

クラウド戦略で陥る6つの失敗

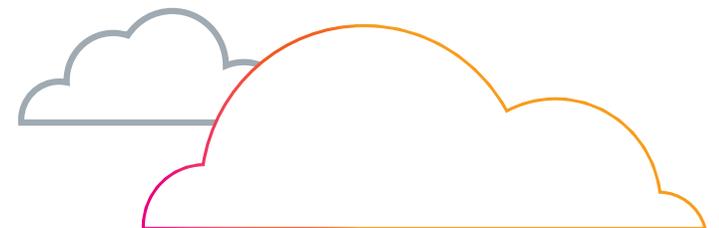
失敗を回避し、確実なクラウドデータ戦略がなければ
クラウドの最大の利点も弱点に

ほぼすべての業界の企業が、オンプレミスのレガシーデータセンターから脱却し、ワークロードとデータをクラウドへ移行しています。その目的は、急速に進化する従業員と顧客のニーズおよび期待に応えるために、コストを最適化して新しいソリューションを提供することです。そのためにクラウド戦略を構築し、マルチクラウド環境とクラウドネイティブなアプリケーションの導入を通じて、テクノロジースタックの最新化を目指しています。

クラウドがもたらすであろうメリットは多様かつ多大です。たとえば、コストの節約、イノベーションの向上および加速、市場動向や競争圧力への俊敏な対応を実現できます。老舗企業でさえも「デジタルファースト」になっており、顧客の期待に応えるためにテクノロジーに多額の投資をしなければなりません。このような投資は、新興デジタル企業がひしめく競争の激しい市場、そして不安定な経済を生き抜くためには必要不可欠です。

あらゆるテクノロジーと同様に、クラウドにも困難やリスクが伴います。また、クラウド戦略のメリットが期待どおりに得られないだけでなく、カスタマーエクスペリエンス全体が脅かされる恐れもあります。クラウドから価値を最大限に引き出す重要な鍵となるのは、複雑化するアプリケーションと関連インフラをどこまで効果的に管理できるかという点です。クラウドベースのシステムからは膨大なデータが生み出されます。これを適切に管理および分析できてはじめて、クラウド戦略により期待どおりの価値を手に入れることができます。

ここまでの成功を実現するには、クラウドの導入にあたって陥りやすい失敗の回避方法を把握しておく必要があります。Splunkでは、特に大きな6つのリスクを明らかにしました。クラウド導入を成功へ導くために、ぜひこのガイドをお役立てください。



クラウドの利点と陥りやすい失敗

失敗1：コストの肥大化

クラウドの利点の1つとしてよく挙げられるのは、コスト削減と資本コストから運用コストへの予算の移行です。しかし、コストを適切に管理できなければ、クラウドサービスの経費はたちまち制御不能になります。

利点

クラウドテクノロジーの大きな利点の1つは、アプリケーションを利用するための投資方法の転換です。固定額の資本支出から、使用状況と直接連動する運用支出へと移行します。多くのIT部門では、調達の際に長いリードタイムが発生し、高額な固定コストもかかっています。そのため、IaaSやPaaSといったソリューションは魅力的な選択肢となります。クラウドを活用すれば、需要に合わせて運用を拡大および縮小でき、ニーズとコストを正確に連動させることができます。

陥りやすい失敗

使った分だけ支払う従量課金制はオンプレミスのインフラ戦略よりもコスト効率が向上する可能性があります。計画が不十分でクラウド環境を適切に監視できなければ、たちまちコストが増加して抑制できなくなります。最大の問題はタイトの場合、使用しているクラウドのインスタンスやサービスに対する可視性の不足に起因しています。多くの企業では、個別のグループがそれぞれ独自のクラウド環境を調達して管理できる状況にあります。このような戦略を使用すれば、各スタッフや各部署が独自の裁量で実際に試してニーズに合った環境を構築できますが、それは同時に、監視が大幅に欠如する恐れもあります。サービスの過剰なプロビジョニング、使われないライセンス、クラウドサーバーの無駄な重複などはすべて、コストを押し上げます。実際に2019年には、アイドル状態のクラウドリソースや過剰なプロビジョニングにより、**クラウド支出の3分の1が無駄になっています**。さらには、多くの企業が複数のクラウドプロバイダーを利用しています。

故意にそうしている場合もあれば成り行きの場合もありますが、ワークロード単位でのコストの比較を困難にしています。何に対して投資しているか見極めるだけでなく、その投資からどのような価値を引き出しているかを把握するのが難しいケースは少なくありません。

