エンタープライズクラウド選定ガイド

クラウド選びで困ったら

～要求仕様作成と提案書評価のための基礎知識～

平成 28 年 1 月

JASA-クラウドセキュリティ推進協議会

改版履歴

版	日付	改版内容
Ｖ1.0	2016.1.15	初版発行

はじめに

近年、わが国においてもクラウドコンピューティングサービスの利用が拡大しつつあります。これに伴い、クラウドコンピューティングサービスに伴う情報セキュリティ管理の重要さについても、関心が高まってきました。わが国では、経済産業省が「クラウドコンピューティングサービス利用のための情報セキュリティマネジメントガイドライン」を 2011 年 4 月に公表（2014 年 3 月に改訂）しています。これ以降、このガイドラインはクラウドコンピューティングサービスの利用者や事業者の指針として広く活用されることとなりました。また、このガイドラインに基づき、わが国が ISO 国際標準化を働きかけ、ISO/IEC27017 規格が策定されました。更に、総務省は「クラウドコンピューティングサービス提供における情報セキュリティ対策ガイドライン　～利用者との接点と事業者間連携における実務のポイント～」を平成 26 年 4 月に公表し、より詳細な情報セキュリティ管理について、示している状況です。

これらの規格やガイドラインでは、クラウドコンピューティングサービスの情報セキュリティマネジメントが利用者と事業者の共同責任であり、事業者が適切な情報セキュリティマネジメントを行うと共に、利用者が自ら行う情報セキュリティマネジメントに必要な情報を提供すること、また、利用者がその情報に基づきリスク分析を行い、適切な対応をとることが必要とされています。そして、利用者と事業者が、共にその責任分解点を明確にしたうえで、適切な情報交流に基づき、情報セキュリティを確保することが望まれます。

クラウド事業者は、こうした期待に応えるためサービス提供の際に様々な情報を開示し、利用者の情報セキュリティ対策に資するように努力しています。ただ、クラウドサービスの種類や提供形態などに多様性があるため、それらを統一的に表現することが難しいというのが悩みです。統一的な表現がないため、異なったクラウド事業者の情報において、定義や算出根拠が異なる要素が、似通った表現で行われていることがあります。その結果、異なったクラウド事業者間のクラウドサービスの相互比較が分かりにくくなっているという状況もみられます。

更に、近年、クラウド事業者とクラウド利用者の間に立って、システムの選定や開発・運用を行うクラウドパートナーが大きな役割を持ち始めていることで、クラウド事業者からラウド利用者への情報伝達にもう一つの要素が加わりました。クラウドパートナーはクラウドサービスをより有益なサービスとすることに大きな意義がありますが、クラウド事業者とクラウド利用者の責任分担に、さらにクラウドパートナーが加わることで、情報セキュリティに関する責任の関係がより複雑となってきています。

本ガイドブックでは、これらの状況を踏まえて、クラウドパートナーを含めたクラウドサービスに関わる各主体の責任の範囲を解説した上で、クラウドサービスの仕様に関わる用語概念についての解説を行い、クラウドサービスに関心をもつ人々が正しくサービスを比較し、より適切なサービス利用ができるようすることを目的としています。

目次

第 1 章　クラウドコンピューティングに係わる主体と責任

1　クラウドサービスとクラウドを活用したシステム

(1) クラウドサービスとそのタイプ

クラウドサービスは、SaaS、PaaS、IaaS の 3 つに分けられることが一般的です。

SaaS は、ソフトウェアを提供するサービスです。クラウド利用者は、クラウド事業者が提供するインターフェイスを通じて、ソフトウェアを利用します。具体的には、クラウド利用者が画面から直接データやコマンドを入力することで、必要な処理が実行されます。クラウド利用者は、システムの内容や管理の状況を気にすることなく、情報処理を行うことができます。

PaaS は、プラットフォームを提供するサービスです。プラットフォームは、業務目的等に応じて用意されるもので、Web サービス、OA、EC サイトなどがその代表的な例です。クラウド利用者は、サーバーやネットワークを調達することなしに、目的に応じたシステム利用することができます。例えば Web サービスの場合には、クラウド事業者が提供する Web サーバーを、テンプレートを用いて必要な事項を入力（多くは選択できる）するだけで、簡易にホームページ時を立ち上げ、さらにその運用をクラウド事業者に任せることができます。

IaaS は、コンピューターシステムの基盤を提供するサービスです。クラウド事業者が提供するコンピューターシステム基盤の上に、クラウド利用者がサーバー・ストレージ・ネットワーク等のシステムを設定し運用するものです。サーバー・ストレージ・ネットワーク等のシステム等の機器は仮想化されており、クラウド事業者が用意した様々な種類の仮想機器をクラウド利用者が選択し、組み合わせていくことで、最適なシステムを構築することができます。

図　1.1.1　クラウドのタイプ

SaaS に関しては仮想化技術を用いないサービスもありますが、物理的環境のサービスと対比すると、SaaS は ASP（アプリケーションサービス）サービス、PaaS はホスティングサービス、IaaS はハウジングサービスに類似した論理的環境のサービスと言えるでしょう。

クラウドサービスの分類としては、上記の 3 つに加えて様々なものがあります。例えば、HaaS（Hardware as a Service）はハードウェアを仮想化したものを提供するサービスで、システム環境をクラウド利用者が自ら構築することができるサービスです。クラウドの用語を定義している ISO/IEC17788 では、DSaaS（Data Storage as a Service）というストレージ環境のみを提供するサービスと NaaS（Network as a Service）というネットワークを仮想化して提供するサービスが定義されています。今後、クラウドサービスが発展すると様々なタイプのサービスが出てくる可能性があると考えられます。

本書の目的はクラウドサービスのタイプを説明することではなく、サービスの内容により「クラウド利用者ができること/行うべきこと」と「クラウド事業者が行っていること/行うべきこと」が異なることを示すことにあります。アプリケーションを提供する SaaS のように、クラウド利用者がその背後にあるコンピューターシステム環境を気にすることなく利用できるサービスの場合、クラウド利用者はデータやコマンドの入力に係る部分についての責任を果たせばよく、コンピューターシステム環境のほとんどはクラウド事業者が用意し、適切な管理を行う責任があります。

一方、IaaS のようにコンピューターシステム環境の一部を提供するサービスの場合には、提供される一部のコンピューターシステム環境についてクラウド事業者が用意し、適切な管理を行う責任があるものの、提供されるコンピューターシステム環境上にクラウド利用者が行うシステム構築・運用管理など多くの部分は、利用者が責任を持って行うことが求められます。

(2) クラウド事業者、クラウド利用者、そしてクラウドパートナー

経済産業省が「クラウドサービス利用のための情報セキュリティマネジメントガイドライン」を作成した2011 年のころは、クラウド事業者とクラウド利用者の二つがクラウドサービスの利用に係る役割モデルとして、想定することで、クラウドサービス利用に係る様々な問題点を説明することができました。その後、クラウドコンピューティングサービスが大きく発展した結果、クラウドサービスに係るサービス内容が多様化し、クラウド事業者が提供する様々なサービスの内容をよく理解し、クラウド利用者のニーズに沿った最適なシステムやサービスを構成するための業務を行うクラウドパートナーの事業が拡大してきました。

クラウドコンピューティングのアーキテクチャを定義する ISO/IEC17789 は、クラウドサービスに係る主体を、図 1.1.2 のようにクラウド利用者・事業者・パートナーの 3 つであるとしています。[1]

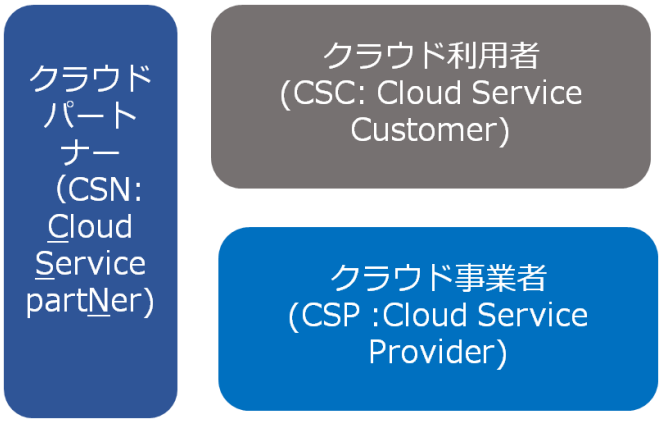


図 1.1.2 クラウドサービスに係る主要主体

クラウドパートナー[2]とは「クラウド利用者とクラウド事業者のいずれか又は両方に対して、助力/支援を約束する主体」（ISO/IEC17788）と定義されています。その役割は、クラウド利用者あるいはクラウド事業者とパートナーとしてのタイプと関係により異なります。

クラウドパートナーは、更に、クラウドデベロッパー、クラウド監査人、クラウドブローカに分かれています。クラウドデベロッパーは、クラウドサービスを利用し、システムのデザイン、開発、テスト、実装、運用などを行う事業者です。クラウド監査人は、クラウドサービスの様々な側面を監査し、情報セキュリティを含むサービスの信頼性を評価し、クラウド利用者またはクラウド事業者に伝える役割を果たします。クラウドブローカは、クラウドサービスについて手を加えずに、クラウド利用者とクラウド事業者の仲介を行うものです。具体的には、顧客に代わって行うクラウドサービスの評価、クラウドサービスのマーケットでの評価、法的な合意のための支援などの役割を担います。

クラウド利用者は、クラウド事業者と業務上の関係をもち、クラウドを利用します。また、様々な目的のために、クラウドパートナーとも業務上の関係をもつ可能性があります。クラウドパートナーの存在は、クラウドコンピューティングサービスの利用をより強力に推進するものなので、望ましいものです。ただし、情報セキュリティマネジメントの観点からは、クラウド利用者と事業者に加えて新たな主体が介在することになり、その責任範囲が分かりにくくなるという課題が生じています。

クラウドサービスの提供の基本は、標準化された仕様に基づく、多数の利用者へのサービスです。一方、クラウドパートナーの協力により、クラウドを生かしたシステムを構築し、利用者に最適のシステムを提供す

---

[1] Given that distributed services and their delivery are at the core of cloud computing, all cloud computing related activities can be categorized into three main groups: activities that use services, activities that provide services and activities that support services.

[2] Party which is engaged in support of, or auxiliary to, activities of either the cloud service provider or the cloud service customer, or both.

ることが可能となっています。クラウドコンピューティングサービスの利用は、クラウドコンピューティングサービスそのものを直接的に利用する形態（以下、クラウドサービス利用）とクラウドコンピューティングサービスを生かしたシステムを利用する形態（以下、クラウドシステムの利用）とでは、クラウド利用者、パートナー、事業者の責任範囲が異なっています。この点を明確に認識して、情報キュリティマネジメントを行うことが、安全なクラウドコンピューティングサービス利用に欠かせないといえましょう。

(3) クラウドにおける情報セキュリティ対策の構造と利用者責任

クラウドサービスは共通のリソースを複数のクラウド利用者が利用するしくみです。一般に、クラウド利用者が用いる資源と管理できる範囲は、一致しません。このため、クラウドにおける情報処理は、クラウド利用者とクラウド事業者及びクラウドパートナーとの共同責任となるのです。

図 1.1.3 は、IaaS 上に別の事業者が PaaS サービスを構築し、最終クラウド利用者に提供している場合を例に、各主体の所有と管理の範囲の相違を図示したものです。

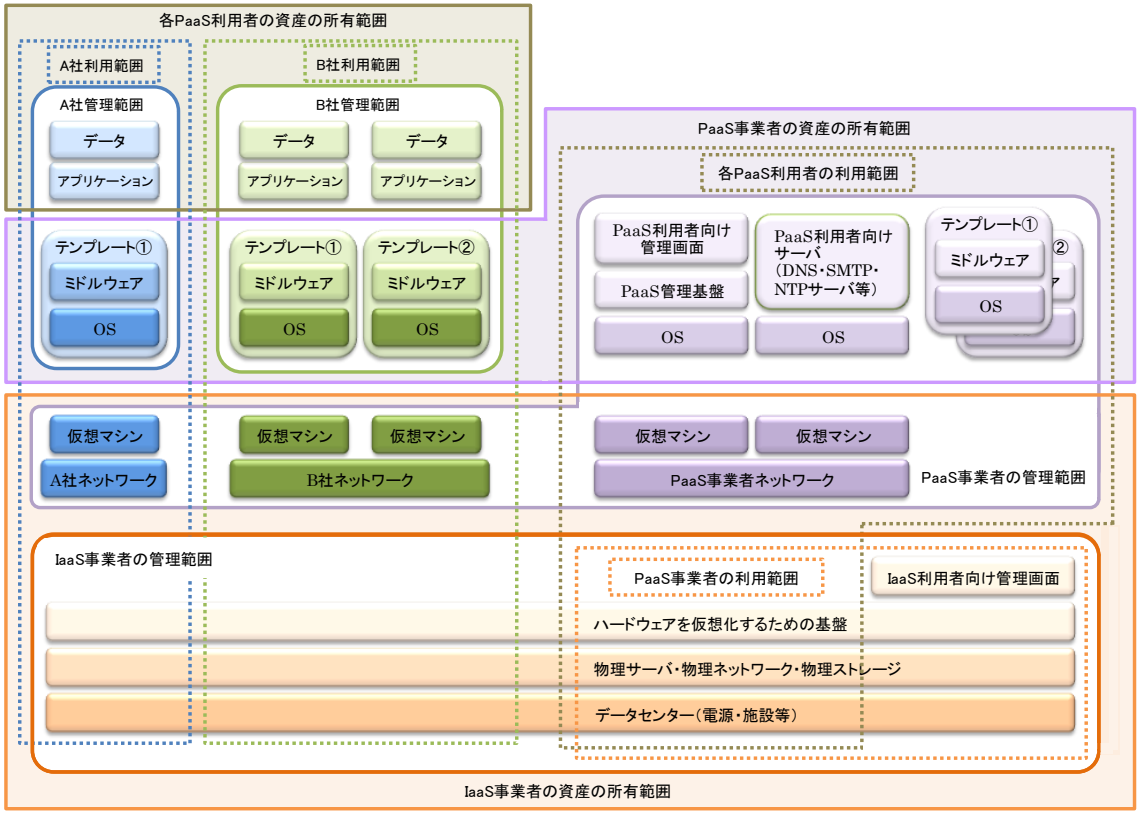


図 1.1.3 クラウド関係者の所有と管理の範囲（PaaS を例にしたモデル）

IaaS 事業者は、物理的な資源とその上に構築されたネットワークおよび仮想マシンまでの範囲を所有し、IaaS の利用者である PaaS 事業者は、仮想マシンに実装した OS、サーバー、ミドルウェア、そして PaaS 利用者向けの管理システムを所有しています。そして、PaaS 利用者は、データ及びアプリケーションが所有範囲です。

物理的な部分の管理は IaaS 事業者の責任になります。仮想マシンとネットワーク管理は IaaS 事業者の責任範囲ですが、PaaS 事業者は個別のマシンやネットワークについて管理することがあり、責任が重なり合う範囲となっています。実際には、契約により責任範囲が明確にされています。なお、PaaS 利用者と PaaS 事業者の管理範囲は、原則としてデータとアプリケーションの管理を PaaS 利用者が担い、ミドルウェアと OS の管理を PaaS 事業者が担うのですが、ミドルウェアの設定に関しては、共同責任となることが

多いのです。

PaaS 利用者の情報処理は、当然のことながら、物理的なものから最上位層のデータに至る全ての層に関わります。所有範囲と責任範囲に関わらず情報処理はすべてが的確に稼働する必要がありますので、PaaS 利用者の情報処理に関しては、IaaS 事業者も PaaS 事業者も責任の一端を担うことになります。これが、情報処理における共同責任ということです。

情報セキュリティは情報処理の一部であるため、クラウドの情報処理が共同責任であるように、情報セキュリティもクラウド利用者とクラウド利用者の共同責任となります。

クラウドシステムの場合には、クラウドパートナーの役割により、責任や管理範囲が大きく異なります。ここでは、クラウドパートナーがクラウドデベロッパーの役割を果たしているケースを想定してみましょう。クラウドデベロッパーがクラウド利用者の委託を受けて、システムのデザイン、構築、運用といういわゆるシステム・インテグレータの役割を果たしている場合のクラウドシステム利用のケースを、クラウドサービス利用と比較したものが図 1.1.4 です。

