PostgreSQL インサイド

クラウドで攻めのビジネスを！

選択すべきクラウドサービスの種類と、これからのシステムに重要な業務継続性を考える

シェアリングサービスの登場やキャッシュレス化の推進など、企業にとって ICT はビジネスに欠かせない存在になりつつあります。
多くの企業が、いま、ICT を活用したサービスの拡大に着手しています。例えば、製造業の場合、BtoB システムにより小売店経由で販売していたものを e コマースで消費者へ直接販売したり、IoT を活用してモバイル端末などから製品を制御するサービスを提供したりなど、様々なサービスが拡大しています。この動きは製造業にとどまらず、あらゆる業種に広がっています。
これらの新サービスは、ビジネスチャンスを逃さないためにも迅速に提供することが求められています。そこで注目されているのがクラウドサービスの活用です。クラウドサービスであれば、高価なハードウェアの導入コストを抑えられるだけでなく、システムの運用管理の手間も省けて、サービスそのものに注力できると考えられているからです。
本記事では、クラウドサービスを利用する際にサービスの種類に何を選択すべきか、またクラウド環境でシステムを構築する際に押さえておきたいポイントについて紹介します。

攻めのビジネスに最適なクラウドサービスの種類を見極める

クラウドサービスの中で、いま注目されているのが PaaS です。近年、クラウドベンダーから高機能なマネージドサービスが提供され、IaaS に比べて簡単にサービスを立ち上げられ、運用負荷も軽減できると言われています。中でもデータベースのマネージドサービスが充実してきています。クラウドベンダー各社から PostgreSQL や MySQL など OSS ベースのデータベースを活用したマネージドサービスが提供されており、これらは運用負荷を下げながら安価にデータベースを利用できると注目されています。 ただし、従来オンプレミスでサービスを提供してきた企業が導入する場合、「運用管理」や「システムのライフサイクル」の考え方の違いに注意が必要です。

PaaS のマネージドサービスは「運用管理の手間を軽減＝型化」

まず、運用管理の違いについて考えてみましょう。オンプレミスで構築する場合、自社のシステムに合わせて運用を設計できます。しかし、マネージドサービスの場合、クラウドベンダーごとに運用が型化されているため、自社のサービスに合った運用ができるかを確認する必要があります。
例えば、バックアップ運用の場合、同じ PostgreSQL のマネージドサービスを提供している Amazon Web Service （以降、AWS）と、Microsoft Azure 、Google Cloud Platform で実施方法が少しずつ異なります。

AWS の RDS for PostgreSQL

- 自動スナップショットによりバックアップを取得可能
- 5 分前の時点に復旧可能

Microsoft の Azure Database for PostgreSQL

- フルバックアップと差分バックアップ、スナップショットの 3 種類のバックアップを取得可能
- バックアップの保持期間は 7 日間、最大 35 日まで延長可能。保持期間の任意の時点に復旧可能
- 選択するストレージのサイズにより、バックアップの種類と取得のタイミングが異なる

Google の Cloud SQL for PostgreSQL

- 自動バックアップとオンデマンドバックアップの 2 種類を取得可能
- バックアップの保持期間は 7 日間。保持期間の任意の時点に復旧可能

このように、同じ PostgreSQL のマネージドサービスでも、各社で運用ルールが異なるため、提供するサービスに合う運用かを事前にしっかり調査する必要があります。

将来的にマルチクラウドを考えている場合、「クラウドベンダーごとに異なる運用ルール」が負荷になる可能性があります。クラウドサービスを積極的に活用している企業からは、マルチクラウドを活用して迅速なサービスを提供するための鍵は「汎用的に使える共通ノウハウである」という声があります。これは、同じ PostgreSQL を利用する場合でも、マネージドサービスのようにクラウドベンダーごとに異なる運用ノウハウをそれぞれ理解して進めるよりも、IaaS でオンプレミスからクラウドまで 1 つのノウハウで構築・運用を進められることが重要である、ということを意味します。

PaaS のシステムのライフサイクルはミドルウェアのサポート期間

次に、システムのライフサイクルの考え方です。オンプレミスの時は、ハードウェアから OS、データベース、アプリケーションまで、すべてを自社で用意し、構築・運用していたため、システム更改まで 10 年といった長期で運用しているところも少なくありません。
しかし、クラウドサービスの場合、システム運用の一部をクラウドベンダーに任せることになります。「任せる＝クラウドベンダーのサービス保証期間に委ねる」ことを意味します。例えば、PaaS の場合、OS のサポート期間は 10 年近く対応しているものもありますが、データベースなどのミドルウェアのサポート期間は、3 年から 5 年と短いものが多くなります。つまり、PaaS にすることでシステムの運用負荷を軽減するメリットがある一方で、システム更改を短サイクルで回す必要が出てきます。システム更改は、サービスの追加がない場合も、OS やミドルウェアのバージョンアップに伴う非互換対応などの修正が必要になり、開発・テスト・サービスの入れ替えなど、かなりの負荷がかかります。このように、PaaS を選択する際には、運用・保守コストとシステム更改のコストのバランスを考慮する必要があります。

