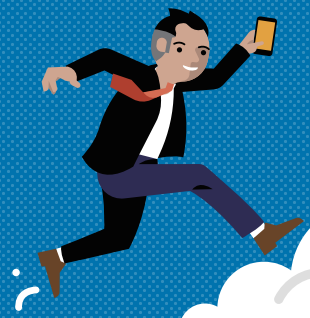
Microsoft

今からでも
間に合う！

これ1冊で クラウドの 「キホン」を理解する

～ 日本を支えるこれからの ICT 活用 ～

- クラウド登場の背景
- クラウドについて
- クラウドの責任範囲とコンプライアンス準拠
- クラウドのサイバー セキュリティ対策
- クラウドの本質的価値
- クラウドの移行方式と選択



情報システムのクラウド化への移行、準備は万全ですか？

本冊子は、
中央省庁や地方自治体で働く皆さまに、
クラウドとは何か、そのメリットや提供形態、
移行方式などについて
分かりやすく解説したガイドブックです。

事業者があらかじめ用意したコンピューティング資源を、
ネットワークを通じてサービスとして利用できる「クラウド」は、
事業者によって用意されたサービスを、必要な時に必要な分だけ利用できるため、
情報システムの構築や準備に時間がかからず、業務の繁忙や、
事業の終了などによる環境の変化に対し、
迅速、柔軟に対応できる仕組みということができます。

政府が情報システムの構築などを行う際に、
クラウド活用を第一として考える「クラウド・バイ・デフォルト原則」
が提唱され、各省庁においても情報システムのクラウドへの移行や新規構築が検討されています。

各省庁は、クラウド環境を含めた外部事業者の環境に保存することができない
機密性の高い情報を有するため、同原則に沿って情報システムの移行、構築を行うのであれば、
既存の環境とクラウドとの併存を前提とした「ハイブリッド クラウド」が現実解となります。

しかし、多くの省庁では、どのシステムを既存の環境に残し、
どのシステムをクラウドに移行すればよいか、
また、どういうクラウドの提供形態を選び、どのように移行シナリオを描けばよいかという
実務上の課題があるのが現状です。

本冊子は、クラウドへの情報システムの移行、構築を成功に導くため、
クラウドとは何か、そのメリットや提供形態、移行方式について解説したもので、
各省庁のあらゆる職位の方に役立つガイドブックです。

クラウド登場の背景

Q これまでの「物理サーバー」の課題って何？

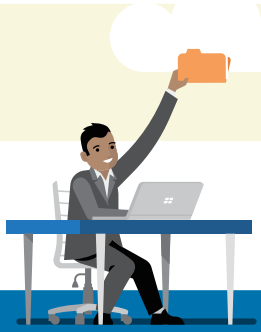
A

物理サーバーの「所有」を前提とした運用には、
設置場所や電源、冷却設備の確保などにコストがかかるうえ、
システム構成にも柔軟性や俊敏性がないなどの課題があります。

これまでの組織の IT システムは、物理サーバー（パソコンが高性能化・大型化し数多くのタスクを同時処理できるマシンのこと）の「所有」を前提にした運用（オンプレミス：自社運用）が行われてきました。
しかし、システムが高機能化、大規模化していくに伴い、物理サーバーの台数も増えていきます。これらを自組織で設置、運用するためには、設置場所（データ センター）の確保が課題となります。また、物理サーバーを安定的に稼働させるには、データセンターの室内を一定の温度に保つ必要があり、電源の確保や冷却のための設備を準備する必要もあります。
これらの初期導入コストに加え、システムの柔軟性や俊敏性にも課題があります。システムの構成は、業務の繁忙期にあわせて設計するため、サーバー資源の多くが使い切れていない状況があり、また、突発的に業務が忙しくなった場合などにも、サーバー資源が自社の設備に依存しているため、急に追加するなどの変更に多くの時間とコストを要するのです。

ここがPOINT

物理サーバーは、調達、設定、構築にコストや時間がかかり、
変更などを柔軟に、スピーディに行うことが難しい！



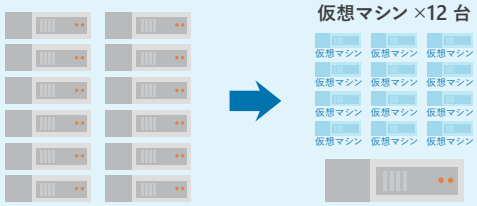
Q「仮想化技術」ってどんなもの？

A

仮想化技術とは、物理サーバーを分割できる「分身の術」。たとえば、1 台の
物理サーバーに、100 台のサーバーがあるかのように運用することができます。

こうした物理サーバーの課題を解決するために登場したのが「仮想化技術」です。仮想化技術とは、物理サーバーを仮想的に分割させる技術で、これにより、1 台の物理サーバーに、100 台のサーバーがあるように仮想的に見せることが可能になります（仮想化技術により、物理サーバーを仮想的に分割させたものを「仮想マシン」といいます）。
いわば、仮想化技術とは「分身の術」ともいうべき技術で、1 つ 1 つの仮想マシンに異なる仕事を割り当てることができるようになり、物理サーバーの台数を減らすことができるようになりました。