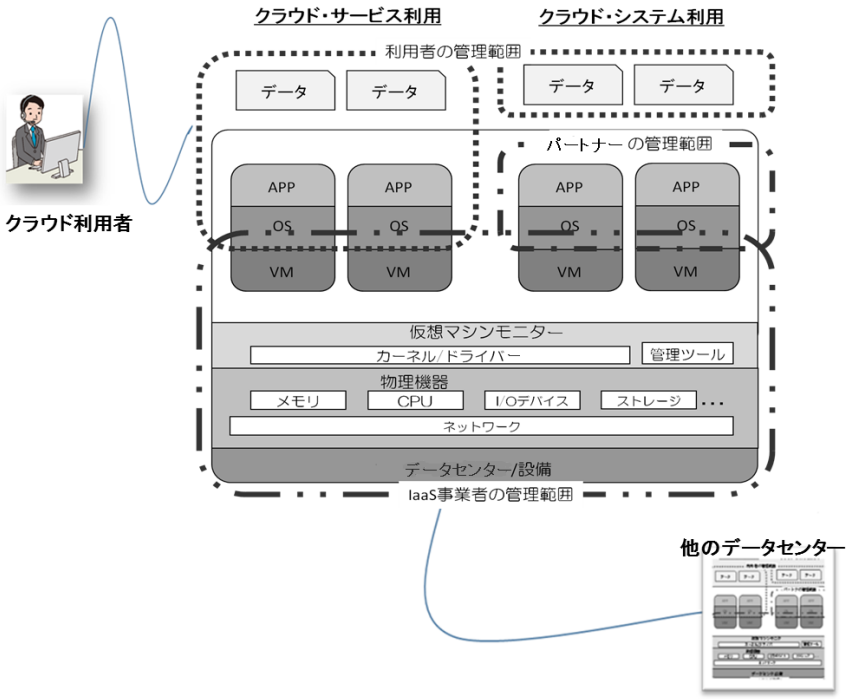


図 1.1.4 クラウドサービス利用とクラウドシステム利用における管理責任の相違

図 1.1.4 の右側はクラウドシステム利用、左側は顧客がパートナーなしにクラウドサービスを利用しているケース（クラウドサービス利用）です。

クラウドパートナーにシステムインテグレーションを委託すると、その業務範囲についてパートナーは管理する責任[3]を有することになります。具体的には、利用者が IaaS 上に構築した仮想マシンからアプリケーションの層までが、クラウドパートナーの管理範囲です。クラウドパートナーは、顧客のニーズを把握し、適切な IaaS サービスを選択し、その事業者が提供可能な仮想機器を選定したうえで、OS、ミドルウェア、アプリケーションを開発・実装し、運用します。そして、クラウドシステム利用者は、データに責任を負うことになります。一方、クラウドサービスをクラウド利用者が直接利用する場合には、この部分も含めてクラウド利用者の責任範囲になります。

[3] 業務委託管理の責任は、クラウド・システム利用者の責任となる

2 クラウドサービスの提供形態と事業者責任の範囲

(1) 事業者責任の意味

事業者責任とは、事業者が様々な活動を行っている時点で発生した災害や事故について、事業者が問われる刑事責任、民事責任、行政責任、社会的責任を指します。

事業者が法令に違反をした場合や、法律を順守していても発生した障害や事故の防止に対する努力が足りない場合、事業者に対して様々な責任が課せられる可能性があります。特に民事責任を問われた場合は、事業者の原因によって発生した障害や事故に対する損害賠償が発生することが想定されますし、社会的責任は、障害や事故が各種のメディアに報道されることで、事業者の社会的信用が失墜することが考えられます。

この章で説明するクラウドサービスにおける事業者責任は、次のように大別できます。

(ア)クラウド事業者のサービス提供に関する責任

クラウド事業者のサービス提供は、クラウド事業者自身で定めている品質保証制度（SLA）に基づき、品質の定量化、計算式、適用の例外を定義しており、自身の定めたサービス品質を下回った場合、翌月以降の利用料金について減額を行う措置を取るようになっているところが多く見られます。このケースには、障害などにより、利用者のデータが消失・破損してしまった場合も含まれます。

但し、クラウド事業者の実施する補償は、あくまでサービスが利用できなかったことに対する利用料金の減額に限られ、障害の発生に起因するクラウド利用者の機会損失に対する損害は、補償の対象外となっています。

(イ)クラウド事業者のセキュリティ対策に関する責任

クラウド事業者のセキュリティ対策は、事業者の実施しているセキュリティ対策についての定期的な報告（セキュリティホワイトペーパーでの報告など）、及び公的第三者による認証制度に基づいた認証資格の取得によりセキュリティを担保しています。

但し、サービス提供の場合と異なり、情報漏洩の対策は記載されていますが、情報漏洩が発生した場合に対する補償は、発生したケースにより対応が異なることから、利用規約などには記載されていないことが多いようです。

(2) SaaS サービスの事業者責任とその留意点

SaaS サービスにおけるレイヤと事業者責任の範囲の例を図 1.2.1 に示します。設計・構築時と運用時では責任範囲が異なることに注目してください。

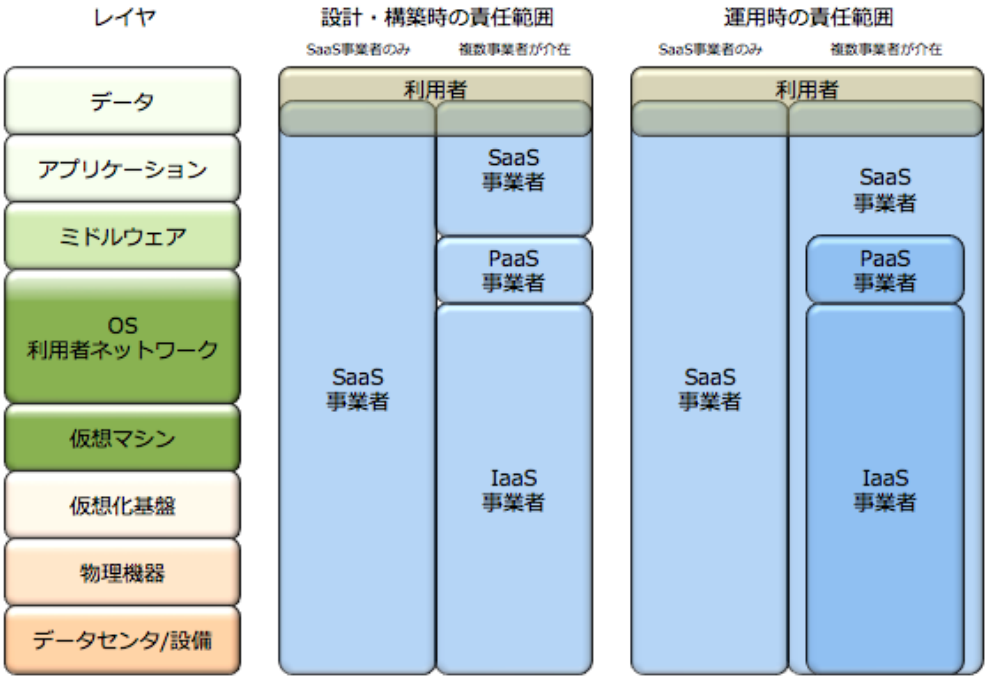


図 1.2.1 SaaS サービスの責任範囲（代表例）

SaaS サービスは、利用者の視点から見た場合、相対する事業者は SaaS 事業者しか見えないため、前提として、データの保護・管理は利用者側の責任範囲、アプリケーションからファシリティまでは SaaS 事業者の責任範囲となります。

実際には、SaaS 事業者はインフラやプラットフォームを提供する他のサービスを利用してサービスを提供している場合があり、複数の事業者のサービスを利用している場合も存在します。このような場合、SaaS 事業者がどのような構成と契約でサービスを提供しているかによって、契約内容や責任範囲が複雑になります。

設計・構築時の責任範囲は、SaaS 事業者と PaaS 事業者、及び PaaS 事業者と IaaS 事業者間において契約関係が成り立つことが考えられ、その契約に準じた責任範囲が存在することになります。具体的には、SaaS 事業者に対する PaaS 事業者の責任範囲（OS～アプリケーション、及びデータ保護の手段提供）、及び PaaS 事業者に対する IaaS 事業者の責任範囲（ファシリティ～OS テンプレートの提供）が存在することになります。

運用時の責任範囲は、利用者と SaaS 事業者間の契約に基づき、前述したとおり、データの保護・管理は利用者側の責任範囲、アプリケーションからファシリティまでは SaaS 事業者の責任範囲となります。このような場合、SaaS 事業者が、サービスを提供するためのリソースを自社で調達・用意をしているのか、他のサービスを利用しているのかについて利用者には説明していない場合がほとんどですし、利用者側もサービスを提供するための仕組みがどうなっているかは、関心がないのが一般的です。

サービスの利用にあたっては、利用しようとするサービスを提供するサービス事業者間の契約は不問とし、その分のリスクを受容するのか、もしくは、サービスを構成する事業者間の関係まで明確化するのか、どちらかを選択する必要があります。

いずれにしても、クラウドの特徴であるデータの保管先が不明確であること、サービスの提供については複雑な契約関係がありうること、さらに、障害が発生した場合、発生する損害を回避する契約条項が存在

するかに留意する必要があります。

また、データは、バックアップの採取や、障害発生に備えた機器の二重化などの手段をサービス事業者が用意してはいますが、最終的な保護・管理の責任はサービス利用者にあることを忘れないようにしてください。

(3) IaaS サービスの事業者責任とその留意点

IaaS サービスにおけるレイヤと事業者責任の範囲の例を図 1.2.2 に示します。

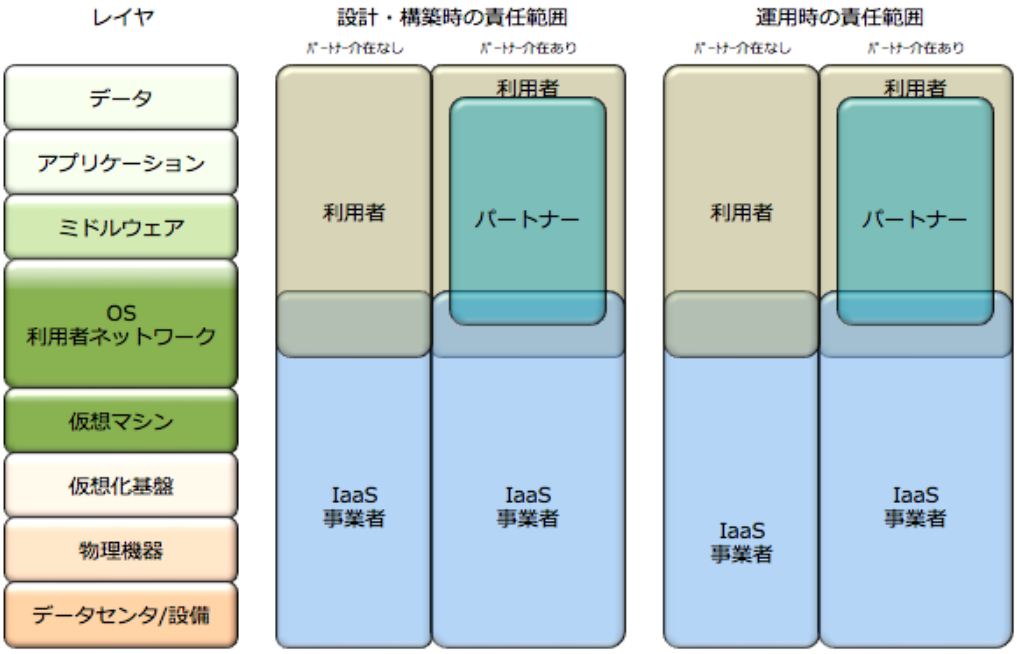


図 1.2.2 IaaS サービスの責任範囲（代表例）

IaaSサービスは、SaaSサービスの場合と異なり、利用者の視点から見た場合、利用者に相対するサービス事業者は IaaS 事業者のみになります。

OS に関しては、IaaS 事業者がテンプレートとなる OS イメージを用意していることが多く、テンプレートとなる OS イメージに関しては IaaS 事業者の責任範囲となりますが、テンプレートを利用して作成、設定を変更した仮想マシンの OS は利用者の責任範囲になります。

同様に、ミドルウェア～アプリケーションのレイヤは、利用者の責任で管理する必要があり、SaaS、PaaS と比較すると、サービス利用のために自由な構成が選択可能な反面、各種の設定やセキュリティ対策など、利用者の責任範囲が広くなります。利用者の責任範囲（作業範囲）が広範囲に亘ることから、クラウドパートナーに設計・構築を依頼する、または運用を依頼する場合が少なくないと思いますが、この場合は、利用者とパートナーの間での契約に沿って、責任範囲が決定します。

IaaS の場合は、SaaS と比較するとシンプルな契約になることが多いように感じますが、利用者側の責任範囲が広範囲であること、複数の IaaS サービスを利用する場合があることなど、状況によっては契約関係が複雑になること、またパートナーとの契約内容について留意する必要があります。

データについては、SaaS サービスと同様に、システムやデータのバックアップの採取や、障害発生に備えた機器の二重化などの手段をサービス事業者が用意してはいますが、最終的な保護・管理の責任はサービス利用者にあることを忘れないようにしてください。

3 事業者から提供される情報の読み解き方

(1) 事業者から提供される情報

クラウドサービスの事業者は、提供するサービスの内容や、様々な事柄に関する取り組み、及び利用者に対するお知らせなどの情報を発信しています。利用者は、サービスを利用する際に事業者が発信している情報について読み取り、内容を把握・理解するとともに、利用者が必要とするサービスや情報提供の要求に対して、どの程度充足しているかを確認する必要があります。

事業者が提供する情報としては、大きく次のように大別できます。

①提供するサービスの機能を説明したもの

②提供するサービスの契約内容や条件を説明したもの

③提供するサービスのセキュリティに関するもの

事業者が提供する情報の最たるものは、上記の①、②にあたるサービスの提供内容や、サービスを利用する際の契約内容になりますが、クラウドの利用パターン、契約形態や条件は、多種多用なパターンが存在するため、利用する際は提供されるサービスの内容、料金の形態と契約内容に関する資料を一読することをお勧めします。

なお、事業者が提供する情報の中で使われている用語は、次章で詳細に説明を行っていますので、情報を読み解く際の辞書や解説として役立てていただきたいと思います。

この章では、上記の③にあたるセキュリティに関する部分、事業者が提供する情報について、どのような部分に気を付けて読み解いていくかを説明します。

(2) 第三者認証に関する情報

事業者は、自身の実施しているセキュリティ対策について、信頼できる第三者によって管理体制や実施しているセキュリティ対策が適切であるか否か評価し認証を受けています。これを第三者認証と呼んでいます。第三者とは、特定の案件・関係について、当事者（利害関係者）ではないその他の者を指します。クラウド事業者が取得している第三者認証について、主要なものを次に示します。

(ア)ISO/IEC 27001（JIS Q 27001）

企業や組織が情報を適切に管理するための包括的な枠組みです。 コンピューターシステムのセキュリティ対策だけでなく、情報を扱う際の基本的な方針（セキュリティポリシー）や、それに基づいた具体的な計画、計画の実施・運用、一定期間ごとの方針・計画の見直しまで含めた総合的なリスクマネジメント体系です。

ISO/IEC 27001 は、ISMS の確立及び実施について、それをどのように実現するかという方法ではなく、企業や組織が何を行うべきかが主として記述されています。

ISO/IEC 27001 の認証は、一般財団法人日本情報経済社会推進協会（JIPDEC）から認定された民間の ISMS 認証機関が行います。

なお、JIPDEC は 2016 年夏に、クラウドセキュリティ認証を ISMS 拡張認証として行うことを発表しています。クラウドセキュリティ認証では、通常の ISMS で要求事項となっている付属書 A の管理策に加えて、クラウドサービスの情報セキュリティ規格として 2015 年に発行された、ISO/IEC27017 の管理策および実施の手引きを取り込んだ対策を行っている組織を認証するものです。ISO/IEC27017 では、利用者が行うべきこと、事業者が行うべきことが定められており、認証は利用者と事業者の双方に対して行われ、事業者に対して認証されたものは、クラウド固有のリスク対策が行われていると考えられます。

また、クラウド上で扱う個人を特定できるデータ（PII: Personally Identifiable Information）の取り扱いに関する規格である ISO/IEC 27018 への準拠性を、民間の審査機関が認証するサービスもあります。