IaaS は長期に利用できる柔軟なシステムを構築可能

IaaS で OSS コミュニティーが提供している PostgreSQL を導入したとしても、クラウドベンダーが提供する PostgreSQL のマネージドサービスとサポート期間が変わらないと思われるかもしれません。
そこでお勧めしたいのが富士通の「FUJITSU Software Enterprise Postgres（以降、Enterprise Postgres）」です。PostgreSQL ベースでありながら、導入・運用をサポートする GUI や、バックアップ / リカバリーなどの信頼性機能、暗号化などのセキュリティ対策機能を拡張しており、コミュニティー版の PostgreSQL と比べ導入・運用が容易です。そして、Enterprise Postgres のサポート期間は最短でも 7 年とコミュニティー版に比べて長く、標準サポートで 10 年以上使える PostgreSQL なのです。

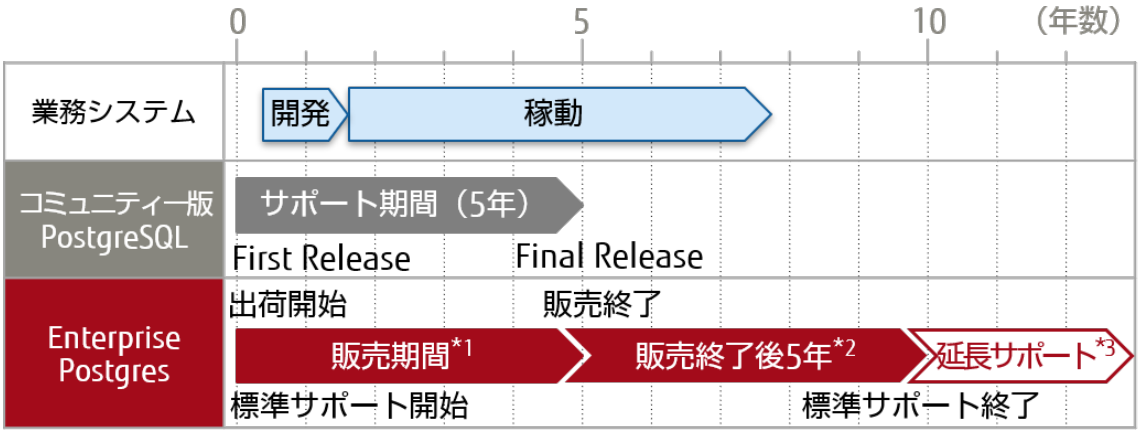

図 1：Enterprise Postgres サポート期間

- *1　図中の出荷開始時期は実際とは異なります。コミュニティーがリリースした日を起点として、期間を比較したものです。また、販売期間は目安であり、実際の販売期間と異なります。
- *2　標準サポート期間は、出荷開始後 7 年、または販売終了後 5 年のどちらか長い期間です。
- *3　延長サポート終了日は、延長を希望されるお客様との契約により設定します。

IaaS ではミドルウェアの運用管理の負荷を下げることはできませんが、オンプレミスで高価なハードウェアを導入・運用することを思えば、IaaS でも十分にサービスの迅速性と導入・運用コストを削減できるメリットはあります。また、PaaS の場合、利用できるミドルウェアに制限があることも多く、オンプレミスで使い慣れたミドルウェアが使えないといった声もあります。クラウドサービスの種類を選択する際には、導入・運用コストだけでなく、システムのライフサイクルや開発・運用要員のスキルも含めて検討する必要があります。

IaaSで押さえておきたいセキュリティ対策と業務継続性の考え方

クラウドサービスの選択として、IaaSでも十分にメリットがあることをお伝えしました。ここからはIaaSを利用する際に押さえておきたいセキュリティ対策と業務継続性の確保についてお伝えします。これは、単にオンプレミスからクラウドに変わるからではなく、これからのビジネスを拡大していくうえで押さえておきたいポイントでもあります。