データ戦略

クラウド戦略ではデータ戦略を構築することが重要です。ROIを最大限に引き出し、計画した予算にクラウドコストを収めるためには、クラウドへの投資を正確に予測および監視しなければなりません。クラウドサービスのコスト管理全体を一元化することで、コストが増加して抑制できなくなる前に、非効率的なジョブや、重複しているワークロードなど、無駄な経費を把握できるようになります。また、複雑さが増しているシステムの障害点とその発生原因を理解するために重要になるのが、オブザーバビリティのための機能です。オブザーバビリティをもたらす適切なプラットフォームがあれば、クラウドサービスが使用されている場所を問わず、使用状況のレポートを標準化して統合できます。つまり、1つ1つのクラウドアプリケーション導入をビジネス上の個別の意思決定として扱えば、各グループの自主性を維持しながらも、クラウドの請求書を見て驚くようなこともありません。

失敗2：イノベーションの加速と安定性におけるトレードオフ

クラウドネイティブなDevOpsのベストプラクティスを採り入れると、イノベーションとトランスフォーメーションを加速させることができますが、新たな障害が生まれる可能性もあります。

利点

従来のオンプレミスのデータセンター環境では、主に一定の予算サイクルによってインフラに関する決定が行われます。たとえば、一般的な予算策定の範囲外でハードウェアやソフトウェアリソースの追加を必要とする新しい計画が持ち上がった場合、それらのリソースに必要なインフラを用意できるまでその計画を進めることができません。その結果、イノベーションが鈍化し、競争力が損なわれます。しかし、クラウドならインフラとサービスを速やかに増強できるため、イノベーションに迅速に対応できます。

陥りやすい失敗

アジャイル開発やDevOpsの手法を採り入れると、モノリシックなアプリケーションを低頻度でリリースしていたのが、分散型のクラウドネイティブなアプリケーションを高頻度でリリースするようになります。複雑性が増すことで、管理が難しくなる可能性があります。なぜなら、複雑な依存関係を持つ分散設計のクラウドネイティブなアプリケーションには、より多くの障害点があるからです。また、こうした新しいクラウドアプリケーションの多くでは既存のバックエンドシステムも関連しており、これらに依存しているため、サービスデリバリーのパイプラインが複雑化します。このような環境のトラブルシューティングは、早々に手に負えなくなります。実際に、最近の[レポート](#)によると、「開発者は年間

6.2億時間をソフトウェア障害のデバッグに費やしている」ことが明らかになりました。つまり、エンタープライズソフトウェア市場では、テストの失敗によるコストが年間610億ドルに上る計算になります。そして、可視性を確保せずに移行を急げば、安定性が損なわれ、クラウドの導入も進まなくなります。

データ戦略

サービスやアプリケーションの新たなアーキテクチャを導入すると、そこから生じる新たなデータストリームも取得できるようになります。サーバーレス関数やマイクロサービスなどのソースから生じるこうした新しいデータストリームは、クラウド環境で起きる問題に答えをもたらす可能性を秘めています。すべてのクラウドプラットフォームと、依存関係のあるレガシーシステムにおいて、すべてのデータを観測可能にすることが重要です。先にも述べましたが、重要なのはオブザーバビリティです。すべてのデータをもとに、今起きていることをリアルタイムに把握して理解できなければ、運用において適切な対策を講じることはできません。目標は「既知の確定要素」だけでなく、「未知の不確定要素」も把握して監視できるようにすることです。これを適切に行えれば、問題の根本原因を迅速に究明しながら、期待どおりの迅速な導入、スケーラビリティの向上、ビジネスプロセスの全体的な効率向上を実現し、迅速性と安定性を両立できます。

 **以前は可視性が不足しており、迅速に対応することができませんでした。しかし、Splunkのおかげで製品や機能をスピーディーに開発し、確実かつ迅速にリリースできるようになりました”**

—Arlo社、クラウドプラットフォームエンジニアリング担当VP、Jishnu Kinwar氏

[Arlo社の事例を読む](#)

失敗3：セキュリティ戦略が欠如したクラウド戦略の立案

クラウドベンダーは世界トップクラスのセキュリティ体制を敷いています。しかし、クラウドネイティブなソリューションとDevOpsは「スピードと現状打破」を推進するものであり、セキュリティが優先されないこともあります。