(イ)SOC2（Service Organization Controls 2）

受託業務（サービス利用）の法令順守や運用の内部統制を保証するものです。委託企業の IT ガバナンスにおける統制の有効性や効率性の評価を行う際の手助けとなります。規準には次の 5 項目があり、そのうち 1 項目以上を含むものになります。

・セキュリティ：サービスが未承認のアクセスから保護されている
・可用性　　：サービスは契約とおりの運用、及び利用が可能です
・処理の整合性　：サービスは完全で、正確で、タイムリーで、承認されている
・機密保持　　：機密と指定された情報が、契約に基づき保護されている
・プライバシー　　:個人情報が、企業のプライバシー規定などに基づき、収集、利用、保持、開示されている。

SOC2 の認証は、日本国内では公認会計士が、海外では米国公認会計士協会（AICPA）に所属している公認会計士が行います。

(ウ)FISMA（Federal Information Security Management Act of 2002）

連邦情報セキュリティマネジメント法。アメリカ国立標準技術研究所（NIST）が規定したセキュリティ基準です。連邦政府機関や、連邦政府機関より業務委託を受けている民間の外部委託先に対して、情報セキュリティ対策の実施を法律で義務付けています。

FISMA の認証は、米国連邦政府が指定した認定審査機関が行います。

(エ)PCI DSS（Payment Card Industry Data Security Standard）

クレジット業界におけるグローバルセキュリティ基準です。特筆すべき点は、情報セキュリティに対する具体的な実装を要求しており、「侵入テストの回数と時期」、「パッチリリース後の適用までの期限」「ログオン失敗時のロックアウト」など、具体的な施策が定量的に示されており、アメリカではクレジットカード情報とまったく関係ない企業や組織が PCI DSS を基準として採用しています。

PCI DSS の認証は、PCI 国際協議会によって認定された審査機関(QSA=Qualified Security Assessor)が行います。

上記（ア）～（エ）に示したものの他、業種業態に特化した基準や、日本国内のみで適用されるものも存在します。

第三者認証は、保有していないよりも、保有していた方がよいわけですが、保有していることが必ずしもシステムの安全性を保証しているものではありません。

ISMS は「情報セキュリティのマネージメントに関して、①ルールが制定されているか、②PDCA サイクルが適切に実施されているか」を認証するものであり、システムの安全性に関して認証（保証）しているものではありません。

さらに、ISMS は、PDCA サイクルの実施に際し、企業や組織がどのようなルールを決めているか、また、そのルールに基づきどのような実装をすべきかは、詳細に定義されていません。但し、一定の範囲内ではルールを制定しているので、ルールが制定されている方が安心感は高くなります。

したがって、第三者認証を取得しているから、システムの安全性が高いとは、一概には言えないということになります。

なお、上記で挙げた第三者認証の中には、SOC2 や PCI DSS のように、システムの実装面まで踏み込んで確認を行う認証も存在します。これらの認証はサービス（システム）の稼働、運用までを含めて確認が行われますから、認証の範囲内においての安全性は確保されているといってもよいでしょう。

また、第三者認証は、認証の適用範囲が設定できるものがあります。ある事業者が ISO/IEC 27001 を取得した際の範囲は次のとおりです。

①接続サービス
②Web サービス

③クラウドコンピューティングサービス

④および関連するインターネットサービスプロバイダー業務

ISO/IEC 27001 では、ISMS の適用範囲は、「事業・組織・所在地・資産・技術の特徴の観点から、ISMS の適用範囲、及び境界を定義する。」と定めています。このことから、適用範囲は、適用範囲を全社/一部の業務や事業所とすることも可能です。

PCI DSS は、ISO とは根本的に異なり、仮に準拠する組織側でリスクがないと判断しても、カード会員データを取り扱っている範囲、もしくはそこに接続されているフラットネットワークはすべてが含まれます。ネットワークレイヤからアプリケーションのレイヤまですべてが対象となりますが、適用される範囲がカード会員データに関する部分に限定されているため、クラウド全般への適用を行うものではないと判断されています。

第三者認証で一括りにした場合でも、仕組みに対する認証を行っているのか、実装を含めた認証を行っているのかによって安全性が異なること、また、認証の適用範囲がどのように規定されているかについて、利用する際には十分な確認が必要です。

事業者の取得している第三者認証の内容は、事業者のホームページ、または、セキュリティホワイトペーパーなどの資料に記載されていますので、事前に確認し、不明な部分があれば事業者に問い合わせを行い、後で問題が発生しないようにしましょう。

(3) セキュリティホワイトペーパーに関する情報

事業者の実施しているセキュリティ対策の内容について、その全体をホワイトペーパーでまとめられていることが多くなっています。ホワイトペーパーは定期的に更新され、事業者のサイトで閲覧/ダウンロードが可能になっているので、事業者を選定する際は、その内容について確認を行って下さい。

ホワイトペーパーに記載されている内容は、事業者毎に多少の違いはありますが、大別すると次の内容が記載されています。次は、IaaS 事業者のセキュリティホワイトペーパーに記載されている例です。

(ア)データセンターに関するセキュリティ対策

データセンターの立地、施設の構造、信頼性などのセキュリティ対策について記載しています。セキュリティの観点から、詳細な場所は明記されていないのが一般的です。 具体的には、施設の耐震/免震構造、電源の確保、停電発生時の UPS や自家発電装置入館/入室の対策、及び入館/入室時の認証方法について記載があります。

(イ)ユーザーアカウントに関するセキュリティ対策

事業者が発行する利用者毎（契約毎）のアカウントに関するセキュリティ対策について記載しています。アカウントは、事業者によって厳正に管理され、他の利用者の資産へのアクセスは、原則的に禁止されています。

(ウ)仮想化基盤に関するセキュリティ対策

利用者の提供する仮想化基盤に関するセキュリティ対策が記載しています。利用するための仮想化基盤の仕組みは事業者毎に異なっており、仮想化基盤上で作成されたリソースについて、他のリソースと独立していることを確保しています。

(エ)利用者資産の消去に関するセキュリティ対策

利用者がリソースを破棄した場合、または、事業者が物理的資産を破棄する場合の取り扱いについて記載されています。 上記で述べたように、利用者の資産は仮想化基盤上に配置されているため、破棄した場合、他の利用者からアクセスできないようになっています。

(オ)OS に関するセキュリティ対策

IaaS 事業者の提供する OS のテンプレートに関するセキュリティ対策が記載されています。IaaS に特有の内容になりますが、OS のテンプレートは、セキュリティパッチを適用したものを提供してくれますが、ほとんど

の場合、そのままで利用することはなく、利用者が必要な資産のインストール、必要な設定、データを配置して利用するため、その責任範囲は、事業者と利用者で重複する形になります。

(カ)ネットワークに関するセキュリティ対策

事業者の提供するネットワークに関するセキュリティ対策について記載されています。 パブリック/プライベートネットワークの設定、ファイアウォールの設定や、利用者が接続する際のセキュリティ対策について記載されています。

(キ)物理障害発生時の対応

上記で記載しているとおり、利用者の資産は仮想化基盤上に配置されますが、そのベースとなる物理基盤に障害が発生した場合、事業者がどのような対応を行うかが記載されています。事業者の提供する仮想化基盤の機能にもよりますが、障害発生時に自動的に他の物理基盤上で再起動を行うものもあれば、そのような機能を持たないものもあるため、可用性を考慮する場合、事業者がどのような機能を持っているかを確認しておく必要があります。

(ク) 事業者の提供するサービス独自のセキュリティ対策

利用者が提供する機能毎に、どのようなセキュリティ対策を行っているかが記載されています。 標準的に提供されている機能以外で、セキュリティを向上させるための仕組みについて、利用者が選択して利用することが可能ですので、必要に応じて利用してみてください。

(4) 性能・可用性比較時の留意点

クラウド・コンピューターサービスの性能等の比較を行う場合に、クラウドサービスとクラウドシステムの相違について、注意を払う必要があります。クラウドサービスとして仮想マシンを提供するのが IaaS 事業者の役割です。仮想マシンのスペックには多様性があり、クラウド利用者（または、クラウドパートナー）の情報処理のニーズに応じて、選択することになります。IaaS サービスは標準ですが、仮想マシンのスペックやその上に載せるミドルウェアやアプリケーションは多様性があり、一概に比較はできません。

同様に、レスポンス、BCP など、システムに関わる様々な要求水準も、どこまでを範囲として評価するかによって異なります。仮に、アプリケーションまで含めた場合には、どのようなシステムをシステム・インテグレータが構築するかにより左右されるため、クラウドサービスとしての比較は意味をなしません。システムのパフォーマンスやセキュリティ対応は、システムをどのように組み上げるかにかかっているといえます。

IaaS サービスの場合に特に上記のことは重要ですが、PaaS についてもクラウド事業者がどのようなサービスを行っているかによって、セキュリティ対策や性能が異なります。

クラウドサービスを利用して快適な業務処理を行う場合には、クラウドサービスとその上に利用者のニーズに合わせたシステムが構築されることがあるということを十分認識して、適切な選択を行うことが利用者の責任として重要です。

クラウドコンピューティングサービスの可用性の比較を行う場合には、性能や BCP などに関する知識が必要です。これらに関わる情報も、その用語と誰の立場で発せられたものかを理解しないと、対応が適切ではなくなる恐れがあります。例えば BCP についてみると、クラウドサービスの BCP とクラウドサービスを生かしたシステムの BCP について混乱がみられます。

実際には、標準的なサービスを提供するクラウド事業者がコミットできる範囲は限られており、多くはクラウドパートナーの力量に依存することとなります。この点を明確にしないまま、BCP などを比較することは、誤った認識を広めることになり、望ましいとは言えません。

第 2 章　主な用語とその意味

第 1 章ではクラウドサービスに関わる様々な主体とそれぞれの責任範囲の考え方、並びにクラウド事業者が提供する情報の解釈を行う際に前提となる基本的な枠組みについて説明してきました。本章では、各システム領域、とりわけ性能やセキュリティに関する領域にフォーカスし、クラウド事業者が提示する仕様書等で使用頻度の高い用語について、その意味とクラウド環境に特有の考慮点を解説します。

一見同じ用語であっても、クラウド事業者によって用語に対応する概念は必ずしも同じであるとは限りません。そこで本章では、これらの用語が意味するところを俯瞰的にとらえ、関連用語を含めて解説していきます。

1)運用
- 運用時間
- 計画停止

2)サポート
- ヘルプデスク
- プレミアムサポート
- サービスポータル

3)性能
- 計算能力
- IOPS
- ネットワーク帯域

4)キャパシティ管理
- スケールアップ・ダウン
- スケールアウト・イン
- リソース監視

5)可用性
- 稼働率
- 冗長化

6)セキュリティ

[ネットワークセキュリティ]
- ネットワーク分離
- アクセス制御
- ネットワーク暗号化
- 侵入対策
- DDoS 対策

[データセキュリティ]
- マルウェア対策
- データ保護
- データ消去

[統制/ガバナンス]
- 認証管理
- ログ管理

1 運用

(1) 概要

ここでは、運用に関する次の用語について解説します。

- 運用時間
- 計画停止

運用時間や計画停止は、サービスの最も基本的な仕様を構成するものです。これらに関しては、各クラウドサービスであまり大きな違いは見られません。用語の意味及び定義内容においても比較的似通った内容を持っています。

(2) 運用時間

「運用時間」は、当該サービスが利用できる時間を表す用語です。運用時間に類似する用語として、次のような用語が使用されています。

- サービス時間
- サービス対応時間
- サービス保証時間
- 稼働時間

これらの本質は同じであり、サービスが利用できる時間帯を定義するものです。多くのクラウドサービスでは、クラウド事業者側の視点に立った「サービス提供時間」の定義を行っています。

表 2.1.1 は運用時間の定義例です。

表 2.1.1 運用時間の定義例

例	運用時間・サービス提供時間
1	24 時間 365 日。
2	24 時間 365 日。但し計画停止、緊急メンテナンスを除く。
3	24 時間 365 日。但し年末年始を除く。
4	24 時間 365 日。但し各種受付窓口は、平日 09：00～18：00。
5	24 時間 365 日。但し依頼作業実施は、平日 09：00～18：00 のみ実施可。
6	24 時間 365 日。但し依頼作業実施は、当社営業日・営業時間帯のみとする。

多くのクラウドサービスでは、運用時間（サービス提供時間）を「24 時間 365 日」としていますが、具体的な対象やサービスの範囲は、クラウド事業者により異なる場合があります。多くのサービスでは、運用時間中にメンテナンスを中心とする計画作業や緊急作業を実施することをうたっています。

これらメンテナンス時間の考え方は、SLA/SLO の「稼働率」の算出にあたって重要な意味を持つ場合があります。稼働率算出の際にメンテナンス時間が含まれるのか除外されるのかなどは、クラウドサービスにより異なります。詳細は、**5(2)稼働率**の考え方に関する記述も参照してください。

なお、サービスの中心的な機能（クラウド環境のサーバーの稼働等）以外の部分は、夜間や休日には利用できないケースもあります。例えば、利用者による各種問合せや依頼申請の受付や対応は、平日の昼間に限定するなどの制限を設けているケースがあります。

特に、「当社営業日」等の独自の定義がある場合には、営業日の定義をクラウド事業者に確認しておくことが必要です。

また、クラウド事業者によっては運用時間（サービス提供時間）を定義していない場合があります。このような事業者の場合、24 時間 365 日を前提としているケースが大半ですが、念のためクラウド事業者に確認を行うとより確実です。

(3) 計画停止

「計画停止」は、予告した日時・期間に当該クラウドサービスの全部または一部を停止することを指します。計画停止は通常、予防保守作業やサービスに影響のある各種変更作業等、計画作業を目的として実施されます。

計画停止に類似する概念/用語として、次のような用語が使われています。

- メンテナンス時間
- 定期保守時間
- 計画保守時間

計画停止に関する予告期間や停止時間の考え方などは、表 2.1.2 に示すようにクラウド事業者によって異なります。

表 2.1.2 計画停止の予告期間例

例	計画停止の定義
1	作業開始前までに利用者に通知するよう努める。（＝事前通知努力）[注]
2	最低 24 時間前までの予告。
3	最低 1 週間前までの予告。
4	最低 1 か月前までの予告（緊急時を除く）。
5	最低 3 か月前までの予告（緊急時を除く）。回数は最大 2 回/年。

注 事前の通知タイミングについて、期限を定めていないもの

クラウドサービスの利用者が構築するシステムの稼働への影響を最小限にするため、計画停止に関しては「なるべく短いこと」「なるべく回数が少ないこと」が典型的な評価指標となります。

計画停止によってクラウドサービスが停止される際、クラウド利用者は自らのシステムや業務への影響を最小限とするために、適切な措置を講ずる必要があります。このような対応には時間を要する場合もあり、利用者の観点からは計画停止を可能な限り早期に把握することが重要です。そのため、計画停止実施時における「予告期間（何日前に予告されるか）」は重要な評価軸の 1 つになります。

また、計画停止以外に「緊急停止」や「緊急メンテナンス」などの項目を設けているクラウドサービスもあります。これは重大なセキュリティリスク等が生じた際、これに対処するため、緊急にサービスを停止して作業を実施するものです。その際、クラウドサービス停止に関する利用者への通知は、作業開始 1 時間前など作業の直前としている場合が多くみられます。

緊急時は、事象の内容により柔軟に取り扱うべきではありますが、クラウド事業者側の対応について一体の指針を出している点は、クラウド事業者の対応内容全般についての信頼性をより高めるものと理解できるでしょう。

(4) 留意事項

基本的にはクラウドサービスによる違いはあまり見られません。ただし、特に海外のクラウドサービスを利用する場合には、クラウド事業者が基準とする時間（タイムゾーン）と、日本時間に時差がある場合があるため、メンテナンス時間や営業日等の定義について留意が必要な場合があります。なお、メジャーな海外クラウドベンダーについては、日本にサービス拠点を有する場合も多く、この場合各種時間の定義も日本時間を基準としている場合もあるため、現実的にはあまり問題にならないケースが多いと考えられます。

2 サポート

(1) 概要

ここでは、サポートに関する次の用語について解説します。

- ヘルプデスク
- プレミアムサポート
- サービスポータル（セルフサービス）

ヘルプデスクとサービスポータルは、事業者やクラウドサービスの性質によって、提供のされ方に大きな違いが見られます。全般的な傾向として、ヘルプデスク機能が充実しているクラウドサービスはサービスポータル機能の提供機能があまり充実しておらず、サービスポータル機能が充実しているクラウドサービスは逆にヘルプデスク機能があまり充実していないという関係にあります。これは、各クラウドサービスの位置付けの違いに起因します。