仮想化技術とは（イメージ）



ここがPOINT

仮想マシンの登場によって、物理サーバーの台数削減が可能に！
しかし、設置場所や電力、冷却が必要な点や、システム構成、変更が容易でない課題は、
単に物理サーバーを仮想化しただけでは解決しません。

マメ知識 オンプレミスとは？

サーバーやソフトウェアなどの資源（リソース）を、使用者（組織）が所有し、自組織が準備、管理する施設内に設置、運用する自社運用のことです。クラウドが本格的に登場、普及しはじめる 2007 年ごろまでは、オンプレミスが情報システムの一般的な運用形態でした。

クラウドについて

Q クラウドって何？

A

これまでの「所有」を前提とした運用でなく、事業者があらかじめ用意した膨大な仮想マシンなどの IT 資源（リソース）を、ネットワークを通じて必要な分だけ料金を払って「利用」する運用形態です。

クラウドとは、物理サーバーやソフトウェアなどの IT 資源（リソース）を「購入して所有」するのではなく、クラウド事業者が用意した膨大な仮想マシンを、ネットワークを経由して必要な分だけ料金を払って「利用」する形態のこと。これまでの物理サーバーの課題であった、調達や設定、構築にコストや時間がかかり、変更などを柔軟に、スピーディに行えない課題を解決するものです。

利用者（組織）が使いたいときに使える仕組みであるため、データセンターやサーバー ルームなどの準備、投資が不要で、物理サーバーやソフトウェアなどの購入、設置、管理なども不要です。また、業務繁忙期などにサーバー リソースを増やしたいときなどにも、柔軟に、スピーディに変更、増減を行えます。

ここがPOINT

事業者が用意した膨大な仮想マシン等のコンピューティング資源を、使いたいときに、使いたいだけ利用できるもの

Q クラウドの利用を検討する際に重要なことは？

A

物理サーバーやソフトウェアなどのコンピューティング資源やネットワーク、物理的な装置、データ センター敷地、電力などといった、制約概念を捨てることが大事です。

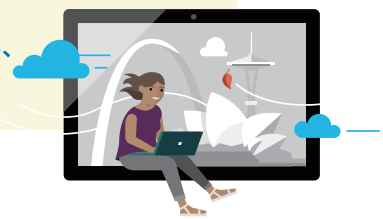
クラウドによって、クラウド事業者が用意したコンピューティング資源を利用したいだけ利用することが可能になります。事業者側では、データ センター敷地やサーバー、ソフトウェア、ネットワークなど、1 利用者では使いきれないほどの膨大なリソースを用意していますので、利用者はコンピューティング資源の不足や、クラウドのネットワーク混雑等を心配する必要はありません。たとえば、企業の IT システムを、店舗運営になぞらえて考えてみましょう。業務閑散期には、店舗を小さくし、スタッフの数を減らして運営する（サーバー リソースを減らす）ことが、管理画面上からスピーディに変更することが可能です。

また、業務繁忙期には、店舗のフロアを拡大し、スタッフの人数を増強する（サーバー リソースを増やす）ことも、簡単に行うことができます。さらに大人数が瞬間的に利用するといった場合にも、たとえば、スタジアムのような大規模施設を、10 分間だけ貸し切るといった対応が可能になります。

さらに大人数が利用するような突発的な状況にも、たとえば、都市そのものを 30 分だけ利用するといった対応を、スピーディに、柔軟に行うことが可能になるのです。

ここがPOINT

「所有」という物理的な制約がないクラウドの世界は、利用者の環境変化に対しても、「利用」した分だけ、時間課金によって柔軟に、スピーディに対応可能！



マメ知識 クラウドの本質は「スピーディ」さにある

クラウドは、決して “新しい” 技術というわけではありません。しかし、これまでの企業 IT の仕組みとはまったく異なるスピードで進化を続けています。たとえば、クラウド サービスの根幹をなす技術のひとつである仮想化技術に関しては、2004 年に EMC Corporation が 6 億 3,500 万ドルで VMware を買収し IT 業界を驚かせたように、2004 年には多くのシステムで仮想化技術を利用する時代を迎えました。その 2 年後の 2006 年には、パブリック クラウドの Amazon Web Services (AWS) がサービス開始しました。また、マイクロソフトが仮想化システム「Hyper-V」をリリースしたのが 2008 年で、わずか 2 年後の 2010 年にはパブリック クラウドの「Microsoft Azure」がサービスを開始しています。このように、仮想化技術登場以降のクラウドの進化のスピードはめざましく、組織には、クラウド技術を活用しながら、環境変化に適応したシステムを開発、運用していくことが求められているのです。