クラウドのセキュリティ対策ではデータまで確実に守る

セキュリティ対策の必要性は言うまでもなく、オンプレミスの時も様々な対策が取られてきました。しかし、パブリッククラウドにデータを置くとなると、従来の対策と同じにようにはいきません。特に注意したいのがデータベースの暗号化です。というのも、オンプレミスの時は、ファイアウォールや通信の暗号化、アクセス制御など、外部からの侵入対策は実施しているものの、社内にあるデータベースについては運用管理体制を徹底することで保護し、データの暗号化までは実施していない企業が多いのが実情だからです。
パブリッククラウドの場合、データを社外に置くため、この点の見直しが必要です。IaaSの場合、ストレージの暗号化機能を利用してデータを暗号化できますが、これは暗号化対策として十分とは言えません。ストレージに対する盗聴からはデータを守れますが、OS ユーザーやストレージ管理者がデータベースのデータファイルやストレージボリュームを直接参照することで、データの内容を盗み見ることができてしまいます。
また、ディスクの廃棄処理が適切に行われなかった場合、そのディスクから情報が漏えいする可能性もあります。クラウドベンダーがしっかりとした管理体制で運用していても、運用管理から廃棄処理まで多くの人が介在する中で、リスクをなくすことはできません。万が一、悪意のある第三者の手に渡った場合、消去されたディスクから情報を復元される可能性がないとは言い切れないのです。そして、情報が漏えいした際の最終的な信用問題は、その個人情報を保持していたクラウド利用企業側にかかってくるのです。

このようなことから、IaaSを利用する場合は、ストレージの暗号化だけでなく、データベースの格納データそのものを暗号化する必要があります。
Enterprise Postgres は、データベースの格納データを容易に暗号化できる透過的データ暗号化機能を備えています。透過的データ暗号化機能は、格納データだけでなく、ログやバックアップをすべて暗号化することができます。暗号化アルゴリズムには、共通鍵ブロック暗号の 1 つでアメリカ国立標準技術研究所（National Institute of Standards and Technology　：NIST）が定めた AES（Advanced Encryption Standard　）の 128bit / 256bit　に対応しています。これは、現在最も強固なアルゴリズムと言われています。 Enterprise Postgres の暗号化は、テーブルを格納する「テーブルスペース単位」で設定できるため、必要な部分に絞って暗号化できます。また、暗号化してもデータファイルのサイズは大きくならず、暗号化/復号によるオーバーヘッドも 3%未満に抑えているため、暗号化の範囲に迷った場合にすべてを暗号化しても、リソースや性能に影響を与えません。
そして、暗号化キーの管理も容易です。暗号化キーは暗号化するテーブルスペース単位に設定されますが、管理者はマスター暗号化キーをパスフレーズで管理するだけです。暗号化キー自体も暗号化されているため、データを安全に管理することができます。

これからの業務継続性に必要な考え方はツールの併用型から ICT 完結型のサービス

次に、業務継続性の確保についてです。クラウドサービスを利用する場合、トラブル発生時の復旧はクラウドベンダーの対応待ちになります。このため、業務継続に対する何らかの対策が必要になることは間違いありません。しかし、ここで押さえておきたいのは、クラウドサービスの利用に限らず、これから新領域へとサービスを拡大していくうえでの考え方です。
オンプレミスのシステムで、サーバー1 台、もしくは仮想化ソフトウェアの High Availability 機能を利用して、バックアップ運用のみで業務継続性を確保している企業は少なくありません。このような企業の多くは、BtoB の企業向けシステムと、電話やメールなどのツールを併用して運用しています。システムトラブル時も代替手段があるため、バックアップ運用でも十分に対応できていました。
しかし、サービスを一般顧客向けに拡大する、もしくは一般顧客向けの新サービスを提供する場合は、従来のバックアップ運用では対応が難しくなります。サービスのターゲットが企業から一般顧客に変わると、システムの利用者数やサービス提供時間が大きく変わるからです。一般顧客向けでは利用者自体が増えるため、電話やメールでの対応は実質的に困難になります。また、顧客のライフスタイルに合わせて、サービスの時間を 24 時間対応にするなど広げる可能性もあります。これもまた、人に頼った運用では対応しきれなくなることでしょう。このように、業務継続を従来の考え方のままで進めることは、ビジネスチャンスを逃すことにもつながります。この問題は一般顧客向けのサービスに限ったことではありません。働き方が急速に変化している現在、従来の企業向けサービスもツール併用型の運用から ICT 完結型へ、つまり止まらない ICT サービスが求められてきているのです。

IaaS の機能だけでは業務継続性は確保できない、ミドルウェアでの対応が必要

では、IaaS での業務継続性はどのように確保していけばよいのでしょうか。クラウドサービスでは、システムの可用性を高めるためのマルチ AZ（Availability Zone）が提供されています。また、クラウドベンダーからは、クラウドの可用性や性能などのサービスレベルを保証する SLA（Service Level Agreement：サービス品質保証）が提示されており、中には可用性の稼働率 99.99%と高いサービスレベルを保証するところもあります。
これだけ高いレベルの保証であれば、システムの業務継続性の確保も問題ないと思われるかもしれません。しかし、IaaS で保証されるのはハードウェアのみです。ハードウェアのトラブルには、AZ の切り替えや再起動など対応してくれますが、ミドルウェアのトラブルは保証の対象外になるため、利用者側で可用性を確保する必要があります。

