのかなど、自組織で現状を把握しなければなりません。その上で、自組織に合ったクラウドサービスはどのような形式のものであるか、IaaS・PaaS・SaaS に代表されるような様々なカテゴリの中から構築の仕方を検討していきます。

4.1.2. どのクラウド事業者・サービスを選定するのか

クラウド事業者の選定に当たっては、大きく 3 つのポイントがあります。

共存・共栄できる事業者

まずは、クラウドサービスを提供する事業者として適切な管理体制があるのか、関連する認証を取得しているのか、利用実績数や事例、品質に対する考え方など、クラウド事業者そのものの信頼性の確認です。具体的には、有事の際のインシデント対応において共に連携できること、利用者がクラウドを活用して提供するサービスの重要度に応じてクラウド事業者側のログデータ(ログの種類、保存期間など)等のインシデント対応に必要な情報を即座に提供できること、その情報の入手フローの確認を含め、想定外のインシデントでも問題解決のための提案ができること等、クラウド事業者のサポート方針やサポートレベルを見極める必要があります。

クラウドサービスの信頼性

2 つ目は、サービスの稼働率やこれまでの障害の発生状況、クラウドサービスのセキュリティ対策、データの保管やバックアップの体制など、サービスそのものの信頼性の確認です。SaaS の機密性やデータ安全に関して、ISMAP(日本)や FedRAMP(米国)といった認定制度があり、選定の際の参考となります。

情報開示方針

3 つ目は情報開示の明瞭性です。規約や約款などの契約面における適切な記載はもちろんのこと、サービス自体やそのサポート内容の公開方法や公開項目、そして障害発生時の情報開示の方法や体制など、目に見える形でクラウド事業者が情報公開に努めている様子があるのかなどを確認します。なお、総務省においては利用者向けのクラウドサービスの比較・評価・選択等を目的とした「クラウドサービスの安全・信頼性に係る情報開示指針」を公表

しています[9]。

4.1.3. 既存の方針や規程のままで対応が可能か

クラウドサービス利用に当たって、組織が運用している方針や規程(セキュリティポリシー等)と抵触が生じないかを確認します。例えば、これまで組織で定義している「重要な情報については外部に持ち出したり保存したりしてはならない。」といったポリシーを運用している組織で、クラウドサービスを活用して、外部で重要な情報についても保管や保存ができるようにする場合、既存の方針や規程に抵触している場合があります。そのため、方針や規程を確認し、クラウドサービス活用に当たって、抵触が生じないか確認します。

＜実装＞

4.1.4. 選定したクラウドサービスの理解を深める

実装に向けて注意すべきことは、サービスの概要を理解することはもちろんのこと、設定の不備によるインシデントが起きないように設定方法の理解を深めることや、そもそもの設計思想を理解することも大切です。特にシステム的な視点だけではなく、利用者が守らなければならないデータがより安全な状態を維持するためにはどのようにしたらよいのか、クラウドサービスを提供している事業者はどのように考えているのかを確認し、理解を深めます。クラウド事業者が構築や運用に関するガイドを提供している場合は、対象の文書に目を通し、加えてクラウドサービスのサポート情報やFAQなどを確認しましょう。また、それでも不明な点がある場合は、直接サポート窓口に確認することも大切です。

なお、自組織ではなく外部への委託や支援を受けて実装を考えている場合は、この設計思想などのクラウドサービスを実装する初期段階から共に理解を深めることが望ましいです。

クラウドシステムの急速な広まりから、組織内の基幹システム等にも幅広くクラウドサービスを活用する利用者が増加しています。組織におけるクラウドシステムへの依存度の高まりに伴い、クラウドサービスの障害は事業継続や可用性の観点から、組織に与える影響は大規模化しています。3.2.でもデータ面について述べたとおり、重要な情報資産であればあるほど、マルチクラウドやオフラインでのバックアップなどを検討し、事業継続を見据えた設計及び実装をする必要があります。

4.1.5. 実装は誰が行うのかを明確にする(構築者・設置者・運用者など)

全ての設定や実装作業を利用者のみで行えるケースは少なく、SIer やコンサルティング企業などの外部支援を受けて実装している組織が多いのが現状です。忘れてはならないのはクラウドサービスの利用主体は利用者にあり、根本的な実装責任は(クラウド事業者側の仕様変更などを除いて)利用者にあることです。外部の支援を受けることは決して悪くはないですが、利用者が自ら具体的な実装は行わないような場合でも、より主体的に実装に携わ