Q データ センターとネットワークは誰が用意するの？

A

クラウドでは、サービスを提供する事業者がデータ センターやハードウェア、ネットワーク機器や事業者のデータ センター間を接続する WAN (Wide Area Network) 網などを用意するため、利用者側ではこれらの準備が不要です。

クラウド事業者は、広大な土地を用意し、床を強化し防犯対策や強固な物理的セキュリティ対策や電源、冷却装置が確保された建屋 (データ センター) を完備しています。そこに膨大な量の物理サーバーをはじめとするハードウェアや仮想化された仮想マシン、ソフトウェア、さらにはネットワーク機器が準備されています。

それらの設置・設定・運用・保守はクラウド事業者が行うため、利用者 (組織) は準備不要ですぐに利用を開始できます。たとえば、Microsoft Azure であれば、グローバルで 60+ リージョン、100 以上のデータ センターを擁し、各データ センター間を接続するネットワーク網も敷設済みです。

クラウド事業者が回線も敷設済

Microsoft の例　データセンター間の帯域として最大 1.6Pbps
大西洋海底ケーブルとして 160Tbps を敷設

- 国内には、東日本・西日本の 2 リージョン
- 東日本と西日本は、マイクロソフトが閉域接続済
- 東日本と西日本で、データのレプリケーションが可能

データセンター間のファイバー
200 万 km

バックボーン
72 TB/秒 以上

Azure リージョン
60+

データセンター
100 以上

サーバー
数百万

ここがPOINT

システム構築に必要となるデータ センター施設や、ハードウェア、ソフトウェア、ネットワークの大部分は、利用者側は準備不要

マメ知識 パブリック クラウドとプライベート クラウドの違い

クラウドには、大きく「パブリック クラウド」「プライベート クラウド」の 2 つの形態があります。パブリック クラウドは、クラウド事業者が用意したサーバーやソフトウェアなどの資源 (リソース) をネットワーク経由で提供するサービスのことで、プライベート クラウドは、仮想マシンなどの資源 (リソース) を提供する基盤を、利用組織の占有環境として利用者自ら準備、もしくはサービス提供を受ける形態のことです。パブリック クラウドで、特定の装置を専有している状態を、プライベート クラウドと呼ぶ場合もあります。

クラウドの責任範囲とコンプライアンス準拠

Q クラウドの提供形態にはどんなものがあるの？

A クラウドのサービス提供形態には大きく「IaaS（イアース）」「PaaS（パース）」「SaaS（サーズ）」の 3 つの種類があります。

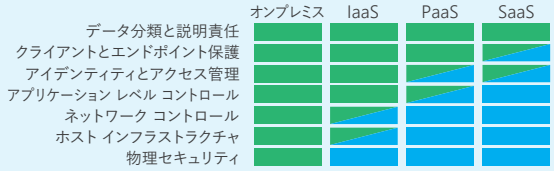
クラウドには、事業者が用意したネットワークやハードウェアなどのインフラストラクチャーが利用できる「IaaS（イアース）」、アプリケーション開発環境やミドルウェアなどのプラットフォームが利用できる「PaaS（パース）」、そして、業務アプリケーションなどのソフトウェアが利用できる「SaaS（サーズ）」の大きく 3 つの提供形態があります。
クラウドの責任範囲を「インフラ管理」「セキュリティ」の両面に着目して整理したのが右図です。
これを見ると、オンプレミスは、すべての要素を利用者である組織が管理する必要があります。そして、クラウド事業者による管理責任の範囲が最も広いのが SaaS であることが分かります。
しかし、SaaS においても、データに関わるガバナンス（分類や説明責任）や、ユーザーが利用する PC などに対するデータ保護（情報漏えい対策）、ID 管理や認証などのセキュリティについては、利用組織側で責任を負うケースがあることに注意が必要です。

責任範囲には 2 種類存在　■ ユーザー管理　■ 事業者管理

① インフラ管理に注目した責任範囲

オンプレミス	インフラストラクチャー (IaaS)	プラットフォーム (PaaS)	ソフトウエア (SaaS)
アプリケーション	アプリケーション	アプリケーション	アプリケーション
データ	データ	データ	データ
ランタイム	ランタイム	ランタイム	ランタイム
ミドルウエア	ミドルウエア	ミドルウエア	ミドルウエア
OS	OS	OS	OS
仮想化	仮想化	仮想化	仮想化
サーバー	サーバー	サーバー	サーバー
ストレージ	ストレージ	ストレージ	ストレージ
ネットワーク	ネットワーク	ネットワーク	ネットワーク