ヘルプデスク機能が充実しているクラウドサービスでは、サービスポータル機能が提供する機能も含めてヘルプデスクの担当者がきめ細かく柔軟に対応することによって、利用者の利便性の向上を図っています。これにより、クラウド環境に不慣れなクラウド利用者や運用人員・体制に不安を抱えるクラウド利用者でも安心して利用できるようにしています。一方、サービスポータルの機能が充実しているクラウドサービスでは、サービスポータル上で利用者が自らクラウド環境に対する操作を実施することで、迅速性を高めるとともに利用料の低減を図っています。これにより、クラウドサービスの特性を生かし、その利用効果の最大化を図っています。多くのクラウドサービスではサービスポータルを充実させています。

ヘルプデスク、サービスポータルいずれの機能を重視するかは、クラウド利用者の利用形態や運用組織等の状況により異なります。各機能の解説及びサービス間での比較の観点を参考に、自組織に最適なクラウドサービスを選定することが重要です。

(2) ヘルプデスク

「ヘルプデスク」は、クラウドサービスの利用者からの各種要求を受け付ける窓口の概念を表す用語です。ヘルプデスクに類似する用語として、次のような用語が使われています。

- サービスデスク
- 窓口機能

ヘルプデスクは、電話やメール等の窓口を通じて、担当者がユーザーからの連絡を受付けます。

受付内容は質問/回答（QA 対応）が一般的ですが、これにとどまらず、利用者からの様々なリクエスト（要求）への対応も含まれます。

ヘルプデスクが提供する機能や役割には表 2.2.1 のようなものがあります。

表 2.2.1 ヘルプデスクの提供機能例

例	ヘルプデスク提供機能
1	問合せの受付/回答
2	利用メニューの追加契約/変更/解約手続き
3	利用環境の設定変更依頼対応、ネットワークの構成変更依頼対応
4	データや各種ログの抽出依頼対応
5	アカウントの追加/廃止依頼対応
6	パスワードリセット依頼対応
7	SSL 証明書等の発行や更新の依頼対応

いわゆるパブリッククラウド系のサービスの場合、サービスポータル上で利用者自らによる操作（＝オンデマンドセルフサービス）により、表 2.2.1 のような機能を実現していることが多くみられます。この場合、ヘルプデスク機能は「問い合わせ対応のみ」の提供にとどまるなど、提供機能が大きく限定されている場合があります。また、そもそもヘルプデスク機能を提供せずポータル上でのセルフサービスのみとしているサービスもあります。

なお、この時クラウド利用者のクラウドサービスに対する期待と実際に提供されるサービスの内容との間で、ギャップが生じる場合があります。クラウド利用者に"運用アウトソーシング"の志向があり、柔軟なオペレーションを期待しているにもかかわらず、ヘルプデスク機能があまり手厚くない場合には、クラウド利用者は期待する運用サービスを受けることができず不満が生じる可能性があります。例えば、パスワードリセットがヘルプデスク経由でのみ受け付けられている場合には、留意が必要です。夜間や休日の作業中にパスワードリセットが必要になった際、ヘルプデスク機能が利用できないため作業が途中でストップする場合があるためです。

(3) プレミアムサポート

クラウドサービスによってはヘルプデスク機能の提供レベルに幅を持たせ、「プレミアムサポート」などの形でオプション化し、より手厚いサービスを提供している場合もあります。追加メニューを契約することにより、通常のヘルプデスク機能に比べてより柔軟でより迅速な手厚いサポートが提供されます。

具体的な提供内容の例は表 2.2.2 のとおりです。

表 2.2.2 プレミアムサポートの提供内容の例

例	提供内容
1	窓口提供時間の延長（通常 平日 9:00-18:00 → プレミア 24 時間/365 日）
2	ゲストサーバー上の OS・MW・APL の環境構築作業の代行
3	ゲストサーバー上の OS・MW・APL の監視及び障害対応の提供
4	ゲストサーバー上の OS・MW・APL の脆弱性管理、パッチ提供作業の代行
5	顧客専任担当者（コンシェルジュ）の設定
6	各種依頼への優先対応
7	多言語対応（英語、中国語、その他）

これらのサービスは、通常のヘルプデスク機能とは異なり、月額またはオペレーション単位での有償提供となっていることが一般的です。プレミアムサポートは、次のような利用ケースにおいて効果的です。

- 特にアウトソーシング志向が強いケース
- クラウド上で重要なシステム（ミッションクリティカルなシステム等）を稼働させる場合

(3) サービスポータル

「サービスポータル」は、クラウドサービスの利用者が各種操作を行うために設けられた、Web インターフェイスです。サービスポータルに類似する概念/用語として、次のような用語が使われています。

- カスタマーポータル
- コントロールパネル
- ユーザーポータル
- ダッシュボード

サービスポータルは、主にユーザー認証を伴う専用の Web サイトとして提供されます。利用者は同サイトにログインし、Web 画面上においてクラウドサービスに関する各種操作を行うことで、リクエスト（要求）を実現することができます。

サービスポータルが提供する主な機能の例は表 2.2.3 のとおりです。

表 2.2.3 サービスポータルの主な提供機能例

例	ポータル提供機能
1	サービスステータスの確認、クラウド事業者からの連絡確認
2	利用環境のリソース状況・パフォーマンスの参照
3	構成情報の参照
4	性能統計データや各種ログのエクスポート
5	ファイルや OS イメージのアップロード
6	サーバーやデータのバックアップの取得
7	サーバーのクローニングやテンプレートの管理
8	契約メニューの追加、変更、解約
9	仮想サーバーの作成、変更、削除
10	仮想サーバーのローカルコンソール接続
11	SSH キーの作成、取得
12	SSL 証明書の発行、更新
13	DNS サーバーの管理
14	ユーザー管理
15	パスワードリセット

クラウドサービスによっては API を提供し、サービスポータルの機能を外部のアプリケーションやシステムから利用することができるものもあります。API を活用しクラウド環境に対する操作を自動化することで、運用を効率化することが可能です。多くの場合、APIはREST形式で提供されています。アクセス方法や利用可能できるメソッドについての仕様は、サービスポータルまたは当該サービスの紹介サイト上で広く公開されています。

既製の統合運用管理ツールの中には、このようなクラウドサービスの API と連携し、一元的に管理する機能を有するものもあります。このような統合運用管理ツールを活用することで、オンプレミス環境とクラウド環境から構成されるハイブリッドクラウド環境を一元的に管理することも可能です。

利用者のシステム操作に関するスキルが高い場合や、システムの開発を担当する人員が直接操作する場合などでは、サービスポータルを利用することにより迅速かつ効率的にクラウド環境を利用することができます。

統合運用管理ツールや RBA（RunBook Automation）ツール等により高度な自動化を実現している利用者は、API を活用することで極めて効率的な運用を実現することができます。

担当者のシステム操作のスキルがあまり高くない場合や運用体制が手厚くない場合には、これらの機能を利用することがむしろ運用担当者の負担になる場合もあります。これらの機能の構築や運用を行うためには、運用担当者が新しい技術を習得したり運用を通じて新たに設計や維持メンテナンスしたりするスキルが必要になるためです。

サービスポータルやAPIは、多くの場合インターネット経由でのアクセスとなるため、不正アクセスや情報窃取等への対策が不可欠です。各クラウドサービスでは、表2.2.4のようなセキュリティ機能を有しています。

アクセス可能なプロトコルについては、ほとんどのクラウドサービスは、暗号化通信（HTTPS、SSL/TLS 等）に限定しています。

表 2.2.4 サービスポータル及び API のセキュリティ機能の例

対象	セキュリティ機能
サービスポータル	通信の暗号化（HTTPS、SSL/TLS）、
	アカウント/パスワード認証
	（アカウントパスワード認証における）ワンタイムパスワードの利用
	トークンや電話等を使用した 2 要素認証
	アクセスログの記録
API	通信の暗号化（HTTPS、SSL/TLS）
	アカウント/アクセスキー
	アクセスキーや時刻情報を元にしたシグネチャ認証
	アクセスログの記録

(4) 留意事項

クラウド利用者は、クラウドサービスに期待するサポート内容を適切に把握したうえで、各クラウドサービスを評価することが必要です。把握すべき点は大きく次の 4 点です。

- 自組織の運用体制、スキルセット（特にクラウドサービスの利用スキル）
- 柔軟性に関する要求
- 運用アウトソーシングの志向度合い
- クラウドパートナーの存在

システムを担当する組織の人員が少ない場合や、他業務との兼任者が多くあまりシステムに関するスキルが高くない場合など、自組織の人員によるシステム構築や運用に難がある場合には、ヘルプデスク機能が提供する手厚いサービスを利用することでこれを補うことができます。

自組織の人員が十分な場合であっても、クラウド環境についての運用アウトソーシングの志向が強い場合には、同様に手厚いヘルプデスク機能が提供されるサービスを選択することでこれを満たせるでしょう。加えて、運用人員による対人的なサービスになるため、比較的柔軟なサービスを受けることができます。（サービスポータルの場合には、クラウド事業者があらかじめ設定した範囲でのみ操作が可能です。）

一方、システムを担当する組織の人員・スキルともに十分な場合には、サービスポータル上でのセルフサービス機能を十分に活用することができるでしょう。これにより、クラウドサービスを利用するメリットを最大化されることが期待できます。この場合、ヘルプデスク機能の充実度はあまり重要ではなくなります。自組織の運用体制に関わらず、運用アウトソーシング志向が低く自組織にてすべての運用オペレーションを実施する意識が強い場合にも、サービスポータルを活用した運用を実現することが考えられます。

クラウドサービスでは、無償のトライアル期間や試用期間を設けている場合があります。このようなサービスを利用し、事前に使用感を把握しておくことは、利用開始後のギャップやトラブルを避ける上で有効です。

また、運用体制においてクラウドパートナーが存在するかどうかも大きな検討要素になります。クラウドパートナー（特にSIer等）は、クラウド利用者とクラウド事業者の間に立ち、通常クラウド利用者が実施する各種オペレーションを代行することがあります。この場合、クラウドパートナーが実質的にヘルプデスク機能を担う形となります。

クラウドパートナーが十分なスキルや体制を有している場合、クラウドサービス固有のヘルプデスク機能やサービスポータル機能/API の充実度はあまり重要ではなくなります。クラウドパートナーがこれらの機能をカバーするためです。

ただし、利用するクラウドサービスが有するヘルプデスク機能やサービスポータル機能/API の内容により、クラウドパートナーとの契約内容や契約金額に影響を及ぼす場合もあるため、この点は注意が必要です。

クラウドサービスの利用開始後のトラブルを避けるため、事前にクラウドパートナーと協議・検討しておくことが重要です。

3 性能

(1) 概要

クラウドサービスの性能は、大きく分けてクラウドサービス自体の運用・管理に関する性能と、サービスが提供するシステム資源やアプリケーションの性能が考えられます。クラウドサービスの運用・管理に関する性能指標は、ヘルプデスク、注文処理、障害・保守時の HW 交換などの対応速度や保障についての定量的な値となります。システム資源やアプリケーションの性能は、クラウドの SPI サービス・モデルによって概ね次のような指標が考えられます。

- SaaS における性能指標 ： 提供するサービスの応答時間や同時接続数など
- PaaS における性能指標 ： 最大同時実行数、平均応答時間、提供リソースの容量上限など
- IaaS における性能指標 ： CPU、メモリ、ストレージ、ネットワークの性能仕様など

ここでは、IaaS における性能に関する次の用語について解説します。

- 計算能力
- IOPS
- ネットワーク帯域

IaaS プロバイダーは、利用者が求めるシステム性能要件に合わせてシステム資源をより安価に、且つ、迅速、容易に調達できるように、サービステンプレート化されたメニューから注文する仕組みを提供しています。選択メニューは、多くの場合、提供するリソース別の性能仕様と提供方式、SW および各種オプション指定により価格設定された内容になっています。

(2) 計算能力

各社のサーバー性能仕様は仮想 CPU(v CPU)のコア数およびメモリ容量が明示されていますが、クロック速度や物理専有率までは開示されていない場合もあり、一概に比較することは難しい状況となっています。

計算能力は、一般にクロック速度×コア数で近似されますが、実際にはベンチマーク（DMIPS や SPECint など）や実機で想定するトランザクションでのシミュレーションによって結果が大幅に異なる場合があります。その理由の 1 つは、利用するアプリケーションやトランザクションの多重度により、メモリ・キャッシュやマルチ・スレッドの効果が異なるためです。また、同一周波数であっても、最新のプロセッサーの方が高性能であり価格性能比に優れています。クラウドでは必ずしもプロセッサー名が開示されておらず、クラウド・プロバイダー間での単純な比較をより困難にしています。

仮想サーバーは vCPU 数が指標となっていますが、HW を専有できる場合をのぞき、他の VM の影響を完全に排除することはできないため、ベアメタル（物理専有型のサービス）とは違い、机上でのパフォーマンス期待値と実際との差異が発生する可能性があります。特に特権区画（例えば、Xen ハイパーバイザーにおける DOM0 や Hyper-V のルート・パーティションなど物理リソースへの特別アクセス権を持つ区画）での処理を必要とするシステム・コールが多いトランザクションを実行する場合（またはそのような第三者の VM が同一 HW 上に展開された場合）マルチテナントの影響が大きくなると考えられます。CPU インテンシブなシステムでは、HW 専有型や、オートスケールによるスケールアウト構成を採用するなど、目的に合わせた選定が推薦されます。

表 2.3.1 に IaaS のサーバー性能の例を示します。

表 2.3.1 IaaS のサーバー性能の例

項目	A 社	B 社	C 社
提供形態	仮想インスタンス 専有仮想インスタンス（HW 専有の仮想インスタンス）	仮想インスタンス	物理サーバー 仮想インスタンス 専有仮想インスタンス（HW 専有の仮想インスタンス） 垂直統合サーバー OpenStack System
使用プロセッサー	IvyBridge など使用プロセッサー公開	使用プロセッサー非公開	IvyBridge SandyBridge など使用プロセッサー公開
CPU コア数	1～32VCPU	1～16VCPU	・1～16 コア（仮想） ・4 から 40 コア（物理）
インスタンス	・バースト・インスタンス（オートスケール可） ・汎用インスタンス ・高性能インスタンス ・GPU インスタンス インスタンス・モデルとサイズを指定（S/M/L/XL/2XL など）	・ベーシック・モデル ・スタンダード・モデル ・コンピューティング・モデル ・最新 CPU 指定モデル ・バッチ・モデル（オートスケール 1～1000 コア）	・仮想：CPU コア数、メモリ・サイズ、ストレージ、NW など自由に組み合わせを指定 ・物理：HW モデルと CPU,メモリ、ストレージ、NW など自由に組み合わせを指定

(3) IOPS

ストレージの性能は、IOPS やハードウェア（SATA,SAS,SSD）が、ネットワークストレージの場合は、ネットワーク帯域が一般的な指標となります。ローカル・ストレージでは、クラウド・プロバイダーによっては、サイズやストレージ・タイプ（HDD,SSD）を選択できる場合もありますが、多くの場合、インスタンス・モデル毎に固定で決まっています。ネットワークストレージでも、2～3 のストレージ・ボリュームのタイプから選択をする場合が多いようですが、まれに IOPS 値を直接指定できるプロバイダーもあります。このような指標のばらつきがあるため、ストレージ性能をプロバイダー間で直接比較することは困難であり、実際のベンチマークや検証により評価せざるを得ない状況であるといえます。

表 2.3.2 に IaaS のストレージ性能の例を示します。

表 2.3.2 IaaS のストレージ性能の例

項目	A 社	B 社	C 社
ローカル・ストレージ	HDD/SSD インスタンス・タイプにより固定	HDD/SSD インスタンス・タイプにより固定	仮想:RAID10 サイズ指定 物理：SATA/SAS/SSD RAID タイプ、サイズ指定
ネットワークストレージ	ストレージタイプ、インスタンスにより最大 IOPS が異なる ・General Purpose（SSD） ・Provisioned IOPS（SSD） ・マグネティック（HDD）	・Basic ・Standard ・Premium（SSD）	・IOPS 指定型 ・GB あたりの IOPS 指定型 から自在に選択可能