[9] 総務省「クラウドサービスの安全・信頼性に係る情報開示指針」
https://www.soumu.go.jp/main_content/000475596.pdf

らなければならないということです。その上で、構築者や設置者などはクラウド事業者から取得している情報を開示し、インシデントが起きにくく、利用しやすい環境の構築に努める必要があります。ステークホルダーの対応範囲を明確にし、実装における不備を抑制するためにも、役割分担を明確にしておく必要があります。

＜検証＞

4.1.6. ポリシーや設定など、適切な構築や設定が行えているのか

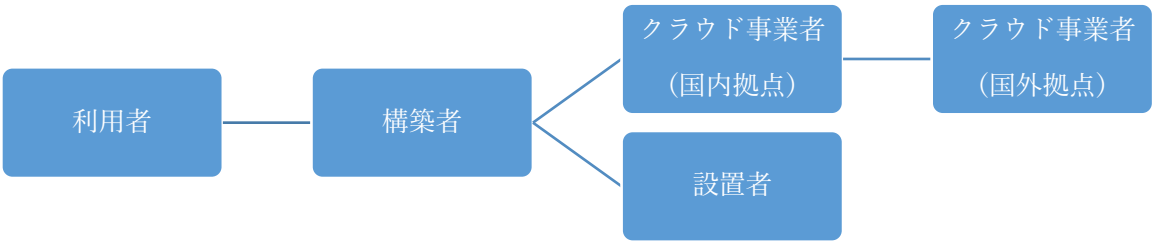
利用者が主体となり、構築者や設置者が実装した環境が、クラウド事業者が提供している情報に基づき適切に構築できているのかどうかを検証します。利用できる状況になったら直ちに利用を開始するのではなく、オンプレミス型のシステム同様に検証のプロセスを忘れてはなりません。できる限り第三者に依頼し、安全に設定できているのかどうか、設定不備や脆弱性に係る診断、ペネトレーションテストなどの実施により、インシデントが発生しない状況にあるのかどうかを確認します。なお、先にも述べたとおり、クラウドサービスは定期的にクラウド事業者側での仕様変更が行われています。そのため、このような検証は運用段階になっても定期的に実施するのが望ましいです。

4.2. 運用時の注意点

4.2.1. 体制

これまで述べてきたとおり、クラウドサービスを活用するからといって、利用者のシステム運用がなくなるわけではありません。クラウドサービスを活用して事業やサービスを展開していれば、その責任は利用者にあります。また前述のとおり、責任共有モデルを理解した上で、自組織の対応範囲を確認し、特に双方に責任がある領域においては、協議を行い、対応を事前に確認し、体制を確立しておく必要があります。利用者とクラウド事業者だけではステークホルダーは完結せず、構築者や設置者、運用者などがそれぞれいる場合や、さらにはクラウド事業者側の対応として、国外の拠点が対応に関係する場合もあります。このため、ステークホルダーを含めた体制の構築が必要です。

【代表的なステークホルダーの例示】



運用体制の確保は、まずは相談や連絡が可能な窓口を把握することから始まります。

そして、クラウドサービスを含むシステム運用に関する責任者を任命します。これはインシデントが発生したときに対象のサービスやシステムを利用停止する判断を行ったり、重

要な更新などが生じた場合に判断を行ったりするための指揮系統を明確にするためです。その上で、実際の作業や指示を行う担当者を任命します。主に利用者のステークホルダーとの連携や、確認した情報の展開や具体的な作業の現場監督のような役割を担います。

さらに、これまで述べてきたとおり、クラウドサービスは事業者側の仕様や約款などの変更が利用者側の変更のタイミングと合わせて行われるわけではなく、定期又は不定期に更新されます。また、昨今クラウドサービス上でのインシデントも発生していることから、脅威情報や脆弱性情報など、クラウドサービスに関連する情報を収集し、展開する担当者を任命しておくと、より安全な活用が可能です。

上記それぞれに責任者や担当者を任命することが難しい場合は、兼任であったとしても組織としての任命をする必要があります。

4.2.2. 対応

クラウドサービスに関する対応として、平常時とインシデント発生時の 2 つに分けて解説します(インシデント発生時については「6.インシデント発生時のステークホルダー連携の在り方」で後述。)。