② セキュリティに注目した責任範囲



Q クラウド事業者はコンプライアンス準拠のためにどんな取り組みをしているの？

A クラウド事業者の管理責任範囲に対して、証跡や監査などを通じて第三者機関の“お墨付き”を取得しています。

クラウドを利用する際に「セキュリティが心配」と言われたのは昔の話。クラウド事業者は、管理責任対象となる領域に対して、グローバルや政府、業界、地域ごとに定められたコンプライアンス認証を取得しています。たとえば、データのバックアップやサイバー セキュリティ対策、データの適切な管理やプライバシーへの配慮などについて、正当な第三者機関の証跡や監査を受け、その取り組みについて“お墨付き”を取得しているのです。
たとえば、Microsoft Azure は、さまざまな業界・国ごとの 90 以上のコンプライアンスに準拠しており、あらゆるクラウド サービス プロバイダーの中で最も広範なコンプライアンス カバレッジです。
また、グローバルで定める「ISO 27017」は、クラウド サービスの提供や利用に対して適用される第三者認証のひとつですが、クラウド事業者は、この認証に準拠するため、1,500 を超えるコントロール項目に対応する必要があります。

代表的なコンプライアンス認証

CS ゴールド マーク（日本）／FedRAMP／ISO 27017／ISO 27018／SOC 1, 2, 3／PCI DSS

● マイ ナンバー法（日本）　● FISC（日本）

例）ISO 27017 管理策に含まれるコントロール

- 情報セキュリティのための方針群
- 情報セキュリティの役割及び責任
- 関係当局との連絡
- 資産目録
- 情報のラベル付け
- 利用者登録及び登録削除
- 利用者アクセスの提供
- 特権的アクセス権の管理
- 利用者の秘密認証情報の管理
- 情報へのアクセス制限
- 変更管理
- 容量・能力の管理
- 情報のバックアップ
- イベント ログ取得
- クロックの同期
- 技術的ぜい弱性の管理
- ネットワークの分離
- 情報セキュリティ要求事項の分析及び仕様化
- セキュリティに配慮した開発のための方針
- 供給者との合意におけるセキュリティの取り扱い
- ICT サプライチェーン
- 責任及び手順
- 情報セキュリティ事象の報告
- 証拠の収集
- 適用法令及び契約上の要求事項の特定
- 知的財産権
- 記録の保護
- 暗号化機能に対する規則
- 情報セキュリティの独立したレビュー
- クラウド サービス カスタマの資産の除去
- 仮想コンピューティング環境における分離
- 仮想マシンの要塞化
- 実務管理者の運用のセキュリティ
- クラウド サービスの監視

など

ここがPOINT

大前提としてクラウドを検討すべきですが、特定秘密や極秘文書を扱うために、オンプレミスが候補となる場合もあります。現実には報道されるようなオンプレミスでのセキュリティ事案も発生しています。クラウドに限らずお墨付きはあらゆる検討において考慮する事が大事です。

クラウドのサイバー セキュリティ対策

Q クラウド事業者のサイバー セキュリティ対策は万全なの？

A クラウド事業者は世界規模の膨大なデータをもとに、サイバー セキュリティ対策を行っています。

クラウド事業者は、利用者のセキュリティを守るため、管理責任範囲に対し万全のサイバー セキュリティ対策を行っています。
その一例として、マイクロソフトの Microsoft Azure のセキュリティ対策をご紹介しましょう。マイクロソフトは 2,000 万社以上の企業、10 億人以上のユーザーなど、ビジネス、コンシューマー双方にクラウド サービスを提供しており、これらを通じて世界規模で得られたサイバー攻撃に関する膨大な情報や知見をもとに、サイバー セキュリティ対策を行っています。

世界中の膨大なセキュリティ情報を元にしたセキュリティ対策

地球規模でのセキュリティの知見

年間 **1,100 億円**以上の セキュリティ研究・開発費を投入	**3,500 名**以上のセキュリティ専門家、ビッグデータ・AI を活用した セキュリティ運用の自動化にも 投資を継続	毎月 **10 億台**以上の Windows デバイスが セキュリティ更新を適用
検索エンジンを通じ、毎月 **18 億**以上の Web ページをスキャン	毎月 **4,500 億件**の ユーザー認証を処理	毎月 **4,000 億通**の メールを分析

ここがPOINT

マイクロソフトをはじめとするクラウド事業者のセキュリティ対策は、1 社のセキュリティ対策とは比べものにならない規模で行われており、「クラウドはセキュリティが心配」という常識は過去のものとなっています。

マメ知識 マイクロソフトのセキュリティ対策は「世界最高峰」

- **米国マイクロソフト本社に本部を構え、世界 5 都市にサテライト センターを有する**
  - マルウェア、ボットネット、知的財産 (IP) の窃取などに関連するサイバー犯罪の全般に対応
- **データ センターには機械学習を用いた DDoS/DoS 対策機能を標準で実装**
  - マイクロソフトの全オンラインサービスを防御するため、独自のエンジンで不正なトラフィックを自動検知・遮断
- **最新データをモニタリングし、マルウェアの情報 / 状況を解析**
  - 一日に 5 億件以上のトランザクションをトラックし分析
  - IP アドレス レベルで攻撃元を特定する仕組みも有する
- **全世界のサイバー セキュリティの攻撃状況を分析、情報をセキュリティ関連団体および連邦政府と連携**
  - FBI、インターポール、CERT(Computer Emergency Response Team)、JPCERT、NISC など
- **最新の状況を分析し、すぐにサービスに反映し安全を確保**