(4) ネットワーク帯域

クラウドにおけるネットワークはデータセンター内のネットワークとデータセンター間のネットワーク、お客様拠点とデータセンター間のネットワークに分けて考えることができます。それぞれのネットワーク性能はインターフェイスや回線の速度、ネットワークの帯域専有率、転送遅延（レイテンシー）で評価することができます。データセンター内のネットワーク構成詳細は、開示されていない場合が多く、直接比較することが困難とな

っています。プロバイダーによっては、ルーターやスイッチの配置、ネットワーク・インターフェイスの数やボンディングのカストマイズに至るまで詳細に開示あるいは選択できる場合もあります。こうした開示レベルの高いサービスでは、性能予測や問題判別が比較的しやすいという利点があります。データセンター間のネットワークはインターネットに依存しているプロバイダーと、高速な専用線を利用しているプロバイダーがあり、明らかな違いがあります。お客様拠点とデータセンター間の接続は、多くの場合キャリアの専用回線を引き込むことが可能となっており、回線速度やアクセス・ポイントのネットワーク機器性能により性能を評価することができます。

表 2.3.3 に IaaS のネットワーク性能の例を示します。

表 2.3.3 IaaS のネットワーク性能の例

項目	A 社	B 社	C 社
センター内 LAN	指定なし （インスタンスに依存）	指定なし	パブリック、プライベートの各インターフェイスに帯域指定可能 10Mbps～10Gbps
センター間 WAN	インターネット	不明	プライベートネットワーク 10Gpbs x n
お客様拠点との接続	・専用線サービス(最大 10Gbps) ・VPN	・専用線サービス(最大 10Gbps) ・VPN	・専用線サービス（最大 10Gbps） ・VPN

(5) 留意事項

実際に IaaS 上に実現するシステムの性能は、個別のリソースの性能比較だけでは評価できない場合がほとんどです。例えば、典型的な Web システムをとってみても、1 サーバーの性能だけではなく、各リソースの性能とその組み合わせ方法でシステムの性能が左右されます。安くて遅いサーバーでも複数サーバーを並列処理させることで全体の性能を線形的にスケールアウトすることできます。非分散型の DB や HPC, 科学技術計算など CPU 性能に依存する処理では処理能力に優れたプロセッサーを搭載したサーバーやスケールアップが求められます。

データーアクセスが頻繁に発生するトランザクションの場合、ストレージの性能がボトルネックとならないように IOPS に優れたストレージが求められます。

グローバルな通信、たとえばストリーミング配信など広帯域を必要とするシステムや災害対策システムでは、データセンター間のネットワーク帯域や品質がより重要となってきます。

このように、システムリソースの単純な比較だけではなく、むしろ各プロバイダーのサービス特性を生かした形で、システム要件に応じた設計を行い、それぞれのソリューションとしての比較を行うことが重要であり、より現実的であるといえます。

クラウドを活用したシステムを構築する際に、各クラウドサービスのベンチマークや検証を行うことは、予算や期間、要員などの関係上困難な場合もあります。各クラウド・プロバイダーの性能比較公開情報や、ベンチマーク・レポートを提供している第三者サイト（CloudHarmony など）もあり、性能指針や実機検証を補完する参考情報として活用することができます。

4 キャパシティ管理

(1) 概要

一般的にオンプレミス環境では物理的なコンピューターリソース上限を考慮し、長期的なキャパシティ予測を立て、ハードウェア増設によるスケールアウトやリプレースによるスケールアップを施しています。

クラウド利用者は、オンプレミス環境と同様に、クラウド環境のシステムが利用するコンピューターリソースを適正管理する必要があります。つまり当該システムがどれほどのコンピューターリソースを必要とするのか、その消費状況が常に収容能力を越えないようにしておかなければなりません。

ここでは、キャパシティ管理に関する次の用語について解説します。

- スケールアップ・ダウン
- スケールアウト・イン
- リソース監視・通知

(2) スケールアップ・ダウン

スケールアップ・ダウンとは、主としてサーバー単体の性能を向上（アップ）/低下（ダウン）することを指します。クラウド環境では、コンピューターリソースは事業者内でプールされているため、利用者がオンデマンドでリソースを選択しなおすことが可能です。

パブリッククラウドにて選択できるリソース種類は表 2.4.1 の内容が代表的ですが、その増分量は、クラウド事業者毎に課金を伴うメニューがあり各社各様です。

これ以外に、多くのクラウド事業者が、特定ユーザー向けの専用リソース(ストレージなど)メニューを用意しており、オンプレミス環境から移行し易いサービスを提供しています。

表 2.4.1 リソースの種類及び増分量

種類	増分量（目安）	例（クラウド事業者毎に異なる）
CPU	1vCPU	1,2,4,8,16,32vCPU から選択可能
メモリ	1GB	1.7/3.4/7.5/15/30/60GB の 6 種類から選択可能
ディスク	1～10GB	仮想マシン単位に 10GB から 1TB まで自由に設定可能
ネットワーク帯域	10～100Mbps	インターネット： 1Gbps ベストエフォート、イントラ接続：100Mbps,1Gbps ベストエフォート、FE 自社網接続サービスで 1Mbps～100Mbps

※例 FUJITSU Cloud IaaS Trusted Public S5

なお、スケールアップ・ダウンについては、一部のクラウド事業者を除き、サーバーの再起動を伴う必要があるなどの制限事項も多く、クラウド環境上のキャパシティ制御では過渡期にあります。

(3) スケールアウト・イン

スケールアウト・インとは、同様の機能を持つサーバーや機器の台数を増加（アウト）/減少（イン）させることでシステムやサービス全体の処理性能を向上/低下させることを指します。クラウド環境では、コンピューターリソースは事業者内でプールされているため、利用者がオンデマンドでサーバーや機器を追加/削減することが可能です。この追加/削減したサーバーや機器を稼働中のシステムに追加/システムから除外することで、性能の向上/低下を行います。

システムの負荷が高い場合にはサーバーを増加させて負荷を平準化し、負荷が下がった時点でサーバーを削減することで、突発的な負荷の発生に柔軟に対応することが可能です。

多くのクラウド環境では、こうした柔軟性をタイムリーに享受できるように、予め設定した閾値やイベントトリガーに応じて自動的にリソースを増減する機能(オートスケール)が提供されています。

表 2.4.2 に自動的にリソースを増減するオートスケール(スケールアウト・イン)の具体例を挙げます。

表 2.4.2 オートスケール

基本設定	サーバー台数		1 台～20 台の範囲内で、上限と下限を設定可能
	スケールする単位		1 台ずつ～5 台ずつ
	スケールアウトの間隔		10～ 30 分おき （発生から n 分後に開始）
	スケールインの間隔		10～ 600 分おき （解消から n 分後に開始）
	スケールアウトしたサーバーの寿命		[生成から 30 分] ～ [生成から 600 分]
トリガー 対象	ｻｰﾊﾞｰ	CPU	閾値：使用率＋継続時間
		メモリ	閾値：使用率＋継続時間
		ネットワーク	閾値：流量（Mbps）＋継続時間
	ﾛｰﾄﾞﾊﾞﾗﾝｻｰ	ネットワーク	閾値：流量（Mbps）＋継続時間
スケジュール設定			時間帯、曜日、月内の日、月
オートスケール設定可能数			ゾーンごとに 5 件まで

※例 NIFTY Cloud

(4) リソース監視

各クラウド事業者は、上記のコンピューターリソースを自動監視できるツールを提供しており、コントロールパネルでの表示やアラート通知が代表的です。また、指定リソースの有人監視によるメール・電話通知を行っている事業者もあります。

表 2.4.3 及び表 2.4.4 に、CPU/メモリ/ディスク(サーバー)及びネットワーク(ロードバランサー)に関する自動監視の具体例を挙げます。

表 2.4.3 CPU/メモリ/ディスク(サーバー)のリソース監視

監視ルール	監視項目	PING 結果/サーバーステータス（停止）/CPU 使用率/メモリ使用率/ディスク使用率
	アラート閾値	使用率（0～100%）、継続時間（10～30 分）
	アラート通知先	アラートを通知するメールアドレスの設定（5 件まで）
	設定可能数	10 件まで
アラート履歴		監視状況の履歴をコントロールパネルに表示

※例 NIFTY Cloud

表 2.4.4 ネットワーク(ロードバランサー)のリソース監視

監視ルール	監視項目	ロードバランサー（総量）/ロードバランサー（ポート）のいずれか
	アラート閾値	使用率（0～100%）、継続時間（10～30 分）
	アラート通知先	アラートを通知するメールアドレスの設定（5 件まで）
アラート履歴		監視状況の履歴をコントロールパネルに表示

※例 NIFTY Cloud

(5) 留意事項

クラウド環境を活かすには、手動にせよ自動にせよ、クラウド環境でのスケール方法は、オンプレ環境と同様に、システムの特徴(Web サーバーであればスケールアウト/インが適しており、集約 DB サーバーであればスケールアップ/ダウンが適している)に合わせる必要があります。

クラウド環境の柔軟なリソース増減・拡縮をうまく利用することで、必要とするコンピューターリソースを必要とする時間に割り当てる(月締めのバッチ負荷など)ことでリソースに伴う課金をミニマム化したり、予測不能なリソース消費(マスコミ連動イベントや新規サービスなど)に耐えうる動的なキャパシティにしたり、オンプ

レ環境では実現できないキャパシティ制御が可能となります。

さらに、より多くのメリットを享受するためには、クラウド環境でのキャパシティ監視や性能評価を十分に継続するなど、必要最小限なリソースを見極める綿密なキャパシティ管理が必須となります。

注記 1　クラウド環境利用の現状としては、各社はオートスケール機能を提供しているものの、必ずしも活発に使われているわけではありません。これは想定外の課金懸念もあるものの、クラウドネイティブなシステム管理手法が十分に浸透していない（学習されていない）段階と言えます。

注記 2　システムによっては、オンプレ環境と同様な静的なキャパシティ管理で済む場合も多いので、システム上の業務やサービス特性を把握しておくことが上記の前提となります。

5 可用性

(1) 概要

一般に、システムの耐障害性や稼働性能は RAS として表現される 3 つの要素、すなわち、信頼性（Reliability）、可用性（Availability）、保守性（Serviceability）で評価され、定量的にはそれぞれ MTBF、稼働率、MTTR、が使われています。

一方、システムの設計では、システム要求仕様を定義し、冗長化やバックアップ、BCP/DR 対策により耐障害性を高めた設計・構築をすることで、稼働性能を実現しています。

ここでは、可用性に関する次の用語を解説します。

- 稼働率
- 冗長化

(2) 稼働率

稼働率は、全時間に対する稼働時間の割合のことで、可用性の指標となります。稼働率は、MTBF（MTBF+MTTR）として導かれます。ここで、

MTBF(Mean Time Between Failure) 平均故障間隔。信頼性の指標となります。

MTTR(Mean Time To Repair) 平均復旧時間。保守性の指標となります。

(ア)クラウドにおける稼働率と補償

表 2.5.1 は IaaS における稼働率と補償の例を示しています。表中の「未定義」は、該当 SLA がないか、公開情報から確認できなかったことを意味しています（以下、同様）。

表 2.5.1 IaaS における稼働率と補償の例

項目	A 社	B 社	C 社
サーバー	99.95%（最大 30%SLA クレジット） ただし、複数アベイラビリティー・ゾーンに配置が前提	99.95%（最大 25%SLA クレジット） ただし、同一の可用性グループに 2 以上のインスタンスが構成されていることが前提	99.95% （OpenStack Service の場合）
ストレージ	・オブジェクト・ストレージ 99.9% ・RDB 99.95%最大 25%SLA クレジット）	・SQL 99.9% ・Document DB 99.95% ・Redundant-Storage 99.9%-99.99%	99.95% （OpenStack Service の場合）
ネットワーク	・負荷分散 99.9% （最大 25%SLA クレジット） ・DNS クエリに応答しなかった時間に応じて SLA クレジット発行,4 時間以上で 30 日分 SLA クレジット	・Cache サービス 99.9%（最大 25%SLA クレジット） ・VPN ゲートウェイ 99.9%	100%（2.1 時間以上停止した場合、4 時間ごと 20%、最大 100%SLA クレジット）
管 理 ポータル	未定義	API 管理 99.9%、 99.95%（Premium）	100%（2.1 時間以上停止した場合、4 時間ごと 20%、最大 100%SLA クレジット）
データセンター	未定義	未定義	・HVAC（暖房、換気、空調） 100%（2.1 時間以上停止した場合、4 時間ごと 20%、最大 100%SLA クレジット） ・Tier3 認証（N+1 構成）
MTBF	未定義	未定義	未定義
MTTR	未定義	未定義	HW 交換 2 時間以内

この表から分かるように、クラウドサービスにおける稼働率は、サーバー、ストレージ・サービス、ネットワーク・サービスなど個々のサービスについて SLA が提示されている場合が多く、SLA が満たされなかった場合

は、サービス料金の一部または全額返金といった形で補償が行われています。補償は、利用者のビジネス・インパクトには関係なく、支払い月の利用サービス料金を上限とした一律の基準になっている場合がほとんどです。

障害設計や BCP/DR を考えた場合、SLA における稼働率だけでは十分に要求仕様を満たせない場合があります。これらの要求仕様の実現は、個々のプロジェクトにおけるソリューション設計に依存することになります。

(イ)障害設計と SLA

サーバーの障害設計における要求仕様は、例えば以下のように定義されます。

・障害検知時間　：障害が実際に発生してから、システム的にそれを検知するまでの時間
・切り替え時間　：障害発生後、代替サーバーに切り替えるまでの時間
・縮退要件　：切り替え時の縮退の可否
・技術標準　：負荷分散、クラスタリング、N+1 構成など、冗長化の技術標準

表 2.5.2 は、これらの要求仕様に対するクラウドサービスの SLA を示しています。表から分かるように、クラウドではこれらの要求仕様に対応する SLA は必ずしも提供されていません。利用者は、要求仕様を実現するために、モニタリング、冗長化、ゾーニングや複数センター提供など、クラウドサービスが提供する手段を活用して、ソリューションの組立てを行うことが必要となります。

表 2.5.2　障害設計における要求仕様とクラウドサービスの SLA の例

項目	A 社	B 社	C 社
障害検知時間	基本モニタリング 1 分-3 分 Cloud Watch(オプション)	Web 死活監視など	標準モニタリング・通知 拡張モニタリング（オプション）
切替時間	未定義	未定義	HW 交換 2 時間以内（SW レベルの復旧は利用者責任）
縮退要件	未定義	未定義	未定義

(ウ)BCP/DR と SLA

BCP/DR における要求仕様として、一般に以下が定義されます。

・RPO(Recovery Point Objective) 目標復旧時点、喪失のないデータ復旧を保障する時点
・RTO(Recovery Time Objective) 目標復旧時間、復旧するまでの所要時間
・RLO(Recovery Level Objective) 目標復旧レベル、RTO 内に復旧させる水準

表 2.5.3 は、これらの要求仕様に対するクラウドサービスの SLA を示しています。BCP/DR サービスをクラウド・サービスのメニューとして提供している場合を除き、BCP/DR を想定した SLA は提供されていないのが一般的といえます。データ・レプリケーションや、バックアップリスト、複数センターの活用などを通じて、クラウド利用者が要求仕様を満たすソリューションの組立てを行う必要があります。

表 2.5.3　BCP/DR の要求仕様とクラウドサービスの SLA の例

項目	A 社	B 社	C 社
RPO	未定義	未定義	未定義
RTO	未定義	・Site-Recovery 4 時間-6 時間,100%SLA クレジット	未定義
RLO	未定義	未定義	未定義

(エ)稼働率の補償と対策

クラウドサービスの SLA における稼働率は、努力目標値であり、合意された稼働率が達成されなかった場合は、サービス料金の一部（または全額）が払い戻されるものの、実際のビジネス損失を補填するものではないことが分かります。したがって、クラウドサービス上に構築するシステムの RAS は、クラウドサービスが提供するリソースや機能を上手く活用して、いかに要件に合ったレベルのソリューションに仕立てられるかにかかっていると言えます。具体的な対策として、次のような例が挙げられます。