平常時においては、システムやサービスの設定が適切に行われているか、クラウド事業者が公開しているガイドなどを参照し、見直しを行います。また新しいバージョンの公開やサービスの更新が行われた場合には、変更点や影響の確認を行います。不明な点は契約を行っている運用者やクラウド事業者などに確認を行います。また組織が活用しているシステムやサービスに影響がある脅威情報や脆弱性情報が公開されていないかを確認します。一方で、運用者やクラウド事業者も情報提供を積極的に行い、利用者の確認に対して真摯に対応します。

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

5.1. 普段からのコミュニケーションの方法や注意点

クラウドサービスを利用するに当たっては、①利用者と運用者、②運用者とクラウド事業者、③クラウド事業者と利用者の間では、定期的に協議を行い、窓口・連絡先の把握や信頼関係の構築に努める必要があります。

特にコミュニケーションが大切なタイミングは、クラウド事業者側の仕様や約款の変更が行われたときです。クラウド事業者は、利用者に対して、(エグゼクティブサマリをまとめるなど)分かりやすく情報提供し、また運用者や構築者、設置者に対してはより具体的に情報(ガイドやFAQ など)を提供し、変更に対する説明責任を果たす必要があります。以下に、ステークホルダーのコミュニケーションの例について記します。

5.1.1. 利用者と運用者(又は構築者や設置者)

運用者はクラウド事業者から取得した情報を基に、取得情報そのものの提供や提供するサービスの更新予定・内容などについて利用者と協議します。サービスを更新する場合は、更新理由や更新によって変更する点、機能追加等がある場合は、追加機能、利用時の注意点や設定方法の確認を双方で行います。また運用者は利用者に対してサービス更新時の影響を説明し、利用者はその影響を踏まえた上で、組織への影響を考え、更新や設定を行うか検討する必要があります。なお、協議した内容や資料については議事録を残し、少なくともサービスを利用している間は保管し続けるようにしましょう。

5.1.2. 運用者(又は構築者や設置者)とクラウド事業者

運用者はクラウド事業者から提供されている情報を注視しておきます。クラウド事業者も積極的に運用者に対して情報を開示し、また開示されている情報も国内外で差異が生じないように情報の提供に努める必要があります。クラウド事業者が提供する重要な情報については、一般公開される前に運用者が情報を取得できるような体制や関係性を構築しておく必要があります。また技術的な側面だけではなく、約款などの法律的な側面においても確認、協議することを忘れてはなりません。5.1.1 と同様に協議内容は保管し続けるようにしましょう。

5.1.3. クラウド事業者と利用者

クラウド事業者は運用者に提供している情報と同等の情報を利用者に提供できるように努める必要があることに加え、情報の非対称性があることを理解した上で、より分かりやすく利用者に伝える必要があります。またクラウド事業者と利用者の間においても、できる限り定期的に協議を行うよう努める必要があります。利用者も、自らが活用しているクラウドサービスについては、定期的に更新情報の収集に努める必要があります。特に利用者は、確認したサポート情報や約款などは、サービスを利用している間は保管し、適切に振り返りが行えるようにしましょう。

5.2. インシデント発生を想定した準備

クラウドサービス活用に限らず、利用者はインシデントを想定し、備える必要があります。発生しうる代表的なインシデントは、「システムやサービスの脆弱性を狙った攻撃」、「OSINT 等を活用した攻撃」、「装置故障などによるシステム障害」、「クラウドサービスの故障」、そして「設定の不備」が挙げられます。先にも述べたとおり、クラウド事業者や構築者、運用者等のインシデントであったとしても、組織が提供している事業やサービスそのものにインシデントが波及した場合は、顧客に被害や迷惑が生じ、組織としての責任が問われる可能性があります。

まず、利用者や構築者などは、過去にクラウド事業者(できればクラウド事業者の競合企業を含め)に発生したインシデントを確認します。新しいインシデント発生は誰にも予測できませんが、できる限り「想定内のインシデント」とするように努め、事前に対応や対策を練ることが大切です。

また利用者は、クラウド事業者や運用者などが提供しているサポート(保守・運用)契約について確認し、追加費用などのオプションサービスについてもあらかじめ確認をしておく必要があります。構築者や運用者、そしてクラウド事業者も限られた資源の中でサービスを提供しており、有償の契約であれば 24 時間 365 日のサポートが受けることができる契約や、SLA(Service Level Agreement)や SLO(Service Level Objective)がより明確になったサポート、オンサイト(訪問対応が可能な)サポートなどの契約を準備している場合があります。特に重要なシステムにおいてクラウドサービスを活用する場合は、事前に経営層を含めて当該サポート契約の締結について協議し、クラウド事業者や運用者と契約を行うことが望ましいでしょう。