利点

認証取得済みのクラウドベンダーはセキュリティチェックに合格しているため、セキュリティ部門は開発やインフラが必要なときに安心して速やかに承認できます。クラウドベンダーは独自に厳格なコンプライアンス要件を満たしています。また、その規模を生かしたセキュリティ部門への投資力は、先進的な大企業を超えるほどです。クラウドベンダーは、データがどのように保存および処理されているかを可視化するツールも提供しています。インフラのセキュリティに費やす時間と費用を削減できるため、クラウドへ移行すれば、コスト削減と価値の迅速な実現にもつながります。

陥りやすい失敗

安全なプラットフォームでも、適切に管理されていなければ意味がありません。[Gartner社](#)は次のように述べています。「問題はクラウド自体のセキュリティにあるのではなく、セキュリティの**ポリシー**やテクノロジーと、そのテクノロジーの制御にあります。ほぼすべてのケースにおいて、組織のデータを保護するための管理に失敗しているのは、クラウドプロバイダーではなくユーザーです。そのためCIOは、クラウドが安全かどうかではなく、クラウドを安全に使用しているかどうかを問題にしていかなければなりません」

クラウドは実際に強固なセキュリティを備えています。データの保存および処理に対して可視性もありますが、ある程度の不透明さも持ち合わせています。そのため、この不透明さに加えて攻撃対象が広がることで、セキュリティ体制全体が脆弱になる恐れがあります。また、企業のデータが複数のクラウドと自社のデータセンターに分散されるようになり、セキュリティを理解して統制することがますます難しくなります。そして、各部署がデジタル化を急ぎ、自分たちの要件を満たすのに注力するあまり、一般的なセキュリティ要件を見過ごすことがあります。これらすべてが全体的なリスクの増加につながります。特にネットワーク制御、アクセス管理システム、構成オプションに精通していない場合は深刻です。では、誰がこのようなリスクを管理すべきでしょうか。誰もリスクを管理していなければ、どのような事態に陥るのでしょうか。

データ戦略

強力なクラウドセキュリティ戦略の基盤になるのは、強固なクラウドデータ戦略です。これらの戦略により、データの統制を維持しながら、しかるべき従業員がセキュリティリスク管理を行えるようになります。この戦略の適用対象には、従来のセキュリティとの関連性が高い一般的な運用データだけでなく、顧客およびビジネスの機密データも含まれます。クラウド戦略とセキュリティ戦略は連携させて進めなければなりません。そうすることで協調的な取り組みが可能になり、ビジネスニーズを満たしながら、別々のデジタル化プロジェクトに取り組むさまざまな部署の垣根を越えてセキュリティ管理を行うことができます。また、各部署が一元化されたプラットフォームを使用し、アプリケーションの種類を問わず、さまざまな場所で発生した問題を特定して解決できるようにする必要があります。ベストプラクティスは、データプラットフォームを調達して利用することです。そうすれば、統一されたクラウドセキュリティ対策に基づく体制を敷くことができ、マルチクラウド環境全体のすべてのデータ管理において可視性が得られます。



```
0100 101010011001001010  
000110110101 001 0100110  
10101 01001011011011  
0011010101010101110100
```



REI社 最大のメリットは、境界の保護によるものです。おかげで、パブリック環境に接触するエンドポイントのための境界保護モデルを開発チームが個々に開発する必要がなくなりました”

—REI社、インフラおよびクラウドサービス担当マネージャー、David Bell氏

[REI社の事例を読む](#)

失敗4：統合アプローチを備えていないツールの導入

クラウドソリューションには専用の管理ツールがあり、そのプロバイダーのサービス環境向けに最適化されています。しかし、ほかのプロバイダーや既存のIT管理ツールについて考慮されていません。

利点

クラウドはコストを節約できるよう設計されているため、オンプレミスのレガシーなツールおよびアプリケーションに依存する必要がなくなります。選択したクラウドプラットフォームに備わっているツールを使用すれば管理全体の負担が軽減されるため、IT部門やセキュリティ部門はビジネスのほかの業務に注力できるようになり、時間の節約と経費の削減が可能になります。

陥りやすい失敗

ベンダー専用のクラウドベース管理ツールの場合、マルチクラウド環境を想定した互換性を備えていることはまずありません。そのため、一般的な企業では本格的にクラウドを導入するうちに、レガシーテクノロジーに多かれ少なかれ依存していることに気づき、その欠落を埋めようとし始めます。この状況に陥ると、既存のツールセットの操作により多くの時間を浪費し、クラウドに備わっている機能をトランスフォーメーションに十分に活用できなくなります。さらに、こうしたレガシーツールではクラウドで実行できる最新のアプリケーションアーキテクチャをサポートしていないため、問題などが発生しても正確に認識できなかったり、その認識が分かれたりすることがあります。最終的には、運用に対する可視性が低下し、対応に時間がかかるようになります。その結果、ダウンタイムが増加し、パフォーマンスの問題が頻発し、全体的にリスクが高まります。