マイクロソフトは米国本社に「サイバークライムセンター」を構え、世界 5 都市 (ワシントン、ベルリン、北京、シンガポール、東京) にサテライト センターを有しています。同センターはマルウェア、ボットネット、知的財産の窃取などに関連するサイバー犯罪の全般に対応しています。1 日に 5 億件以上のトランザクションを分析し、マルウェアの情報や全世界のサイバー セキュリティの攻撃状況を分析、これらはセキュリティ関連団体や連邦政府と連携、共有されるとともに、スピーディにサービスに反映され、安全性確保に寄与しています。

クラウドの本質的価値

Q クラウドを利用して IT システムを構築する利点って何？

A

API などによる圧倒的な「機能」の組み合わせによって、容易に、スピーディにシステムを構築できる点がクラウドの本質的な価値です。

国民向けに良いサービスを提供したい、職員が使いやすいシステムを作りたいというときに、ゼロから構築するのではなく、すでに完成したシステムがあり、盛り込むべき機能や要件のすべてが実現できるならば、それが最善の選択肢となるでしょう。または、ゼロから作るにしても、新規で構築すべき範囲（費用）が最小であれば、容易に、スピーディにサービス（システム）を公開することが可能になるはずです。

たとえば、EC サイトであれば、ユーザー登録やログイン、商品検索やショッピング カート、支払い（決済）といった、さまざまな「機能」の組み合わせによって構成されていることがわかります。

クラウドは、API（Application Programming Interface）というソフトウェア同士を連携させる仕組みを通じて、たとえば、仮想マシンやディスク、ストレージやネットワーク、データベース、メールやファイル サーバー、人工知能（AI）や認証など、必要となる「機能」が提供されています。

つまり、あらゆる機能が「部品」として提供されているため、ユーザー側で新規に開発する範囲を最小限に抑えることができ、クラウド事業者が用意した機能を組み合わせるだけでシステムを構築することができるのです。

さらに、これらの「機能」は日々追加されており、クラウド事業者 1 社で、1 年に 1,000 以上の機能が API を通じて公開されています。

圧倒的な数の機能 API（日々増加）＝ クラウド

EC サイト例

ユーザー系	商品系	支払い系	検索系	etc
機能 A (API)	機能 A (API)	機能 A (API)	機能 A (API)	機能 A (API)
機能 B (API)	機能 B (API)	機能 B (API)	機能 B (API)	機能 B (API)
機能 C (API)	機能 C (API)	機能 C (API)	機能 C (API)	機能 C (API)
機能 D (API)	機能 D (API)	機能 D (API)	機能 D (API)	機能 D (API)
機能 E (API)	機能 E (API)	機能 E (API)	機能 E (API)	機能 E (API)

クラウド（既に機能 /API の提供事業者に意味はない点に注目）

仮想マシン	ストレージ	ネットワーク	DB	AI	E-Mail	共有 File Server
機能 A (API)	機能 A (API)	機能 A (API)	機能 A (API)	機能 A (API)	機能 A (API)	機能 A (API)
機能 B (API)	機能 B (API)	機能 B (API)	機能 B (API)	機能 B (API)	機能 B (API)	機能 B (API)
機能 C (API)	機能 C (API)	機能 C (API)	機能 C (API)	機能 C (API)	機能 C (API)	機能 C (API)
機能 D (API)	機能 D (API)	機能 D (API)	機能 D (API)	機能 D (API)	機能 D (API)	機能 D (API)
機能 E (API)	機能 E (API)	機能 E (API)	機能 E (API)	機能 E (API)	機能 E (API)	機能 E (API)

日々拡張
1 社で 1,000+ / 年

クラウド事業者が複数あり、
日々機能が追加される世界

ここが POINT

クラウドを用いる最大の利点の一つは、膨大な「機能」を API などを通じて利用できること。
これらを組み合わせることで、新たなシステムを容易に、スピーディに構築することが可能です。