さらにインシデントが発生すると、利用者や運用者、構築者などは、原因究明に努める必要があります。組織でインシデント対応が行えるように、あらかじめクラウド事業者が提供可能なログやその内容について確認しておくとよいでしょう。例えば、ログの種類や、どれくらいの期間のログが提供可能なのか、またそもそも提供に当たって費用がかかるのか、分析や対応のための教育があるのかなどです。これらの対応は費用に関係するため、クラウドサービスを検討している段階で確認する必要があります。

最後に基本的な内容ですが、どこに問い合わせればいいのか、連絡先を事前に把握し、組織内に共有をしておく必要があります。なお、インシデント発生時にどこの組織に調査や解析などをお願いするのか、事前に見当をつけておくことも大切です。

クラウドサービスは提供しているクラウド事業者がよりサービスを理解しており、「クラウド事業者＞構築者・設置者・運用者＞販売者>利用者」の情報の非対称性があります。そこでインシデント発生時にはエグゼクティブサマリなどの分かりやすい情報提供ができる体制の整備に努め、我が国のシステムや事業がより安心・安全に利用できるように努める必要があります。

コラム：SLA

SLA(Service Level Agreement)とはクラウドサービスの品質に関する合意内容で、クラウド事業者と利用者との契約に含まれる内容となります。SLA の内容は情報漏えい等の法的リスク、損害賠償の内容と関連する契約条項といえますので、情報システム部門だけでなく法務部門とも連携して検討することが望ましいと言えます。

SLA は多くのクラウドサービスでサービス稼働率として表記されます。利用者は SLA に基づき、サービスの停止時間を想定し、許容することとなります。

SLA における許容停止時間の一覧表

SLA	停止時間(週)	停止時間(月)	停止時間(年)
99%	1.68 時間	7.2 時間	3.65 日
99.9%	10.1 分	43.2 分	8.76 時間
99.95%	5 分	21.6 分	4.38 時間
99.99%	1 分	4.32 分	52.56 分
99.999%	6 秒	25.9 秒	5.26 分

稼働率を例示しましたが、クラウドサービスによって SLA の内容は様々です。特定のシステム要件を満たすことを SLA の前提条件とする場合もあります。使用を検討しているクラウドサービスごとに SLA の詳細を確認することが必要です。

コラム：外部認証制度、評価制度

情報セキュリティマネジメントシステム(ISMS)は組織の情報資産のセキュリティ管理体制で、ISO/IEC 27001 として標準化されておりますが、クラウドサービスに対応した情報セキュリティ管理体制は、ISO/IEC 27017 として規格標準化されています。

クラウド事業者は ISO/IEC 27001 と ISO/IEC 27017 の両方の認証を取得し、クラウドサービスセキュリティへの取組を対外的にアピールしています。

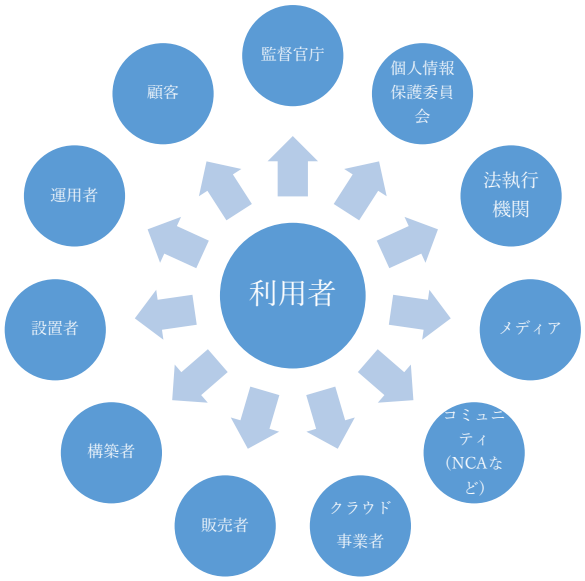
また日本政府では、令和 2 年 6 月に「政府情報システムのためのセキュリティ評価制度」(ISMAP)を立ち上げ、国際基準等を踏まえ策定したセキュリティ基準に基づき、クラウドサービスを第三者が評価を行い、クラウドサービスの調達に活用しています。