データ戦略

必要なのは競争力を保てるツールですが、そのためには既存インフラにも対応した包括的なアプローチが不可欠です。適切なクラウドデータ戦略では、新旧の環境の統合を軸として、1つのデータプラットフォームで全体を把握できるようにする必要があります。コンテキストの中で企業のさまざまなクラウドサービスのあらゆる側面を継続的に分析するためには、AIや機械学習だけでなく回復力の高い機能も必要です。既存のレガシーツールが使用される可能性がある場合は、特に重要です。そうすることではじめて、技術面およびビジネス面のさまざまな問題の特定、分類、予測、自己修復を実際に自動化して、問題が大きくなるのを未然に防ぐことができます。直面している問題だけに対処したり、古いテクノロジーで最新の問題を解決しようとしているのであれば、そこから脱却することではじめて、本当の意味で組織のモダナイズに取り組めるようになります。

失敗5：ツールの増やし過ぎ

クラウドベースのポイントソリューションは数多くあります。成り行きに任せていると、そのうちにすべてのサブスクリプションを購入しているかもしれません。

利点

クラウドテクノロジーへの投資を本格的に始めると、企業の感覚は容易に「クラウド最優先」から「クラウド一択」へと変化します。ビジネスでどのような問題が発生しても、その問題を解決できるクラウドベースのソリューションがあり、必要に応じていつでも別のソリューションに乗り換えられます。さまざまなクラウドベースのアプリケーションやサービスを導入すれば、IT運用の改善から、セキュリティ体制の向上、さらにはビジネスモデル自体の改善まで、何にでも取り組めるようになります。

陥りやすい失敗

実際にあらゆる目的のクラウドソリューションが存在しますが、1つですべてに対応できるソリューションはありません。包括的な監視およびオペラビリティの戦略を採り入れなければ、クラウドサービスの健全性や可用性に関する透明性の確保が難しくなります。たとえば、各部署で自分たちが理想とするポイントソリューションを自由に入手できる状況では、すぐにサイロ化やデータの急増が発生する恐れがあります。これらを管理する包括的な計画がなければ、アナリストは急速に増え続けるデータとアラートへの対応を

余儀なくされるでしょう。結果的に、クラウドテクノロジーを導入することで、より複雑でコストのかかる環境が生まれ、監視も難しくなります。会社としても各部署としても多くのツールに手を出し過ぎたことで、効果的な管理ができなくなる恐れがあります。

データ戦略

単一の一元化された方法で各業務を把握できるデータプラットフォームを用意したうえで、各スタッフや各部署に自分たちのニーズを定義してもらうことが、組織としての運用方針の鍵となります。そのプラットフォームを使用して、複数の外部プラットフォームに接続できるだけでなく、IT、セキュリティ、DevOpsなど、さまざまな部門が1つの画面で可視性を確保し、それに基づいて行動できるようにする必要があります。一元化された管理プラットフォームを使用すれば、加速しながら増え続けるデータを観測および管理できます。そして、クラウドソリューションのうち、どれが有効でどれが不要かをよりの確に判断できるようになります。目標は、オンプレミスでもクラウドでもインフラの無駄をなくすことです。同じような役割を果たす複数のソリューションによりテクノロジースタックが肥大化して、全体的な複雑さに拍車をかけることがないようにします。

Splunkの導入前は、ばらばらな方法でログが作成されていました。統一性に欠けていたため、包括的な視点を持つのが困難だったのです。Splunkを使い続けるうちに、Splunkこそがより広い問題に対応できる解決策だと確信するようになりました”

—Mars社、セキュリティ分析シニアリーダー、Antonio Guedes氏

[Mars社の事例を読む](#)

失敗6：データの価値を引き出しきれない

データが大量に生成されていても、それを有効活用してアクションにつなげられなければ、データがもたらす機会を逃してしまいます。

利点

クラウドテクノロジーを活用すれば、多様なやり取りをデジタル化し、新しい方法でアプリケーションを開発して、より多くのデータを取得できます。取得したデータを適切に利用すれば革新がもたらされ、それまでビジネスに生かせていなかった豊富なインサイトが得られるだけでなく、カスタマーエンゲージメントの強化、従業員の生産性向上、アップタイムの改善、運用の合理化が可能になります。データの使用に重点を置く企業は、データ活用の結果、年間売上が平均5.32%増加していることがSplunkとESG社の調査で明らかになっています。