Q どのクラウドベンダーを選んだらよいの？

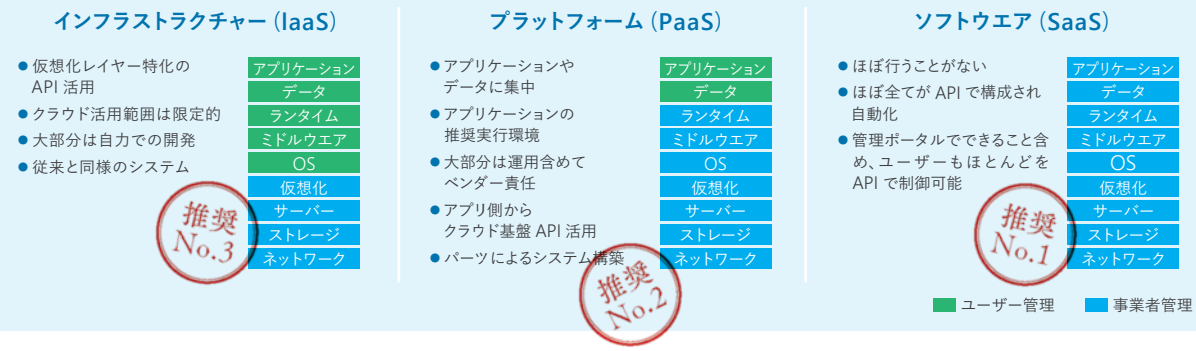
A

クラウドは、どの事業者が公開している API であっても連携は可能なので、コンプライアンス認証に準拠した事業者のサービスを選択するとよいでしょう。

クラウドでは、どの事業者が提供している機能 (API) であっても、その API が別システムからも利用されることを前提としていれば、連携することができます。つまり、どのベンダーが提供するサービスかは重要な問題ではありません。そこで、利用するクラウド サービスを選ぶ際は、自組織の要件に合致したコンプライアンス認定に準拠したサービスを選択するとよいでしょう。

ただし、API でさまざまなクラウド事業者の機能を連携させてシステムを構築する場合には、クラウドのサービス提供形態によって、クラウド事業者側の管理責任範囲が異なることに注意が必要です。「IaaS (イアース)」「PaaS (パース)」「SaaS (サーズ)」の 3 つの提供形態ごとに責任範囲が異なることに留意しましょう (P6 参照)。

クラウドは膨大な数の API の組み合わせ



ここがPOINT

クラウドは、API を通じ、事業者を越えて「機能」を連携させることが可能です。
既存のオンプレミスのシステムとクラウドの共存を前提にした「ハイブリッド クラウド」や、複数のクラウド事業者のサービスを組み合わせる「マルチ クラウド」は当然の選択です。

Q ベンダー ロックイン (特定のベンダーに大きく依存した状態) が起きないようにするにはどうしたらよいの？

A

ベンダー ロックインを回避するには、データのポータビリティ (可搬性) が保たれていることが大事です。

事業者間で「機能」の連携性が保たれたクラウドにおいて、何がベンダー ロックインを生じさせる要因になるでしょうか。それは「データ」です。
クラウドに IT システムを構築 (移行) すると、クラウド事業者のデータ センターにデータを預けることになります。たとえば、「データがエクスポートできない」「他のシステムで扱えない」ということになれば、特定のベンダーに大きく依存した状態となってしまいます。
クラウドの利用に際して、ベンダー ロックインを回避し、ハイブリッド クラウド、マルチ クラウドを実現するには、データのポータビリティが保たれていることが重要なのです。

ここがPOINT

ハイブリッド クラウド、マルチ クラウドを実現するには、データのポータビリティが最も重要！
必要な時に自組織が預けた必要なデータのすべてを取り出せる状態を保つことが大事です。

クラウドの移行方式と選択

Q クラウドへの移行にはどんな方式があるの？

A クラウドへの移行方式には、大きく 7 つの選択肢があります。

既存のシステムをクラウドへ移行する場合の移行方式には大きく次の 7 つの選択肢があります。現実には、コストや時間の制約があることや、データの機密性などからクラウドに移行してはならないシステムがあることを考慮する必要があります。

システムの検討、現在の選択肢は？ コストや時間の制約等を無視すれば、以下の選択肢が存在

1 Retire（リタイア）
統廃合で別のシステムに集約する、あるいは、集約せずに廃棄することです。

2 Replace（リプレース）
SaaS で提供される業務アプリケーションなどに置き換えることです。
たとえば、メールやチャット、ビデオ会議、ファイル共有などの機能を Microsoft 365 に置き換えることなどです。

3 Rehost / Lift & Shift（リホスト / リフト アンド シフト）
システムはそのままに、環境をクラウド上に移行することです。たとえば、オンプレミスで VMware や Hyper-V で仮想化された環境を、Microsoft Azure などの IaaS（仮想マシン）上に移行することなどです。