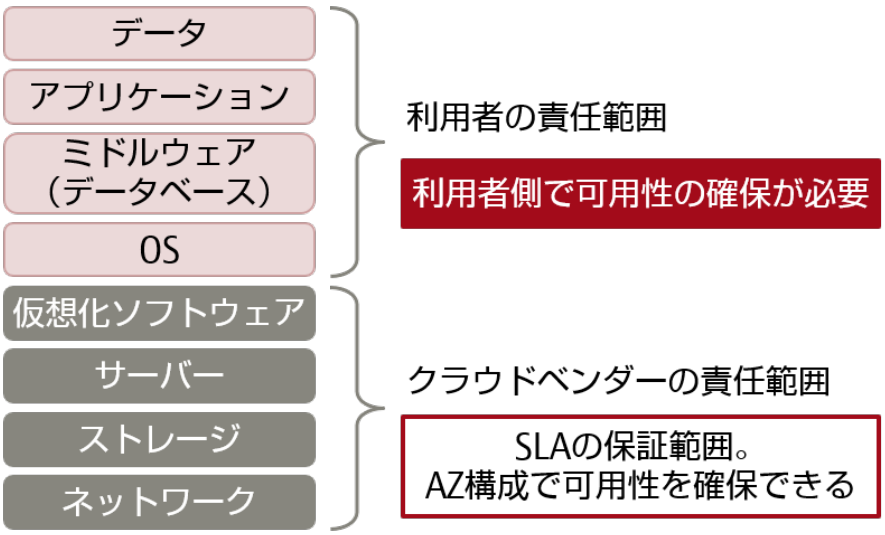

図 2：IaaS の保証範囲

業務継続性を確保する方法はいろいろありますが、ここでお勧めしたいのが、クラスタソフトウェアを利用する方法です。データベースから業務アプリケーションまでシステム全体を冗長化し、トラブル時にはシステム全体を切り替えられるため、運用負荷を抑えて業務継続性を高められます。
Enterprise Postgres では複数のクラスタソフトウェアに対応しています。中でも、クラウドで実績が高いのがサイオステクノロジー社の LifeKeeper です。

クラスタソフトウェアでは一般的に共有ストレージを用いますが、多くのクラウドではこの共有ストレージが利用できません。複数のノード（サーバー）を 1 つの共有ストレージに紐づけるという機能を提供していないのです。しかし LifeKeeper は、共有ストレージ構成とデータレプリケーション構成（ディスクをミラーする）の 2 つの構成を選択できます。このため、共有ストレージが利用できないクラウド環境でも HA クラスタによる可用性を確保することができるのです。AWS や Azure をはじめ、多くのパブリッククラウドに対応しており、Linux 環境はもちろん Windows 環境にも対応しています。オンプレミスの時に Windows Server Failover Clustering（以降、WSFC）を利用されていた方で、クラウドでは WSFC が利用できないので他の手段に変更しなくてはとお悩みの方も、LifeKeeper のデータレプリケーション構成を利用すれば、WSFC のままクラウドに移行することも可能です。
また、LifeKeeper には、導入を支援する「ARK（Application Recovery Kit）」と連携する GUI ツールが提供されているため、Enterprise Postgres をはじめとする主要なソフトウェアのクラスタ構成を、ウィザードで容易に設定・変更することができます。官公庁をはじめ、金融系などのミッションクリティカルなシステムにも多数採用されている実績のあるクラスタソフトウェアです。これから新規サービスを立ち上げる方だけでなく、オンプレミスのシステムをクラウドへ移行することを検討されている方にも最適なクラスタソフトウェアです。

IaaS の柔軟なシステムで攻めのビジネスを

PaaSのマネージドサービスはシステムの導入・運用負荷を軽減できますが、運用の型化やシステムのライフサイクルの考え方なども含めてみると、必ずしも最適な選択肢とは限りません。確かに IaaS ではミドルウェアの導入・運用負荷は軽減できませんが、オンプレミスで培ったミドルウェアのノウハウを利用し、より柔軟なシステムを構築・運用することができます。
もちろん PaaSのメリットを活かした選択もありますが、ビジネス全体を考慮し IaaS を選択してみてはいかがでしょうか。その際は、これからのビジネスに必要なセキュリティ対策や業務継続性をしっかりと確保することをお勧めします。

2020 年 9 月 10 日