陥りやすい失敗

データがあっても、はじめから価値があるわけではありません。データを処理し、分析し、理解することで、その価値を実現できます。企業で生じる膨大なデータが**ダークデータ**（未活用か未発見のデータ）のまま放置されています。クラウドを中心としたシステムでは大量のデータが生成されますが、多くの企業は、それを効果的かつ効率的に活用する力を持っていません。そのようなケースではデジタルトランスフォーメーションは成功

せず、データエコシステムがさらに複雑化し、コストに見合う価値を生み出すことができません。データから価値を引き出す戦略がなく、情報が複数のシステム間で散乱およびサイロ化すれば、大きな機会コストが生じます。

データ戦略

社内のデータを明確に理解しなければ、デジタル化を進めることはできません。いわゆる「ダークデータ」は技術系とビジネス系の両方のシステムで生成されます。必要なときに社内で使用できるよう、整理して、一元的にアクセスできるようにしておく必要があります。ダークデータを効果的に活用すれば、サービス中断への対応の迅速化から、顧客に対するサービス内容の向上まで、さまざまな改善が見込めます。このダークデータのソースとしては、モバイルアプリやマイクロサービス、新たに接続されたモバイルPOSなどのシステム、クラウド監視ツール、新たなシステム統合などがあります。こうしたデータフィードをリアルタイムで生かせるプラットフォームを利用することで、クラウドの導入を適切に進めることができます。

細かいところまで目が行き届くようになりました。保安検査場の任意の個所に注目し、そのパフォーマンスを完全に把握することもできます。データをもとに、「昨日よりも定時到着率を向上させるには?」、「赤字の原因は?」といった問いを検証できます。

—ガトウィック空港、IT開発スペシャリスト、Alex Webber氏、Paul Bannister氏

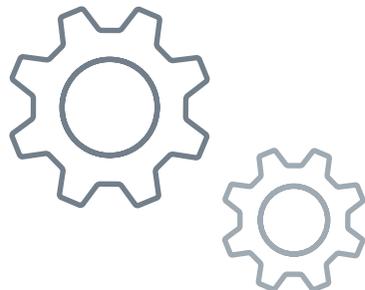
[ガトウィック空港の事例を読む](#)

スマートなクラウド戦略に不可欠な Data-to-Everythingプラットフォーム

クラウドネイティブな組織になることは、必ずしも成功への近道ではありません。経費の肥大化、管理の複雑化、データによる過剰負荷を回避したいならば、事前に考えておくべき重要な課題があります。クラウド導入を長期的な成功に導く重要なポイントの1つは、マルチクラウドから、センサーデータ、顧客とのやり取りに至るまで、多様なデータソースすべてに対し、組織の重要な関係者たちが速やかにアクセスおよび観測できるようにすることです。

これは簡単なことではなく、実現するためには適切なプラットフォームが不可欠です。Data-to-Everythingプラットフォームを提供するSplunkは、クラウド導入のあらゆるステージのニーズに応えます。情報がオンプレミスのデータセンターにあっても、パブリックまたはプライベートのクラウドプラットフォームにあっても、もしくは自社で開発および管理する業務アプリケーションにあっても、Splunkならば対応可能です。広範なデータに対するリアルタイムのアクセス、強力な分析、自動でのデータ収集を

行えるため、重要なビジネスデータを瞬時にインデックス化することも、設定変更が可能なアラートで問題が起こりそうなところへ注意を喚起することもできます。企業のモダナイズとクラウドネイティブなアーキテクチャの導入が進む中で、Splunkのようなプラットフォームは運用の復元性の中核となり、インフラ、アセット、データから本当のメリットを得るために重要な役割を果たします。クラウドの導入で陥りやすい失敗を回避するには、最適なデータプラットフォームが必須です。このようなプラットフォームを使用することで、真の革新性を発揮するための強力なデータバックボーンを築くことができます。





**この6つの失敗に速やかに対処しなければなりません。
Splunk Cloudを活用して調査、監視、分析を行い
適切なアクションにつなげましょう。**

[詳細はこちら](#)

© 2020 Splunk Inc. 無断複写・転載を禁じます。Splunk, Splunk>, Data-to-Everything, D2EおよびTurn Data Into Doingは、米国およびその他の国におけるSplunk Inc.の商標または登録商標です。他のすべてのブランド名、製品名、もしくは商標は、それぞれの所有者に帰属します。

20-14077-SPLK-6-Cloud-Strategy-Pitfalls-How-to-Avoid-Them-LS-JA-202009

splunk>
turn data into doing™