① サーバーの稼働率に関する対策例

- クラウドサービスで提供されるオートスケール機能と負荷分散装置のモニタリング機能を活用し Web サーバーをスケールアウトさせることで耐障害性を高める。
- アベイラビリティー・ゾーンや可用性グループといった区分けにより同一リージョン内であっても、メンテナンス・ドメインや障害ドメインの境界を提供しているサービスを活用し、可用性向上を図る。
- HW を専有したシングルテナント型の仮想サーバーや物理サーバーの利用による稼働率の向上を図る。専有物理サーバーでは仮想サーバーに比べて、ハイパーバイザーの障害や、マルチテナントによる影響を受けず、RAID 構成や電源の冗長化、計画停止に対する柔軟性もあるため、より高い MTBF が期待できる。また、仮想環境ではサポートされない場合が多い共有ディスクも、物理サーバーでは可能なため、クラスタリング機能を利用した高可用性構成を実現することができる。
- サーバーの冗長化や負荷分散において、アンチ・コロケーション（異なる HW にインスタンスを割り当てること）により耐障害性を高める。
- 開発環境や、高信頼性を必要としない小規模なシングル構成では、HW 故障に対する交換時間が 2 時間といったコミットメントをしているサービスを活用し、低コストで MTTR 要件を充足する。オンプレミスでは、N+1 のバックアプのために予備機のコストが発生し、あるいは障害時に部品や代替機を調達するために数日の時間を要する可能性があるが、クラウドサービスの利用により解決。

② BCP/DR に関する対策例

- ストレージサービスのレプリケーション機能や、バックアップ・リストア・サービスを活用し、RPO,RTO の要件レベルに見合った構成を実現。
- BCP/DR 対策として、本番センターとは異なる地域のクラウド・センターにバックアップ・データを保存しておき、災害時にサーバーをイメージからプロビジョニングすることで、コールド・スタンバイに近い低コストで、ウォーム・スタンバイ並みの RTO を実現。
- サイト・リカバリー・サービス（VMware や Hyper-V の SRM など）により、仮想化レイヤでのサーバーやストレージのレプリケーション機能を活用して DR を実現。

(3) 冗長化

冗長化とは、システムの一部に何らかの障害が発生した場合に備えて、障害発生後でもシステム全体の機能を維持し続けられるように予備装置を平常時から配置し運用することをいいます。

(ア) サーバー冗長化

サーバーの冗長化方式は大きくわけて次の 2 種類があります。

① 負荷分散による冗長化

負荷分散装置をクローン化された複数のサーバーのフロントエンドに配置し、サーバーへの負荷を分散させることで、耐障害性と処理能力のスケールアウトを同時に実現します。 この方式では Active-Active 構成が一般的ですが、負荷分散のポリシー設定によりスティッキー（振り分け先を固定）させたり、Active-Standby 相当の動作をさせることも可能です。負荷分散装置が単一障害点にならないように、負荷分散装置自体を冗長化する必要があります。負荷分散装置はクラスタリングに

よる冗長化するのが一般的です。

② クラスタリングによる冗長化

２台または複数のサーバー間で互いにステータスを監視しながら、利用可能なサーバーがトランザクションを処理する方式で、通常はクラスタリング・ツールを導入して実現します。VMwareHA など、ハイパーバイザーの機能で、高可用性を提供しているものもあります。ハイパーバイザーの高可用性機能は VM レベルの検知・切り替えであるのに対して、クラスター製品やツールでは、OS、ネットワーク、ミドルウェア、アプリケーションレベルの検知・切り替えが可能である点が異なります。 1:1 の Active-Standby 構成が一般的ですが、N:1 の Active-Standby 構成や Active-Active 構成のクラスタリングを提供する製品もあります。

クラウドサービスによっては、共有ディスクを使ったクラスタリングをサポートしていない場合があります。トランザクションの特性に合わせた冗長化方式の選択と利用するクラウド・サービスでのサポート状況の確認が必要です。

仮想化によるクラウドの柔軟性・拡張性を生かしたシステムの構築を考えた場合、負荷分散装置によるスケールアップ方式が推薦されますが、こうした構成に適合しやすいように、アプリケーション設計の段階からステートレスなトランザクション処理方式を採用するといった対策が有効です。

表 2.5.4 に各社クラウドサービスにおけるサーバーの冗長化例を示します。

表 2.5.4 各社クラウドサービスにおけるサーバーの冗長化例

項目	A 社	B 社	C 社
負荷分散方式	・ローカル/クロス・ゾーン/グローバル 負荷分散 ・共有サービスとして提供	・ローカル/グローバル 負荷分散 ・共有サービスとして提供	・ローカル/グローバル 負荷分散 ・共有/専有 サービスとして提供 ・負荷分散装置の HA オプションあり
クラスタリング方式	・ディスクミラー型のクラスタリングが可能 ・共有ディスクを前提としたクラスタリングは不可 ・クラスタリング・ツールを個別導入して利用	・ディスクミラー型のクラスタリングが可能 ・共有ディスクを前提としたクラスタリングは不可 ・WSFC またはクラスタリング・ツールを個別導入して利用	・仮想サーバー、物理サーバーともクラウスタリングが可能 ・クラスタリング・ツールを個別導入して利用
その他 可用性ゾーンなど	・複数のアベイラビリティー・ゾーンにサーバーを分散配置することでメンテナンス時の停止など回避可能 ・物理障害時の VM 自動リカバリーをサポート	・可用性セット内に複数サーバーを配置することでメンテナンス時の停止など回避可能 ・VM 障害時に別 Node への自動再プロビジョニングをサポート	・複数 POD への配置や、ベアメタルサーバーの利用によるメンテナンスの影響最小化 ・VM 障害時の VM 自動再起動をサポート

(イ) ストレージ冗長化

クラウドでは様々なストレージ・サービスが提供されています。ブロックストレージやファイルストレージの他に、オブジェクトストレージや各種の DBaaS があります。また、ストレージへのアクセス経路（ローカル、FC、ネットワーク）やプロトコル（SCSI、iSCSI、NFS、FTP、CIFS、HTTP など）も様々です。サーバーの OS 領域用とデータ領域用、バックアップ・アーカイブ用、HPC 用、コンテンツ配信用など用途や目的に応じてストレージ・サービスを選択し使い分ける必要があります。 ストレージの冗長化は、これらのストレージ・サービスの種類によって方式が異なってきますが、ここでは、ストレージの冗長化を考える上で基本となるディスクレベルの冗長化とストレージ・サービスとしての冗長化に分けて考えます。

① ディスクレベルの冗長化

ディスクのホットスペア：壊れたディスクを速やかに交換できるように、ホットスワップやホットスペアといった機能が提供されています。ただし、データのリカバリーには RAID による復旧かバックアップからのリストアが必要です。

RAID： ディスクレベルの冗長化により、ディスクの単一または複数障害に対応します。RAID コントローラーは HW と SW があります。RAID1 はミラーリング、RAID5 と RAID6 はパリティーを利用した冗長化、さらにストライピングとの組み合わせにより処理を高速化する RAID10,RAID50,RAID60 などがあります。

② ストレージ・システム レベルの冗長化

ストレージ・サービスはネットワーク、ストレージ・サーバー、ストレージからなる 1 つのシステムであり、サービスを構成する 1 つ 1 つの要素が冗長化の対象となりえます。ストレージ・ネットワークのマルチパス、ストレージ・サーバーの冗長化、分散ファイルシステムによる冗長化、データ・レプリケーション、スナップショット、リモート・ミラーリングなどサービスに応じて提供されている冗長化の内容を確認する必要があります。

利用するストレージ・サービスが十分な冗長化機能を備えていなかったり、TCO の観点から高価な冗長化サービスを利用できない場合、代替策としてバックアップ&リストアによる対策を行うなど、運用面でのソリューションを検討します。

表 2.5.5 に各社クラウドサービスにおけるストレージの冗長化例を示します。

表 2.5.5 各社クラウドサービスにおけるストレージの冗長化

項目	A 社	B 社	C 社
サーバー・ストレージ	・SW RAID 指定可能 ・揮発性インスタンス・ストレージ ・EBS ルート・マウント可	・SW RAID 指定可能 ・ネットワーク・ストレージをページ BLOB の VHD としてアタッチ	・HW＆SW RAID ・仮想:RAID10 ・物理：RAID0/1/5/6/10 ・ホットスペア
ストレージ・サービス	・EBS アベイラビリティーゾーン内自動レプリケーション 99.999%可用性 ストレージへのスナップショット取得が可能 ・ストレージ 複数施設、複数デバイスにコピー、99.999999999%の堅牢性と、99.99% の可用性 ・Glacier 2 拠点で同時にデータ損失起こしてもデータを維持、99.999999999%の耐久性	・ローカル冗長ストレージ 1 施設内に 3 つコピー 99.9%可用性 ・ゾーン冗長ストレージ 同一リージョン内の複数施設に 3 つコピー,99.9%可用性 ・GEO 冗長ストレージ プライマリとセカンダリのリージョンにそれぞれ 3 つコピー 99.9%可用性 ・読み取りアクセス GEO 冗長ストレージ 99.99%可用性	・オブジェクトストレージ データセンター内に 3 つのレプリカを自動取得 ・iSCSI,SAN RAID50 ローカル/リモートへのレプリケーション可能 ・Endurance Storage レプリケーション、スナップショット機能を提供

(ウ) ネットワーク冗長化

ネットワーク冗長化はそれぞれの構成要素個別もしくは組み合わせによって行われます。冗長化には次のようなパターンがあり、何をどのように冗長化するかによって、どのような障害で冗長化の効果があるのかが変わることに注意が必要です。

① クラウド内ネットワーク機器の冗長化（スイッチの冗長化等）
② サイト（データセンター）そのものの冗長化（クラウド提供システム全体を指す）
③ ネットワーク経路の冗長化（迂回経路や Active-Standby 構成）

表 2.5.6 にネットワーク冗長化の例を示します。

表 2.5.6 ネットワーク冗長化の例

項目	A 社	B 社	C 社
ネットワーク構成要素	以下の構成要素があることが記載されている ・DC 内のネットワーク ・DC 間の通信はインターネットを利用	以下の構成要素があることが記載されている ・ネットワークリソースは他の利用者と共用 ・IP アドレスは 2 つ割り当て ・同一アカウントのサーバーはネットワーク接続可能	Whitepaper にクラウドシステムのネットワーク構成概要を記載
ネットワーク冗長化	・DC 間ロードバランシング機能あり	・物理的にデータセンター拠点を分けることが可能	（記載なし）

(4) 留意事項

稼働率は、一見分かりやすく感じますが実際に障害に遭遇し補償を受けようとする場合、次のようないくつかの制約があります。これらの制約はクラウド事業者毎に異なるため、稼働率の数字だけで各サービスの評価を行うことは適切とはいえません。また、クラウドの SLA における稼働率は商業的に努力する目標値としてのコミットであり、実質的な保証ではない点にも注意が必要です。

- 利用者側から稼働率補償の申請と、事象の証明（停止時間を裏付けるログなどの提示）が必要
- 稼働率保障の対象となっていないサービスがある
- 利用者にて冗長化構成をしていることが保障の前提となっている場合がある
- 個別のインスタンスやボリュームの障害を対象外としている場合がある
- 停止時間が短い障害は、複数回発生しても補償の対象外としている場合がある
- 計画メンテナンスによるサービス停止時間は、対象外となる場合が多い
- 補償は 1 ヶ月分の支払いサービス料金を上限としており、場合によっては最大 25%に留まっている
- 補償が SLA クレジットで支払われ、同社のサービスには充填できるが、他社サービスや現金への変換ができない場合がある

ここで、クラウドサービスあるいはクラウドを活用したソリューションにおける MTBF、MTTR、稼働率は、次のように考えることができます。

MTBF：クラウドサービス上で提供される様々なタイプのサーバーやシステム資源の中から何を選択したかにより決定される。専有/共有の選択、仮想/物理の選択、アンチ・コロケーションや障害ドメインを跨いだ冗長化の選択に依存する。

MTTR：上記に加えて、システムの冗長化方式の選択、障害検知時間やリカバリー時間に関する構成設定に依存する。

このように、クラウドにおける稼働率は、クラウドベンダーが SLA で提示している稼働率の数値を直接評価または比較することは必ずしも適切ではなく（前提となるサービスや構成上の制約が異なるため一律で比較することは現実的ではないため）、むしろ各クラウドサービスが提供する機能をどのように組み合わせて、要求レベルにあったコスト・パフォーマンスのよい設計ができるかにかかっているといえます。各クラウドベンダーが提供するサービスや機能の特性を生かして最適化されたソリューションを比較することが重要といえます。

また、稼働率はシステム検証では把握することが困難であり、ロングランやある程度の期間使い込んでみないと実態が把握しにくいと考えられます。各社クラウドサービスの実際の稼働率については、各社の過去の稼働実績情報を Web サイトより確認したり、過去の障害情報を確認したりすることである程度把握することが可能です。また、各プロバイダーの稼働率に関する比較公開情報や、ベンチマークレポートを提供している第三者サイト（CloudHarmony など）もあり、参考情報として活用することができます。

6 セキュリティ

6.1 概要

ここでは、セキュリティに関する次の用語について解説します。

ネットワークセキュリティ
- ・ネットワーク分離
- ・アクセス制御（ファイアウォール）
- ・ネットワーク暗号化
- ・侵入対策
- ・DDoS 対策

データセキュリティ
- ・マルウェア対策
- ・データ保護
- ・データ消去

統制/ガバナンス
- ・認証管理
- ・ログ管理

これらの対策は、オンプレミス環境では全てシステムごとの実装となりますが、クラウド環境（特に IaaS 環境）では、従来の垂直統合型のシステムと異なり、実装の考え方がサービスの基盤のレイヤとその基盤上で展開される利用者環境/テナントのレイヤとで大きく 2 つに分かれます。

各レイヤの位置付けを表 2.6.1 示します。また、各レイヤにおいて想定される保護対象と、その保護のための対策の実装例を表 2.6.2 に示します。

表 2.6.1 対策の実装レイヤ の分類

	実装レイヤ	
	利用者環境/テナント	サービス基盤
対策の方向性	・クラウド利用者ごとに実装し、クラウド利用者ごとに異なるポリシーを適用する	・サービス基盤自体を保護するための共通的かつハイレベルなセキュリティポリシーの適用
特徴	・自組織に最適な対策ポリシーが適用できる ・実装に当たり設計構築の負荷が比較的大きい	・クラウド利用者が共用する設備に対して、最低限かつ最大公約数的なセキュリティポリシーの適用される
対策例	・仮想アプライアンス製品を仮想ネットワークに設置 ・仮想マシン上の OS に暗号化ソフトウェアを導入	・物理ネットワーク上に大型の物理製品である FW、DDoS 対策製品、IDS/IPS 等を設置 ・物理サーバーやストレージレベルでのデータ暗号化機能の利用 ・ネットワーク仮想化技術を利用した仮想ネットワークの利用（VLAN） ・専用製品等を用いた通信経路の暗号化（VPN 等
責任主体	クラウド利用者	クラウド事業者

表 2.6.2 セキュリティ対策の責任レイヤと保護対象・想定される実装の関係（IaaS の場合）

		主な保護対象	対策の実施例
利用者環境/テナント	データ アプリケーション ミドルウェア	・アプリケーション/データ	・ネットワーク暗号化 ・マルウェア対策 ・データ保護 ・データ消去
	OS 利用者ネットワーク	・インターネット回線 ・WAN 回線	・アクセス制御（ファイアウォール） ・DDoS 対策 ・侵入検知 ・認証管理 ・ログ管理
管理設備	仮想マシン 仮想化基盤	・リモートアクセス設備 ・サービスポータル ・ハイパーバイザー ・各種管理サーバー（監視、ログ等）	・ネットワーク分離 ・ネットワーク暗号化 ・アクセス制御（ファイアウォール） ・侵入検知 ・マルウェア対策 ・認証管理 ・ログ管理
	物理基盤	・物理サーバー ・物理ストレージ ・ルーター、スイッチ等	・ネットワーク分離 ・ネットワーク暗号化 ・アクセス制御（ファイアウォール） ・データ保護 ・データ消去
	データセンター/設備	・インターネット回線	・アクセス制御（ファイアウォール） ・DDoS 制御

表 2.6.2 に示す「主な保護対象」とそれに対する「対策の実装例」の組合せは参考例ですが、クラウドサービスを利用するにあたっては、調達要件にある各セキュリティ機能のうち、各クラウド事業者から提供されるサービス仕様や機能・メニューが、上記表に示されるようなカテゴリの中で「どの領域のリソース」として提供されているかを適切に把握する必要があります。