米国においても「クラウドサービスに関するセキュリティ評価・認証の統一ガイドライン」(FedRAMP)を採用し、米国政府の導入するクラウドサービスの採用に役立てています。

しかし、これらはあくまでセキュリティ管理体制、セキュリティ対策の実装状況評価等を行っているものであり、利用者はセキュリティインシデントへの対応体制を整備する必要があります。

6. インシデント発生時のステークホルダー連携の在り方

インシデント発生後は、先のステークホルダーに加えて、監督官庁や法執行機関、(個人情報の漏えい・滅失・毀損に関する場合は)個人情報保護委員会などとの連携が加わります。また、メディアからの問合せや法的解釈が求められる場合に備え、広報や法務に関係する部門や担当者とも連携を行います。そのため、先に述べたクラウド事業者や運用者などの窓口把握だけではなく、自組織の広報や法務に関係する窓口についても事前に把握し、いつでも連携できる体制を整備します。さらに、自組織やシステムの関係者だけではなく、国内外の研究者や技術者から連絡を受けることにより、インシデントが発見される場合があります。状況によってはこのようなステークホルダーとの連携が追加されることも認識しておくことが大切です。



また、複雑化、巧妙化するサイバー攻撃や、クラウドサービスの活用が進んでいる現状において、インシデントが発生したときに、一組織だけで対応するのは難しいのが現実です。そこで日本シーサート協議会(NCA)などのコミュニティに、利用者だけではなく、販売者、構築者、設置者、運用者、そしてクラウド事業者も含め参画し、ステークホルダーが連携しやすい体制の確保を行います。そこでは、他組織でのインシデント発生状況や自組織のインシデント情報の共有などを行い、協力してインシデントの解決に取り組む必要があります。

以下に、インシデントが発生したときの対応概要について記します。

＜サイバー攻撃の場合＞

- 影響範囲に応じて、システムの停止を検討します。
- クラウド事業者からログの取得を行い、利用者や運用者又は他の調査機関で分析を行います。
- 個人情報の漏えい・滅失・毀損に関する場合は、速やかに監督官庁や個人情報保護委員会に報告を行います[10]。

＜脆弱性や設定不備の場合＞

上記、サイバー攻撃の場合に加えて、以下のようなポイントを追加して検討、対応します。

- クラウド事業者のサポート(サービス)情報を確認し、最新の情報を確認します。
- クラウド事業者からガイドやFAQなどが公開されている場合は、参照します。
- 特にゼロデイ攻撃の場合、緩和策や回避策があるか確認し、公開されている場合は、組織内で対応を実施するか検討します。
- 新たなモジュールやパッチが公開されたら、できる限り速やかに適用や更新を行います。

上記のように、インシデントがどのようなインシデントなのか、発生の早い段階で、状況や性質などが理解できればよいですが、クラウド事業者や運用者などステークホルダーから情報開示や共有が行われていない場合、利用者はインシデント対応が難しくなる場合があります。そのため、情報共有や連携を行うコミュニティの活用は欠かすことができず、社会全体でインシデントの早期解決に努める必要があります。

[10] 個人情報の保護に関する法律（個人情報保護法）については、2022年4月1日から改正法が施行されます。当該施行後、個人情報取扱事業者、国の行政機関及び独立行政法人等においては、個人の権利利益を害するおそれが大きい個人データの漏えい等事態（サイバー攻撃を受けた場合等も想定しつつ、不正の目的をもって行われたおそれがある個人データの漏えい等事案等、対象となる事態を個人情報保護委員会規則や「個人情報の保護に関する法律についてのガイドライン（通則編）」等で規定）について、個人情報保護委員会等への報告（同委員会から事業所管大臣に委任されている個人情報取扱事業者に関する報告の受理権限に基づき、当該大臣に報告する場合も含む）及び本人への通知を行う必要があります。なお、地方公共団体の機関及び地方独立行政法人については、改正法が別に施行予定の2023年春頃より個人情報保護委員会への報告及び本人への通知が必要になります。