4 Refactor（リファクター）
ソース コードも含め、システムを部分的に改修し、クラウドに移行することです。
PaaS の活用や、コンテナと呼ばれる新しい仮想化技術を用い、アプリケーション実行環境を構築することなどです。

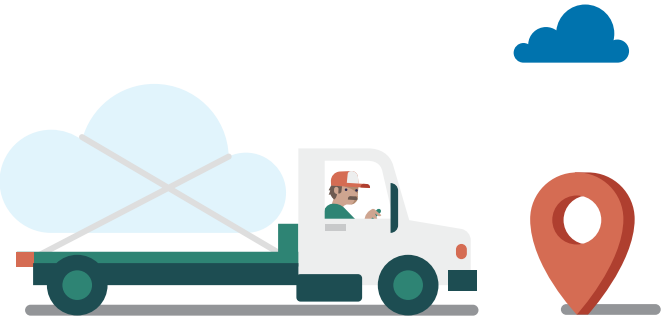
5 Rearchitect（リアーキテクト）
クラウド ネイティブの考え方やクラウド機能を前提に新機能追加などのシステム改修を行うことです。

6 Rebuild（リビルド）
クラウドが提供する機能を活用し、一からシステムを構築することです。

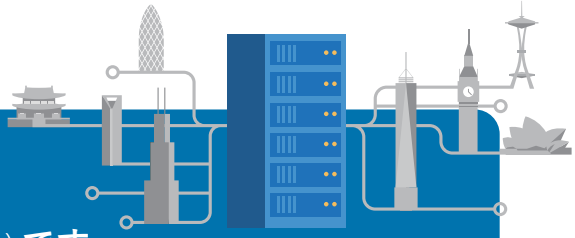
7 Retain（リテイン）
システムをオンプレミスに残留させたり、オンプレミスに構築します。1 年後に廃棄予定なので保守延長でクラウド移行はしないシステムや、極秘文書等がありオンプレミスで保存する必要があるシステムなどです。

ここがPOINT

**システム更新におけるクラウド移行の選択肢には大きく 7 つあります。
たとえば、既存のシステムを「廃棄」する場合にも、PaaS などを利用し、
一から開発するシナリオがありますし、SaaS に置き換えるシナリオもあります。**

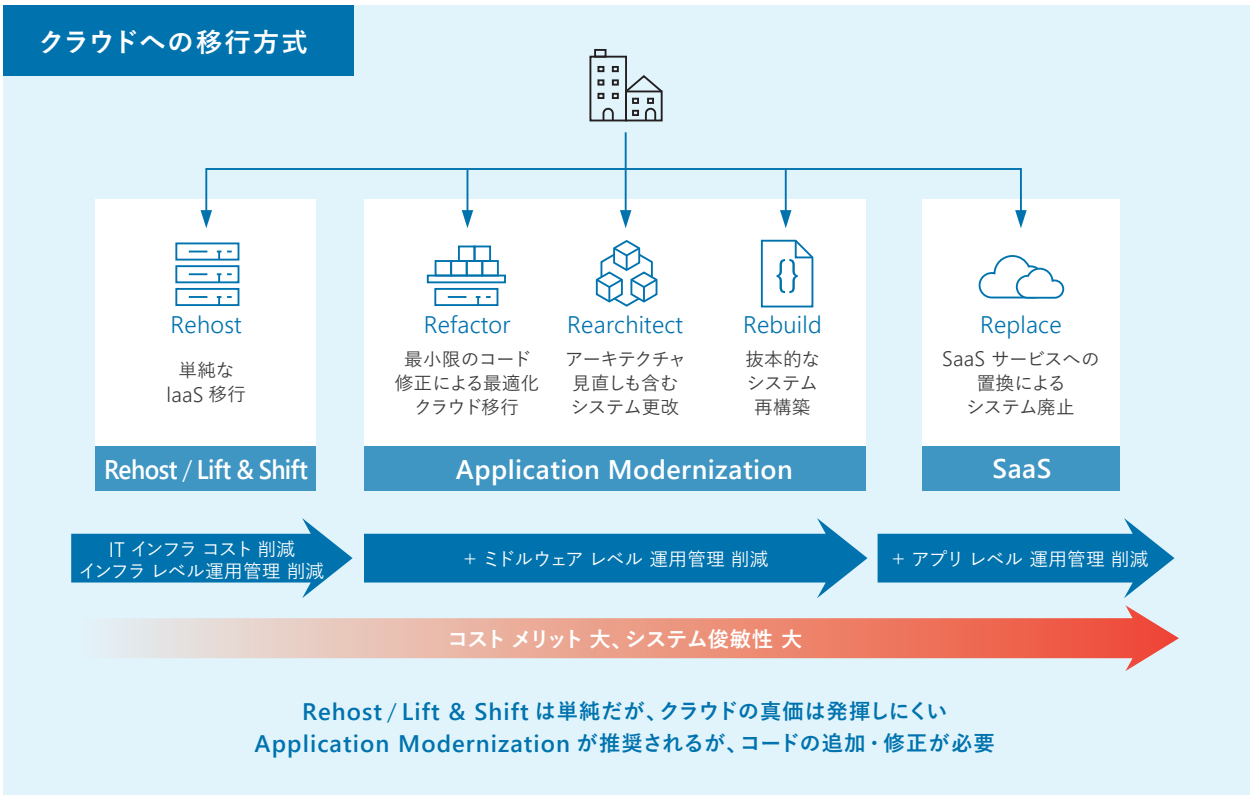


Q 7 つの移行方式のメリット、デメリットを教えて。



A もっともコスト メリットが高く システムの俊敏性が高いのが SaaS 化（Replace）です。

7 つの移行方式をコスト メリット、俊敏性をもとに分類したのが下図です。これによると、SaaS (Replace)、PaaS (Refactor / Rearchitect / Rebuild)、IaaS (Rehost) の順に、クラウドのメリットが発揮しやすいと言えます。