例えば、インターネット回線は「利用者環境/テナント」のレイヤにおいて提供されるものと、「管理設備」のレイヤにおいて提供されるものの 2 種類があります。

利用者環境/テナントとして提供されるものとしては、クラウド利用者ごとにインターネット回線を新規に敷設する場合などが考えられます。一方、管理設備として提供されるものとしては、クラウド事業者が予め敷設したインターネット回線を共用する場合などが考えられます。

このような 2 種類のインターネット回線に対して、提供される保護の内容についても提供レイヤによって 2 種類に分かれます。

(ア) 利用者環境/テナントとして提供されている場合

この場合は、次のような対策の実装が想定されます。

- クラウド利用者ごとに異なったファイアウォールポリシーや DDoS 防御ポリシーの適用
- ファイアウォールポリシーはクラウド利用者の要望に応じて任意に設定

(イ) 管理設備として提供されている場合

この場合は、次のような対策の実装が想定されます。

- サービス仕様で定義された共通のファイアウォールポリシーや DDoS 防御ポリシーの適用
- ファイアウォールポリシーはクラウド事業者が管理し必要に応じて設定
- 利用者ごとの対策は実装できない

同じ保護対象・同じ設備であっても、提供されるレイヤによって実際に適用される内容は上記のように異なります。クラウドサービスによっては、両方のレイヤにおいて設備を提供している場合もあり、その場合には両方を組合せて利用できる場合もあります。

また、いずれのレイヤにおいて提供されるかは、当該クラウドサービスの絶対的な優劣には影響しません。これは、サービス利用者がさらされる脅威及び必要とする保護の内容並びに許容可能なコストにより、最

適な対策とその実装が異なるためです。あるクラウドサービスがある脅威に対する対策機能を有していない場合でも、代替手段や個別の機器の設置によりこれを実現できる場合には、実質的には問題と考えられます。

なお、クラウド事業者による管理設備におけるセキュリティ対策は、「クラウドセキュリティ管理基準等のガイドラインにおいてその指針が示されています。

http://jcispa.jasa.jp/documents/

同基準の内容を参照するとともに、同基準への適合性を評価するクラウドセキュリティ監査の実施状況を確認することで、クラウド事業者における対策の水準が一定の水準にあるかどうかを適切に把握することができます。

クラウドセキュリティ監査を実施済みのクラウドサービスには「CS マーク」が付与されます。マークの有無やマークの種類を確認することで、監査の実施状況を簡単に把握することができます。

以降の各項では、システムセキュリティに関するより具体的な内容として、クラウド環境におけるセキュリティ対策が「利用者環境/テナント」と「管理設備」の大きく 2 種類に分類される点を意識しながら、セキュリティ対策領域ごとにその特徴と考え方について論じていきます。

6.2 ネットワークセキュリティ

(1) ネットワーク分離

ネットワーク分離は、システム環境上のネットワークを一定の単位ごとに分離し、相互の接続を遮断または制限するものです。一般的には、ネットワーク設計によるセグメンテーションや VLAN 技術を使用したネットワーク仮想化などにより実装されます。

ネットワーク分離は、クラウド環境に限らず、オンプレミスの個別環境などでも一般的に使用されるものであり、リスクの対象範囲を限定することを目的としたセキュリティ対策の基本的なアプローチの一つです。単一組織内のネットワークでも、DMZ 環境/内部環境の分離や、内部環境の中でもサーバーネットワーク/オフィスネットワークなど、接続されるノードの種類や求められるセキュリティ水準などに基づいてそれぞれのネットワークを分離し、各ネットワークの境界に設置したファイアウォール等によって相互の通信を制御することが一般的です。

クラウドサービスでもネットワーク分離の考え方は基本的には同じですが、クラウド特有の考慮が必要な個所があります。まず、基本的なポイントとして、表 2.6.3 のようにネットワーク分離の対象が大きく 2 種類に分かれる点が挙げられます。

表 2.6.3 ネットワーク分離のパターン

分離対象	分離の内容
利用者間（利用者同士の）ネットワークの分離	クラウドサービスは資源を共用しているため、同じシステム上の他の利用者と同時に CPU/メモリ/HDD/NW を使用している。 クラウドサービスではこれらを論理的に分離して相互干渉しないようにしています。分離方法はサービスによって異なる。
サービス基盤の管理ネットワークと利用者環境/テナントのネットワークの分離	利用者環境/テナントのネットワークは、クラウド事業者が提供するサービス基盤上で実現されている。 しかしながら両者の通信が分離されずに混在している場合、クラウド利用者・クラウド事業者の双方にとって情報漏えいや不正侵入のリスクとなりえる。 リスクの範囲を限定しセキュリティリスクを低減する観点から、サービス基盤の管理ネットワークと利用者環境/テナントのネットワークは適切に分離されているか、あるいは限定された範囲内においてのみ共有されることが必要である。

上記表に示すネットワーク分離の基本的な考え方に沿って、各社各サービスでは、ハイパーバイザー等のソフトウェアや VLAN 技術等を活用した仮想レイヤでの実装や、機器レベルやポートレベルでの物理レイヤでの実装が行われています。表 2.6.4 に、実際のサービスにおける実装例を示します。

表 2.6.4 クラウドサービスにおけるネットワーク分離の実装例

A 社	B 社	C 社
・ゲスト OS 間はホスト OS によって分離 ・パケットフィルタによって分離	・ゾーン単位で物理的に分離	・ファイアウォールによってネットワークトラフィックを分離

クラウドサービスは、通常管理者の異なるネットワークを複数経由して利用されます。

例えば、IaaS サービスで多く見られる「管理コンソール接続」については、まずインターネット経由の VPN 等でクラウド事業者が管理する管理ネットワークに接続し、そこから複数のネットワーク機器やセグメントを経由して、自らが契約しているサーバーに接続できるようになっているケースがあります。この場合、インターネット、サービス基盤の管理ネットワーク、利用者環境/テナントの管理セグメントなどそれぞれ管理主体の異なる複数のネットワークを経由することになります。

セキュアな通信環境を実現するため、経由する各ネットワークにおいて、前掲の表に示したネットワーク分

離のパターンを満たすような、適切なネットワーク分離の実装が行われていることを確認・検討することが必要です。

(2) アクセス制御（ファイアウォール）

アクセス制御は、ネットワーク経由での脅威への対応及び通信の制御・分離を目的とし、通信の制御を行うものです。一般的には、ファイアウォール（FW）の各製品により実装されます。

クラウド環境特有の要素は比較的少なく、非クラウド環境同様に個別の要件を検討し、対策を実装することが必要です。

前掲の表に示すとおり、提供レイヤや実装責任の観点から、採用する製品やサービスが、サービス利用者の必要とするセキュリティの水準を満たすかどうかを検討することが必要です。

また、クラウド事業者が管理設備（サービスポータルやリモートアクセス専用設備、共用のインターネット回線）において、適切な対策をとっているかどうかについても確認が必要です。

近年はより高機能なファイアウォール製品も普及してきています。IP アドレスや通信ポートレベルだけでなく通信内容そのものについて制御するファイアウォールで、表 2.6.5 に示すような L7FW（Layer-7 Firewall）や WAF（Web Application Firewall）などと呼ばれるものです。これらの機器は単に通信の制御をするだけでなく、通信内容そのものを解析し不正なデータ等を遮断したりすることが可能です。

表 2.6.5 高機能ファイアウォールの種類

種類	機能
L7FW / 次世代 FW (Layer-7 Firewall)	ポート番号のレベルを超えて通信の種類を識別し、通信を制御する。 例として、TCP/80 番ポート（HTTP）を使用するメッセンジャーソフトの通信を識別し遮断するケースなどがある。
WAF (Web Application Firewall)	通信内容のデータを識別し、不正なデータが含まれている場合にこれを遮断（ブラックリスト方式）したり、通常想定されている通信内容から逸脱した不正なデータの通信を遮断（ホワイトリスト方式）したりする。 例として、Web アプリケーションにおける SQL インジェクション攻撃を遮断するケースなどがある。

これらの機器は非常に高価でかつ運用負荷が大きかったことから、ユーザーが個別に導入することが困難でした。しかしながら、近年ではクラウドサービスにおいてサービスメニューとして提供されている場合があり、サービス型で利用できることから個別に導入する場合に比べて安価に利用することが可能です。加えて、クラウド事業者にFWの管理運用業務をアウトソースできる場合もあり、この場合には導入のハードルはより低いと言えます。

L7FW や WAF の導入を検討されている場合には、これらのサービスメニューが提供されていないかクラウド事業者に確認するとよいでしょう。

(3) ネットワーク暗号化

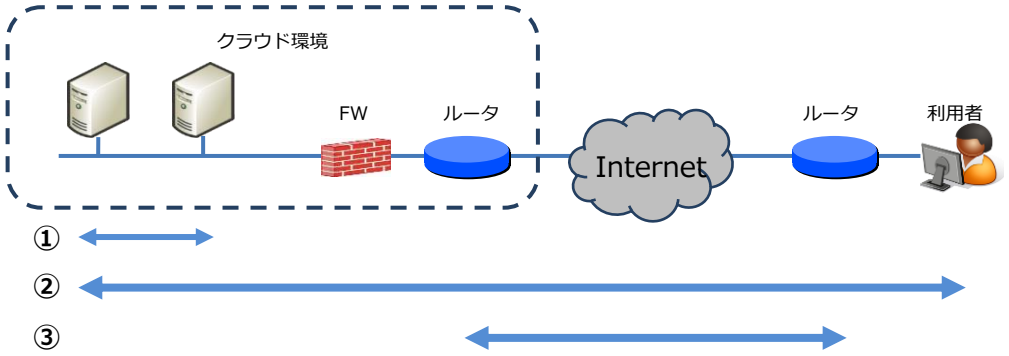
ネットワーク暗号化は、通信内容の秘匿や完全性の確保のために、通信経路の一部または全体（エンドツーエンド）において通信内容の暗号化を行うものです。一般的には、IPsec や SSL/TLS として知られる暗号化通信技術が使用されます。

ネットワーク暗号化の技術自体は、クラウド特有のものではなく、非クラウド環境において使用されるものと同じものです。しかしながら、クラウドサービスは本質的に「WAN や Internet 等のネットワーク越しで利用する」という性質をもつため、非クラウド環境での場合に比べてその重要性は非常に高いと言えます。

クラウド事業者もこの点は認識しており、多くのクラウドサービスでは通信経路の暗号化機能やサービスメニュー、またはより安全性の高い専用線の接続メニューなどを提供しています。また、前述のネットワーク分離で示したとおり、クラウドサービスに関わるネットワークは複数の管理主体が関わっており、かつ各ネットワークにおけるセキュリティ上の脅威は様々です。そのため、経由するネットワークの種類を考慮し、採用する

暗号化通信の方式や適用箇所を選択することが必要です。

図 2.6.1 に暗号化通信の適用例と対応できる脅威の種類について例を示します。



暗号化通信の種類		主な暗号化方式	対応する脅威の種類
①	クラウド内ネットワークの暗号化 クラウドサービス上のネットワーク内で行われる通信を暗号化する。 クラウドサービス上のサーバー間通信などを保護する。	・SSH ・SSL/TLS ・LDAPS ・SMTPS ・SFTP/FTPS/SCP	・クラウドサービス上の悪意ある他の利用者による通信内容の盗聴・改ざん ・クラウド事業者内の悪意ある人間による通信内容の盗聴・改ざん
②	エンドツーエンドの暗号化 クライアントとサーバーの間で行われる通信を暗号化する。 アクセス元からアクセス先までの全経路において暗号化が行われるため、高い秘匿性を実現する一方で、クライアント端末側が当該暗号化方式に対応している必要があるため、利用が困難や制限が生じる場合がある。 Web システムなどの場合はフロントエンドとなる Web サーバーや SSL アクセラレータとクライアント PC 間での暗号化となり、途中経路での盗聴などへの対策となる。	・SSL/TLS ・SSH、SSH ポートフォワード ・SFTP/FTPS/SCP ・SMTPS	・クラウドサービス上の悪意ある他の利用者による通信内容の盗聴・改ざん ・クラウド事業者内の悪意ある人間による通信内容の盗聴・改ざん ・インターネット上に存在する悪意ある人間による通信内容の盗聴・改ざん
③	ネットワークエッジでの暗号化（VPN） エッジルータや FW 等を使用した暗号化及びトンネリング技術により、インターネット等の公衆回線を介して複数の LAN を接続する。 仮想専用ネットワーク（VPN：Virtual Private Network）と称され、専用線の代替として利用可能である。また、広域イーサネット等の WAN 回線に本暗号化方式を組合せることで、更なる高セキュリティを確保する場合もある。 バーチャルプライベートクラウドなどのサービスを利用する場合など、クラウドネットワークと組織のネットワークを直接接続する場合にこのような方法が利用される場合がある。インターネット上で仮想ネットワークを構成する。	・IPsec ・SSL(SSL-VPN) ・PPTP	・インターネット上に存在する悪意ある人間による通信内容の盗聴・改ざん

図 2.6.1　暗号化通信の適用例と対応できる脅威の種類

(4) 侵入検知

侵入検知は、一般的に IDS(Intrusion Detection System)と称するもので、ネットワークやシステムへの不正なアクセスないしその兆候を検知し、アラートを発報するものです。近年は、侵入検知とアラートの発報にとどまらず、該当する不正な通信を自動的に遮断する機能を有する製品もあり、これらは一般的には IPS(Intrusion Protection System)と称します。両者を総称し、IDS/IPS と言及されているケースが多く見られます。

侵入検知の対策は、クラウド環境特有の要素は比較的少なく、非クラウド環境同様に対策を実装することが必要です。

クラウド事業者にてサービスのオプションとして IDS/IPS が提供される場合もありますが、採用する製品やサービスがクラウド利用者の必要とするセキュリティの水準を満たすかどうかを検討することが必要です。

これらの前提として、サービス基盤の設計としてクラウド利用者間の通信が利用者ネットワーク（仮想ネットワーク）において、適切に分離される設計になっていることが不可欠です。

加えて、クラウド事業者が管理設備（サービスポータルやリモートアクセス専用設備、共用のインターネット回線）において、適切な対策をとっているかどうかについても確認が必要です。

(5) DDoS 対策

DDoS 対策は、ボットネットなどによる分散 DoS 攻撃（＝DDoS 攻撃）に対して、その検知及び攻撃元からの通信の遮断等を行うものです。

クラウド環境は、複数のサービス利用者にシェアされた環境であり、DDoS 攻撃においても特有のリスクを有するため、本対策は特に重要なセキュリティ対策の一つです。クラウド環境において特に留意すべき DDoS 攻撃のリスクは、表 2.6.6 のとおりです。

表 2.6.6 クラウドサービスに特有の DDoS 攻撃のリスク

リスク	具体的な影響	主な対策
特定の利用者に対する攻撃により、その他の利用者が悪影響を受ける	同じクラウドサービスを利用する他の利用者が DDoS 攻撃を受けたことで、共用のインターネット回線がダウンし、結果攻撃を受けていない利用者についてもインターネット接続ができなくなるなどの影響を受ける。	共用インターネット回線等において、クラウド環境へのインバウンド通信における攻撃の検知/対処を行う → 事業者責任により設置する管理設備にて実装
クラウド利用者が攻撃元となり、他の組織を攻撃したことで、悪影響を受ける	同じクラウドサービス上の他の利用者がマルウェアに感染し、DDoS 攻撃の攻撃元となって他のクラウド利用者を攻撃したことにより、攻撃元となった共用インターネット回線がブラックリストに登録され、共用インターネット回線を利用するすべての利用者においてインターネット通信に悪影響が発生する。	共用インターネット回線等において、クラウド環境からのアウトバウンド通信における攻撃の検知/対処を行う → 事業者責任により設置した管理設備にて実装

上記対策の中心は、管理設備に対するものです。インターネット回線など特に高いスループットが要求される箇所であることから、物理的な製品により実装しているケースも多く見られます。

この場合、対策の実施はクラウド事業者が行います。クラウド利用者は、管理設備に対して、クラウド事業者がどのような対策を実装しているかを確認・検討することが必要です。

クラウド事業者がサービス基盤の設備（特にサービスポータルやリモートアクセス設備、等）において、適切な対策をとっているかどうかについても確認を行ってください。サービス基盤への対策状況は、サービスの管理機能の可用性に影響します。

6.3 データセキュリティ

(1) マルウェア対策

マルウェア対策は、ウィルス・ワーム・トロイの木馬など利用者の意図に反して悪意ある動作を行う各種プログラム（＝マルウェア）に対して、その検知・駆除または隔離を行うことをいいます。