＜情報が不足している、又はインシデントの特定ができない場合＞

- ステークホルダーは、日本シーサート協議会(NCA)などのインシデントの事前・発生時・事後の連携が行えるコミュニティに参画します。また、クラウド事業者もコミュニティに参画し、事前又はインシデント発生時には、より積極的に情報提供や連携を行うなど、コミュニティを活用します。
- 情報共有ルール(チャタムハウスルールやTLP(Traffic Light Protocol)など)を理解し、ルールに則って、情報を共有します。
- 情報が共有されたコミュニティでは、加盟している組織のインシデント発生状況を確認します。
- 複数の組織で同様の、又は類似したインシデントが発生している場合は、コミュニティと事業者との契約の有無に関わらず、クラウド事業者の窓口に通報や相談を行います。
- クラウド事業者は当該通報や相談に対し、現状把握、調査、回答を行います。
- クラウド事業者も国内外で差が生じることのないよう情報を提供し、インシデント対応が完了するまで支援を続けます。
- 特にコミュニティに対しては、利用者に限らずクラウド事業者も積極的に情報共有や連携を行う必要があります。
- また影響範囲を鑑みて、コミュニティは国家サイバー統括室などの政府機関に共有を行い、官民連携して問題の解決に当たります。
- インシデント対応が完了後、官(関係省庁)、民(コミュニティ(利用者・運用者など)、クラウド事業者)の関係者が参集し、振り返りや勉強会を実施することが望ましいです。

自組織で発生したインシデントを共有することに抵抗感のある組織も多いですが、インシデントは、早期の共有が、早期の解決をもたらします。特に原因の特定ができないインシデントや、ステークホルダーでの対応者が不明瞭になる「狭間のインシデント」は、共有が遅くなればなるほど解決が遠くなります。インシデントの発生は決して恥ずかしいことではなく、早期に共有し合わなければ解決できない時代に突入していることを、(特に経営者が)理解する必要があります。

特に、想定外のインシデントが発生した際に、リスク情報の提供などがステークホルダーにおいて必要なときには、クラウド事業者は秘密保持に配慮しつつ、事業遂行に係る社会的責任を踏まえた対応として、利用者とその顧客に情報の提供や連携を行う必要があります。

コラム：2022 年 4 月 1 日から施行される個人情報保護法

個人情報の保護に関する法律(個人情報保護法)について、民間分野における個人情報を取り扱う事業者(個人情報取扱事業者)に関する改正が 2020 年 6 月に成立・公布され、2022 年 4 月 1 日から全面施行されます[11]。これに合わせ、「個人情報の保護に関する法律についてのガイドライン(通則編)」及びその Q&A の改正等が行われており、個人情報取扱事業者がクラウドサービスを利用する場合に留意すべき点として以下の 2 点があります。

1 点目は、利用者である個人情報取扱事業者がクラウドサービスを利用する場合であっても、契約条項によってクラウド事業者がそのサーバに保存された個人データを取り扱わない旨が定められており、適切にアクセス制御を行っている等、クラウド事業者がサーバに保存された個人データを取り扱わないこととなっている場合には、クラウド事業者への個人データの第三者提供や個人データの取扱の委託には該当しない点です。この場合、利用者である個人情報取扱事業者は、個人データに係る本人が被る権利利益の侵害の大きさを考慮し、その個人データの取扱状況(個人データを取り扱う期間、取り扱う個人データの性質及び量を含む。)等に起因するリスクに応じ、自ら果たすべき適切な安全管理措置を講じる必要があります。

2 点目は、以上の場合において、個人データが保存されるサーバが外国にある場合については、利用者である個人情報取扱事業者が外国において個人データを取り扱うこととなるため、基本的には、当該外国の個人情報の保護に関する制度等を把握した上で、安全管理措置を講じる必要がある点です。さらに、個人情報の取扱に関する透明性を通じて本人関与の実効性を確保するため、クラウド事業者が所在する外国の名称及び個人データが保存されるサーバが所在する外国の名称、それら外国の制度等を把握した上で講じた安全管理措置の内容等を本人の知り得る状態(本人の求めに応じて遅滞なく回答する場合を含む。)に置く必要があります。なお、クラウド事業者によっては、個人データが保存されるサーバが所在する国を特定等できない場合があるため、この場合には、サーバが所在する外国の名称に代えて、①サーバが所在する国を特定できない旨及びその理由、及び、②本人に参考となるべき情報として、例えば、サーバが所在する外国の候補が具体的に定まっている場合における当該外国の名称等を本人の知り得る状態に置く必要があります。