すなわち、SaaS を利用することで、すでに「完成品」として提供されるアプリケーションへ置き換えることが、最もコスト メリットが高く、システムの俊敏性も高いです。しかし、SaaS 化の場合、既存システムの機能を、そのまま SaaS で実現することが難しいケースがあることに注意が必要です。

次にコスト メリットや俊敏性などが発揮しやすいのが、PaaS やコンテナ活用によるモダナイゼーションです。これらの移行方式も推奨されますが、システムによっては、コード追加や修正が必要で、難易度が高い点に考慮が必要です。

そして、IaaS、特に仮想マシンへの移行は、既存のシステムはそのままに、インフラだけの移行となるため、移行作業はシンプルですが、クラウドの真価は発揮しにくいデメリットがあります。

ここがPOINT

Replace による SaaS 利用がもっとも推奨されるクラウド活用です。しかし、自組織の既存システムのすべての機能を、そのまま SaaS へ移行するのは、現実的には難しい場合もあります。
SaaS ➡ PaaS ➡ IaaS の順で検討しましょう。

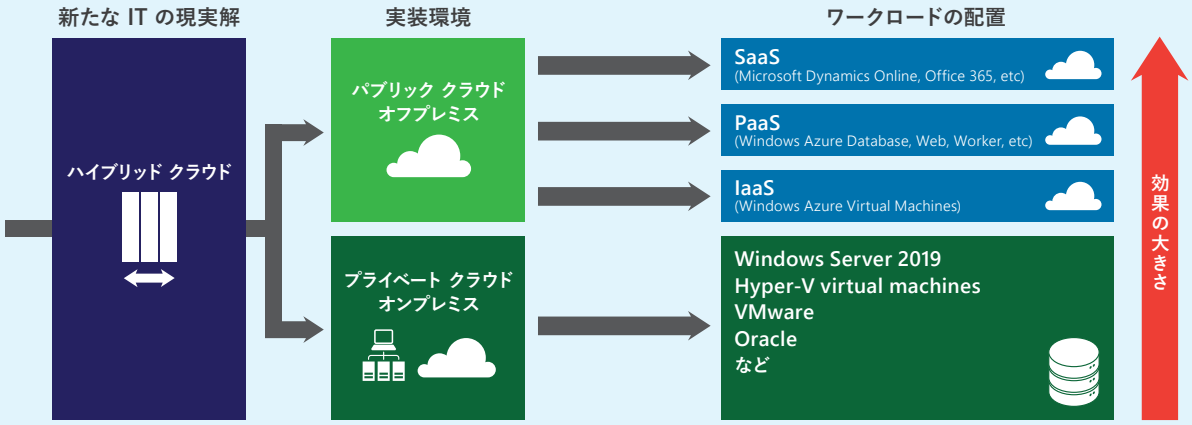
最後にもう1つ

ここがPOINT

クラウド移行のシナリオは「あるべき姿」を考慮しよう

「政府情報システムにおけるクラウド サービスの利用に係る基本方針」によれば、特定秘密及び行政文書の管理に関するガイドラインに掲げる秘密文書のうち、極秘文書に該当するデータはパブリック クラウドでは扱わないとされています。すなわち、システム更新を検討する際には、大部分はクラウドで検討し、クラウド利用ができないものはオンプレミスのシステムを検討する、オンプレミスとクラウドの共存を前提にした「ハイブリッド クラウド」が現実解となるでしょう。

オンプレミスも選択肢に追加すると　どう判断すればいいか？ あるべき姿をまず思い描く



オンプレミスもシナリオの選択肢に追加すると、まずは「完成品」のシステムを利用する SaaS 化が可能かどうか、あるいは利用しようとするクラウド事業者がコンプライアンスに準拠しているかといったポイントを考慮することが大事です。また、技術的な難易度や検討項目の多さだけで判断するのではなく、対象となるシステムや業務を将来どうしたいか、どうなっているのが理想かを前提に検討することも重要です。

その上で、自組織の文化なども考慮に入れ、クラウド活用をどのように進めるかの方針を決めるのがよいでしょう。

本リーフレットついてのお問い合わせ

Microsoft
日本マイクロソフト株式会社
〒108-0075 東京都港区港南 2-16-3 品川グランドセントラルタワー
6328-IP1