マルウェア対策は、クラウド環境特有の要素は比較的少なく、非クラウド環境同様に個別の要件を検討し、対策を実装することが必要です。

前掲の表に示すとおり、提供レイヤや実装責任の観点から、採用する製品やサービスがサービス利用者の必要とするセキュリティの水準を満たすかどうかを検討することが必要です。クラウド事業者が管理設備（サービスポータルやリモートアクセス専用設備）において、適切な対策をとっているかどうかについても確認が必要です。

近年ではサンドボックス型のマルウェア対策製品なども普及してきています。これらの製品は、ネットワーク上でやりとりされるファイルやアプリケーションデータを一度隔離された環境（＝サンドボックス環境）に展開して実行し、不正な動作をしないかどうか確認したうえで転送する機能を有しています。昨今世間を賑わしている標的型攻撃や改ざんされた web サイトから感染するタイプのマルウェアへの有効な対策の一つとして注目されています。

ネットワークゲートウェイのオプション機能やメールサービスのオプション機能として提供しているサービスもあり、サービス型で利用できることから個別に導入するよりも安価に導入することが可能です。

サンドボックス型のマルウェア対策機能の導入を検討されている場合には、これらのサービスメニューが提供されていないかクラウド事業者に確認するとよいでしょう。

(2) データ保護

データ保護は、クラウドサービス上またはクラウドサービスの基盤に関する各種データについて、不正アクセスや傍受等があった場合に、情報漏洩の被害を低減するための各種対策です。一般的な対策としては、データの論理的分離や権限管理の厳格化、データ及び通信の暗号化などがあります。

利用者環境/テナントに存在するデータに関する保護は、クラウド環境特有の要素は比較的少なく、非クラウド環境同様に個別の対策を実装することが必要です。

実装はクラウド環境上でサービス利用者が構築するシステム等においてアプリケーションレベルで行うことが多く見られます。これは、実際に当該データを扱うのがアプリケーションですためです。

サービス利用者は、自らのアプリケーション設計において、データ保護について考慮することが必要です。

クラウド利用者のデータの実体は、サービス基盤内のストレージに格納されます。各クラウド利用者のデータは、クラウド事業者の責任の下それぞれ分離され保管されています（クラウド利用者ごとに分離された単位を、クラウド事業者によっては「テナント」と呼称しています）。

テナントの分離レベルは各クラウド事業者の設計や実装に依存しますが、いずれの場合でも「他のクラウド利用者を含む、許可外のアクセスを不可能とする」レベルの保護が必ず提供されています。

なお、データの実体がサービス基盤上に配置されていることから、当該データに対してはクラウド事業者がアクセスすることが可能です。これを完全に遮断することは原理的に困難ですが、いくつかの方法により実質的なセキュリティを担保することができます。

また、クラウド事業者が管理設備（サービスポータルやリモートアクセス専用設備）において、適切な対策をとっているかどうかについても確認が必要です。

特に、クラウド事業者が保有するサービス利用者に関する各種情報（契約情報や設定情報など）の管理について、留意することが必要です。

表 2.6.7 にクラウド事業者内の悪意あるアクセスからの保護の例を示します。

表 2.6.7 クラウド利用者のデータに対する、クラウド事業者内の悪意あるアクセスからの保護

対策	説明
クラウド事業者内でのアクセス権管理の厳格化	クラウド事業者の担当者によるサービス基盤へのアクセスについて、権限管理を厳格化しそもそも必要最小限の範囲でのみアクセスさせる。 ネットワークやストレージ等のコンポーネントごとに担当を区分し、それぞれの担当ごとに権限を分離することで更に効果を高めることが可能。 特権 ID 管理のシステムや踏み台サーバー等を連携させ、アクセスの都度申請承認等を必要とするような管理を行うことで、より効果的な管理を実現することも可能。 本対策はデータの漏洩対策だけでなく、内部犯によるデータの破壊行為への対策としても効果的。
データの暗号化	実際に保存されるデータについて、サービス基盤上に保存する際に予め暗号化しておく。暗号化キーは必ずクラウド利用者にて管理する必要がある。 データを暗号化することで、悪意あるクラウド事業者の担当者が当該データにアクセスした際でも、データを読み出すことができず実質的にデータを保護することが可能。 データの漏洩対策としては、最も効果的な方式の一つといえる。

(3) データ消去

データ消去は、クラウドサービス上またはクラウドサービスの基盤に関する各種データについて、その廃棄時に確実な消去を行うことで、意図しないデータの復元等を防止する各種対策です。

一般的な対策としては、物理ディスクの破壊などがあります。

クラウド環境では、管理設備側のデータはさることながら、サービス利用者のデータも管理設備内の統合ストレージにホストされる場合がほとんどです。これらの統合ストレージは、当該サービス利用者専用ですことは少なく、多くの場合にはストレージ内部が論理的に区分され（＝LU 等）、これをサービス利用者ごとに割当て使用しています。これは、単一の物理ディスク上に複数のサービス利用者のデータが存在することを意味します。

このため、クラウド環境特有の問題として、従来行われてきたディスクの物理破壊によるデータ消去が困難であるという点が挙げられます。

一般に、クラウド環境上の利用者環境/テナントのデータは、クラウド事業者が管理するストレージ上に保存されており、クラウド事業者側でこれを論理的に削除した場合には、通常これを読みだしたりデータを復元したりすることはできません。

クラウド事業者が、悪意をもって削除済みのデータを復元することは、技術的には可能な場合もあります。しかしながら、多くのクラウド事業者は適切な内部統制体制を確立しており、現実的にそれらの行為を行えないように組織的または技術的な対策を行っています。

近年はサービス利用者の上記懸念に対応するため、データ消去のオプションを提供するクラウド事業者も現れています。表 2.6.8 にオプションの例を示します。

表 2.6.8 データ消去オプションの例

対策	説明
物理ディスク廃棄時のディスク破壊	統合ストレージ上の物理ディスクについて、廃棄する際に必ず物理破壊を行う。 非クラウド環境における物理破壊同様の対応は行うものの、他のユーザーと物理ディスクを共有している場合には、サービス利用者の解約後即時のディスク破壊は行われない場合がある。 実際にディスク破壊が行われるタイミングは、クラウド事業者に確認が必要。
サービス利用者専用の物理ディスクの確保と、廃棄時のディスク破壊	統合ストレージ上の物理ディスクについて、物理ディスク及び論理領域を常に単一のサービス利用者のみが使用するように予め設計しておき、当該物理ディスクの廃棄時には必ず物理破壊を行う。 非クラウド環境における物理破壊と同等レベルの愛作を実現することが可能であるが、物理ディスク等を特定クラウド利用者の専用に切り出す必要があるため、容量単価などが比較的高額になる場合がある。
専用ツールによる論理消去	専用ツールを用いて論理領域のデータを消去する。ブロックゼロイング等を行うとともに、同作業実施のエビデンスを当該ツールから出力できるものもある。 ディスクの破壊を伴わないため、作業は比較的に迅速に実施可能。ただし、ツールの使用に関して、追加の費用が発生する場合もあるので要注意。

6.4 統制/ガバナンス

(1) 認証管理

アカウント認証は、サービス基盤及びクラウド利用者の各システムに対するアクセスについて、ユーザーID等のアカウント情報を元に認証（及び許可）を行うものです。

利用者環境/テナントの各システムにおけるアカウント認証管理は、クラウド環境特有の要素は比較的少なく、クラウド環境以外の場合と同様に個別の対策を実装することが必要です。

サービス基盤における認証管理としては、次のものがあります。

- サービスポータルの認証/許可
- リモートアクセス経路の認証/許可

サービス基盤における認証管理の仕様は、クラウド事業者の設計や実装に依存します。そのため、クラウド利用者が任意の実装を選択することは通常不可能です。しかしながら、サービス基盤における認証管理はクラウド利用によるクラウド環境の管理機能へのアクセスを制御していることが多いため、クラウド事業者の管理状況が不十分/不適切な場合にはセキュリティ上のリスクとなる可能性があります。クラウドサービスの認証機能の実装状況について、事前にクラウド事業に確認することが必要です。

クラウドサービスにおける認証機能の実装について、一般的な確認ポイントを表 2.6.9 に示します。なお、この確認ポイントは例であり、全ての利用ケースにおいて必ず必要または実装可能とは限りません。自組織の利用要件やシステムの特性等を考慮して検討してください。

表 2.6.9 認証機能に関する確認ポイント

確認ポイント	説明
サービス基盤アクセス用アカウントについて、単一アカウントの共用を許容していないこと	管理用のアカウントが単一の共用アカウントでないこと。 単一の共用アカウントの利用は、同時接続数が制限されることによる操作性の低下と、セキュリティ事故の際のトレーサビリティの低下をもたらす可能性がある。 単一のアカウントを共用するような管理方式は、可能であれば避けたほうがよい。
脆弱なパスワードを許容していないこと	パスワード攻撃に弱いパスワードポリシーでないこと。 辞書攻撃やブルーとフォース攻撃等の既知の攻撃に対しては、一般的な対策が既に存在する（英数字記号が混在した 8 文字以上の文字列等）。導入のハードルも比較的低いことから、原則として適用されていることが望ましい。
より強力な認証方式を備えていること	2 要素認証やワンタイムパスワード等が利用できること。 単純なアカウント/パスワード認証だけでなく、トークン/クライアント証明書/電話等を使用した 2 要素認証や、接続の都度異なるパスワードを使用するワンタイムパスワード機能を提供しているクラウドサービスもある。 複数の認証機構を組合せることで、認証の精度を高めることができる。

また、利用者環境/テナントに関する認証機能そのものを提供するクラウドサービスもあります。このようなサービスを利用した場合、利用者環境/テナントにおけるアプリケーション等のユーザー管理・認証管理とサービスポータルやリモートアクセス経路におけるユーザー管理・認証管理を統合することができます。

(2) ログ管理

ログ管理は、クラウドサービスないしクラウド環境上に構築された各種システムにおける、認証やシステム動作に関するログの収集/監視/保管/破棄等を行うものです。

利用者環境/テナントの各システムにおけるログ管理は、クラウド環境特有の要素は比較的少なく、非クラウド環境同様に個別の対策を実装することが必要です。

なお、クラウドサービスによっては利用者環境/テナント向けにログ管理機能を提供する場合があります。

クラウド事業者から提供されるログサーバーやログ管理コンソールを利用することで各種ログを効率的に管理することが可能です。ログの管理保管だけでなく、サービスポータル上でのログのエクスポート機能なども提供されている場合があります。

監査証跡として各種ログの管理が求められる場合には、これらの機能を利用すると効率的です。

ただし、利用者環境/テナントのログには、クラウド利用者固有の情報や機密データが含まれている場合がありますので、データの暗号化や権限管理の厳格化（クラウド利用者の中でも限られた人員のみアクセス可能とする、等）など、当該サービスの提供仕様について十分注意が必要です。

サービス基盤におけるログ管理の対象には、表 2.6.10 のような種類があります。

表 2.6.10 サービス基盤に関する主なログ

種類	説明
サービスポータルに関するログ	クラウドサービスが提供するサービスポータルに関するログ。具体的には次のようなログが含まれる。 ・サービスポータルへの認証ログ（アカウントによるログイン/ログオフ等のログ） ・サービスポータル上での操作内容に関するログ（コマンド実行履歴等） ・サービスポータルへのアクセスログ
リモートアクセスに関するログ	管理用のリモートアクセス設備に関するログ。具体的には次のようなログが含まれる。 ・リモートアクセス設備における認証ログ（アカウントによるログイン/ログオフ等） ・リモートアクセス中の操作内容に関するログ（コマンドラインや GUI の操作内容） ・リモートアクセス設備へのアクセスログ なお、リモートアクセスをサービスポータル上で提供しているクラウドサービスもある。この場合には、サービスポータルに関するログに包含される場合もある。
サービス基盤の設備に関するログ	クラウドサービスのサービス基盤設備に関するログ。具体的には次のようなログが含まれる。 ・サービス基盤機器のシステムログ/エラーログ ・サービス基盤機器に関する認証ログ ・サービス基盤機器への操作内容に関するログ ・サービス基盤機器へのアクセスログ（セッションログ） ・サービス基盤への不正アクセスログ

上記のログは全てクラウド事業者が管理していますが、クラウドサービスにより取得していないものもあります。特に操作ログ関連は、ログのデータサイズが巨大化する場合もあることから、範囲や内容を絞って取得しているケースがあります。

これらのログのうち、サービスポータルに関するログやリモートアクセスに関するログは、当該クラウド利用者に関するものに限ってエクスポート機能を提供したり依頼ベースでエクスポートしたりするクラウドサービスが多く見られます。事故対応時や監査証跡として必要になるケースでは、これらの機能を利用すると効率的です。

一方、サービス基盤に関するログは、多くの場合非公開の位置とされています。これは、クラウド利用者であっても情報公開することがセキュリティ上のリスクとなる場合があるためです。サービス基盤に関するログは、クラウド事業者の責任の下、収集及び監視が行われています。

サービス基盤に関するログには、クラウド利用者固有の情報含まれている場合があります。たとえば、GUI 操作に関するログには画面情報が含まれるため、操作時に画面上に表示されていた情報は全て操作ログとして保存されている場合があります。

このようなデータが含まれている可能性がある場合には、ログデータの保管や監視の仕様について特に留意が必要です。これらログデータが流出した場合には、業務データの流出に準じた影響が懸念されるためです。そのため、クラウド利用者はサービス基盤側で取得されているログについて、その内容や保管仕様等について事前にクラウド事業者に確認しておくことが必要です。

6.5 留意事項

前述のとおり、セキュリティ対策はクラウド事業者の責任領域とクラウド利用者の責任領域のそれぞれで検討することが必要です。

セキュリティ対策は、システム全体で実装することが必要なことから、物理レイヤからアプリケーションレイヤまで通して検討することが必要です。従って、クラウド環境ではクラウド事業者が実装又はオプションとして提供する対策が、システム全体のセキュリティ対策の要求をどの程度カバーするのかを適切に把握し、カバーされない部分はクラウド利用者が個別に対策を実装することが重要になります。

クラウド事業者において実装される対策は、多くの場合すべてのクラウド利用に共通的に適用される内容であることから、最小限の範囲で提供される場合が多いため、各クラウド利用者の個別のニーズを満たさない場合もあります。各クラウドサービスの提供仕様を評価検討し、必要に応じて個別実装も含めた検討が必要です。

検討に当たっては、一定の客観性や準拠性の観点から、各種の認証や監査への対応状況を評価することも効果的です。前述の「CS マーク」は、クラウド環境に特化した仕組みですことから、CS マークの取得状況を確認することは特に有効性が高いと言えるでしょう。

各セキュリティ対策を検討する際にはクラウドパートナーの協力を得ることは非常に有効です。クラウドパートナーを活用することで、クラウドサービスのセキュリティ対策の評価や必要に応じて、個別のセキュリティ対策の実装を効率的かつ効果的に行うことが期待できます。セキュリティ分野の技術革新は日進月歩であり、特に専門性が高い領域であることから、クラウドパートナーを活用するメリットは特に大きいと言えます。

なお、各社ともネットワークは実装方法についての明確な記載がなく、また、記載されている内容も複数の項目に分散して記載され、統合して図でかかれているなどといったものが多いのが現状です。また、詳細なネットワーク構成情報などは原則非公開となっていることが多く、契約前に得られる情報には限りがあります。

執筆者

金丸浩二　グローバルブレインズ株式会社
酒井正紀　伊藤忠テクノソリューションズ株式会社
監物岳夫　ニフティ株式会社
加藤雅彦　株式会社インターネットイニシアティブ
百瀬孝三　日本アイ・ビー・エム株式会社
永宮直史　特定非営利活動法人日本セキュリティ監査協会

編集
木村道弘　特定非営利活動法人日本セキュリティ監査協会

エンタープライズクラウド選定ガイド
クラウド選びで困ったら　～要求仕様作成と提案書評価のための基礎知識～
JASA クラウドセキュリティ推進協議会（JCISPA）

平成 28 年　1 月　15 日　第 1.0　版発行
発　行：特定非営利活動法人日本セキュリティ監査協会
〒135-0016　東京都江東区東陽 3 丁目 23 番 21 号　プレミアム東陽町ビル
TEL 03-6675-3820 FAX 03-6675-3819 http://www.jasa.jp/