以上とは別に、利用者たる個人情報取扱事業者から外国(日本と同等の水準にあると認められる個人情報の保護に関する制度を有する外国として個人情報保護委員会規則で定める EU 及び英国を除く。)に所在するクラウド事業者への個人データの第三者提供や個人データの取扱の委託に該当する場合については、利用者たる個人情報取扱事業者において、クラウド事業者への提供等を認める旨の本人からの事前同意の取得が必要となり、当該取得時に、クラウド事業者が所在する外国の名称、当該外国における個人情報の保護に関する制度、クラウド事業者が講ずる個人情報の保護のための措置その他本人に参考となるべき情報を本人に提供する必要があります。また、クラウド事業者が日本における個人情報取扱事業者が講ずべき措置に相当する措置を継続的に講ずるために必要な体制を整備している

[11] これに加えて、デジタル社会の形成を図るための関係法律の整備に関する法律による個人情報保護法の改正等のうち、国の行政機関及び独立行政法人等に関する部分が 2022 年 4 月 1 日から施行し、地方公共団体の機関及び地方独立行政法人に関する部分が 2023 年春頃に施行予定となっています。これらの機関等がクラウドサービスを利用する場合に留意すべき点については、個人情報保護法のほか、「個人情報の保護に関する法律についてのガイドライン（行政機関等編)」等も参照する必要があります。

場合については、利用者たる個人情報取扱事業者において、本人からの事前同意の取得は不要ですが、クラウド事業者による相当措置の継続的な実施を確保するために必要な措置を講じるとともに、本人の求めに応じて当該措置に関する情報を本人に提供する必要があります。さらに、クラウド事業者への個人データの取扱の委託に該当する場合は、委託先となるクラウド事業者に対する必要かつ適切な監督を行う必要もあります。

諸外国においても EU の一般データ保護規則(GDPR)、カリフォルニア州消費者プライバシー法(CCPA。なお、2023 年 1 月から改正されたカリフォルニアプライバシー権法(CPRA)が適用)など、プライバシー保護規制は拡大しております。国外に拠点をもつ利用者はこれらの法律にも対応しなければなりません。

諸外国におけるプライバシー関連法令

（参考）個人情報保護委員会　https://www.ppc.go.jp/

7. おわりに

本文書はクラウドサービスの基本的な内容や姿勢を明記したものであり、今後このガイダンスは利用者、クラウド事業者などの全てのステークホルダーの連携によって、より一層安全性の確保のために研鑽していくことが大切です。技術や活用方法など様々な変化が生じれば、このガイダンスも継続的に見直していく必要があり、完成に向けた継続的な議論や取組が必要です。

既にクラウドサービスなしでは事業が継続できないほど依存している組織も多く、これからの時代はクラウドサービスの活用は欠かせません。このような時代であるからこそ、普段から、そして特にインシデントが発生したときは、コミュニティを含む全てのステークホルダーが健全に連携し合う必要があります。クラウドサービスのステークホルダー連携こそが我が国のサイバー空間の安全に貢献できると言っても過言ではありません。

「Cybersecurity for All」、誰も取り残すことなく、全てのステークホルダーがクラウドサービスの理解に努める一方で、情報の非対称性を理解した上でそれぞれが説明責任を果たし、誰もが安心・安全にクラウドサービスを活用できる社会を実現していくよう努める必要があります。

8. 用語集

クラウドコンピューティング

利用者がサーバやストレージ等のリソースを物理的、仮想的に共用し、インターネットを介してサーバ、アプリケーション等にどこからでも必要に応じて利用可能とするコンピュータ活用方式。実装方式として、パブリッククラウド、プライベートクラウド、ハイブリッドクラウド等がある。

クラウドサービス

クラウドコンピューティングを活用して提供されるサービス。基礎的なサービスモデルとして IaaS/PaaS/SaaS がある。

パブリッククラウド

クラウドサービスの提供方式のひとつ。CPU、ストレージ、メモリ等のコンピュータリソースの利用率を最適化するために、一般ユーザや複数の利用者でリソースを共用して実装されるクラウドコンピューティング方式。

プライベートクラウド

クラウドサービスの提供方式のひとつ。クラウド事業者が 1 つの組織に対してクラウドサービスを提供するものであり、当該組織外のユーザは利用することができない、その組織専用に実装されるクラウドコンピューティング方式。

ハイブリッドクラウド

パブリッククラウド、プライベートクラウド等、複数の提供方式を組み合わせて実装されるクラウドコンピューティング方式。パブリッククラウドで Web サービスを構成し、認証情報はプライベートクラウドに保管して Web サービスの認証処理を行うといった例が挙げられる。

マルチクラウド

利用者が複数のクラウドサービスを併用する運用形態。ハイブリッドクラウドが複数のクラウドサービスを組み合わせ、単一のシステムを構築するクラウドコンピューティングの実装方式であるのに対し、マルチクラウドはそれぞれ独立したまま活用する運用の形態。バックアップ・リカバリ体制の構築等で活用されることが多い。

オンプレミス

従来型のシステム構築手法で、自組織の施設内(事務所内や自組織で保有するデータセンター内等)にシステムを設置する方式のこと。

IaaS(Infrastructure as a Service)

クラウドサービスモデルのひとつ。利用者に CPU、ストレージ、メモリ等のコンピュータリソースが提供される。利用者はそのリソース上に OS 等を構築することができる。

PaaS(Platform as a Service)

クラウドサービスモデルのひとつ。IaaS に加えて、OS、基本機能、開発環境等もサービスとして提供される。利用者はそれらを組み合わせて情報システムを構築することができる。

SaaS(Software as a Service)

クラウドサービスモデルのひとつ。PaaS に加えて、利用者に特定のアプリケーション(メールサービスやファイルサービス、グループウェア等)の機能がサービスとして提供されるもの。

SLA(Service Level Agreement)

サービスレベル合意書。クラウド事業者と利用者との合意事項で、クラウド事業者は SLA に含まれるサービスレベル(稼働率や性能等)を満たすことを利用者に保証する。そのため SLA を満たせなかった場合は違約規程として返金規約等がある。

SLO(Service Level Objective)

サービスレベル目標。クラウド事業者が、合意した SLA を履行するために、稼働率、セキュリティ、サポートといった項目ごとに、パフォーマンスの目標値を設定したもの。クラウド事業者が設定する目標値のため SLO には違約規程がなく、SLO の内容について利用者に開示されない場合もある。

TLP(Traffic Light Protocol)

情報共有の促進を目的に作られた、適切な組織または人に共有するための標示。情報共有の範囲を 4 色で示す。

TLP:RED	公開不可、関係者限定
TLP:AMBER	限定公開、関係者が所属する組織内で共有可能
TLP:GREEN	限定公開、コミュニティ内で共有可能
TLP:WHITE	制限なく共有可能

デジタル・トランスフォーメーション

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。

クラウド・バイ・デフォルト

情報システム構築の際に、クラウドサービスの利用を第一候補として、その検討を行うものとする考え。

チャタムハウスルール

会議における情報の公開と共有を促すルール。会議出席者は、発言者を匿名化した上で、会議中に得た情報を自由に使用できる。

「政府情報システムのためのセキュリティ評価制度」(ISMAP)

政府が求めるセキュリティ要求を満たしているクラウドサービスを予め評価・登録することにより、政府のクラウドサービス調達におけるセキュリティ水準の確保を図り、もってクラウドサービスの円滑な導入に資することを目的とした制度。

クラウドサービスに関するセキュリティ評価・認証の統一ガイドライン(FedRAMP)

米国政府におけるクラウドサービスの調達プログラム。米国政府にクラウドサービスを提供するクラウド事業者はFedRAMP準拠を証明する必要がある。

オープン・ソース・インテリジェンス(OSINT)

一般に公開された利用可能な情報をもとにする情報収集の手段。OSINT(オシント)と読む。
インターネット情報をはじめ、インタビュー記事や企業のプレスリリースといった情報等を分析して情報収集する。サイバーセキュリティ分野においても、諜報活動を目的としたサイバー攻撃や、サイバー犯罪捜査、分析といった攻防の両面からOSINTの活用が進んでいる。

本ガイダンス執筆協力一覧(五十音順：敬称略)

アマゾン ウェブ サービス ジャパン合同会社
株式会社エヌ・ティ・ティ・データ
グーグル・クラウド・ジャパン合同会社
クラスメソッド株式会社
グローバルセキュリティエキスパート株式会社
シスコシステムズ合同会社
株式会社セールスフォース・ジャパン
株式会社ディー・エヌ・エー
一般社団法人日本コンピュータセキュリティインシデント対応チーム協議会
日本マイクロソフト株式会社
弁護士　北條　孝佳
楽天グループ株式会社
株式会社ラック
立命館大学 情報理工学部 情報理工学科　教授　上原　哲太郎

以上