NUTANIX

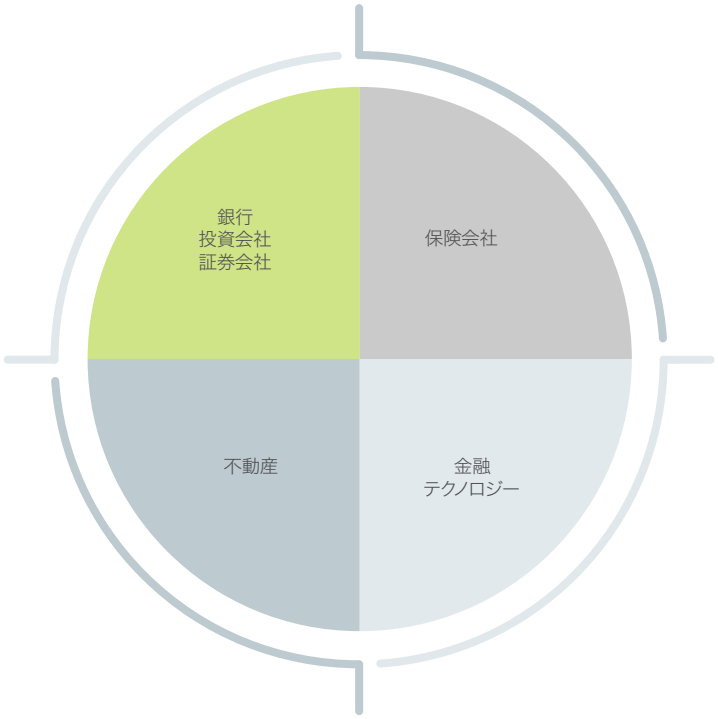
完全ガイド

金融サービスIT

金融サービス企業は、フィンテックとデジタルテクノロジーが発達したこの時代にあって、DevOpsやクラウド化に進むためにIT戦略の先鋭化を図り、多層防御を備えた上で、持続的な競争優位性を確保する必要があります。

本書について

このデジタル時代において、新規参入のみならず、従来から存在する金融サービス機関でさえ、わずか数年前には想像もできなかったような業務課題に直面しています。このような課題を解決できるかどうかは、最新の情報テクノロジー（IT）の強みを十分に活かせる能力を持ち合わせているかどうかにかかっています。



本書は、ITテクノロジーやIT戦略における、最も切迫した課題に関連する最新情報を提供できるよう構成されています。各章では、1つのトピックを掘り下げながら、以下のような点における金融サービス機関の在り方について解説します。

- データセンターのインフラストラクチャーの最新化と、オンプレミスおよびクラウドを両立させる方法
- 多層防御の導入
- アジャイルな方法論の採用による開発・テストチームの先鋭化
- ITと組織構造の大幅な見直し

最終章では、金融サービス企業がどのようにNutanix Enterprise Cloudを活用しながら、テクノロジー上の課題に対応しているかという点について解説します。

01

クラウドと金融サービス

「2008年に発生した金融危機以降、あらゆる状況が不安定なままになっています。問題は、大手銀行の対応が間違っているというよりも、これらの組織における対応の限界や、既存顧客がすぐ簡単に利用でき、優れたエクスペリエンスを低コストで提供する新興の金融サービスに流れて行ってしまっていることです」

– FINTECH, OPEN SOURCE, AND EMERGING MARKETS– FINTECH, OPEN SOURCE, AND EMERGING MARKETS

デジタルトランスフォーメーションは、他のどんな業界にも増して、金融サービス業界 (FSI) に大きな影響を与えています。そして、金融サービステクノロジー（フィンテック）が、従来のビジネスの在り方を大きく変革しています。銀行や保険会社から投資管理会社に至るまで、金融サービス企業は、より迅速に対応できなければ取り残されてしまうというリスクに晒されています。モバイル取引をはじめとする最近のテクノロジー革命が、顧客の期待値を高め、金融サービスの在り方を変革する要因になっています。オンライン、モバイル、店頭など、あらゆるチャネルを通じてシームレスなエクスペリエンスを提供できることが不可欠となっています。

あらゆる業態の金融機関が、以下に示すような業務やテクノロジーに関わる様々な要件に対応する必要に迫られています：

- デジタル化を見据えたクラウドへの投資
- 包括的なサイバーセキュリティ対応
- 人工知能の採用や自動化の促進
- ブロックチェーンなど、急速に広まる公開管理元帳への対応

FSI企業は、これまで他のどんな業界と比べても引けを取らないほど、その収益の多くを情報テクノロジー（IT）に投資していきましたが、業界アナリストによれば、IT予算をさらに5%上乗せしなければならない情勢となってきています。最先端を行く金融機関の多くは、オンプレミスのデータセンターの変革やクラウド戦略に磨きをかけるため、巨額の投資を続けることでしょう。次世代アプリケーションを構築し、ユーザーの満足度をさらに向上させると共に、何年にも渡って業務を支えてきた従来のアプリケーションを維持していくためには、適切なクラウド環境を構築することが必要になります。

クラウドの情勢は急速に変化し続けています。このため、様々なアプリケーション要件を満たし、セキュリティを確保して持続的な改革を行っていく最善の戦略を決定したり、先々まで業務の柔軟性を阻害しないようなインフラストラクチャーを選択することは、決して容易ではありません。

本書は、クラウドをはじめとするITインフラストラクチャーに対する皆様の理解を深め、よりインテリジェントな選択を行っていただけるようにすることを意図してまとめたものです。特に後半の章では、サイバーセキュリティにとって重要な領域や、新しいデジタルサービスの成功に必要な組織改革などについても言及しています。

クラウドに関する理解

規制やその他の懸念事項によって、金融サービス企業全体では、パブリッククラウドやクラウドサービスプロバイダーよりも、むしろオンプレミスのインフラストラクチャーやホストテッドIT、あるいはプライベートクラウドを好む傾向がありました。しかし今や、既存金融機関の多くが、クラウドに「飛び移り」、俊敏性の向上を図ったり、効果的なデジタルサービスを提供する必要があると考えています。

クラウドの進化は非常に早いため、業務要件を満たすことができる選択肢を調査する前に、用語の定義をはっきりさせておきたいと思います。

プライベートクラウド

ITチームは、セルフサービスポータルを使ったクラウドライクなサービスを、プライベートクラウドから提供することができます。このようなサービスは、パブリッククラウドが提供するものに類似していますが、ハードウェアの計画や管理に対する責任は依然としてIT部門に残ります。このような形態は、ITaaS（IT as a Service）と呼ばれることもあります。プライベートクラウドには、幾つかのパターンがあります：

- 仮想プライベートクラウド：外部のクラウドサービスプロバイダーがクラウド環境をパーティション分けし、特定の企業が専用に利用できるようにしたもの。

- ホステッド・プライベートクラウド： プライベートクラウドに関する一切の運用や管理を、サービスプロバイダーに一任する形でアウトソースしたもの。

パブリッククラウド

パブリッククラウドは、Amazon Web Serivices（AWS）、Google Cloud Platform（GCP）、Microsoft Azureなど、外部の企業がハードウェアを抽象化したインターフェースを通じてクラウドサービスを提供するもので、これによって利用者側は、ハードウェア計画などを配慮に入れる必要がなくなります。課金は利用量ベースで行われ、運用経費扱いとなります。多くのパブリッククラウドは、IaaS (Infrastructure as a Service) という形態を取っています。

規制の厳しい業界に属するFSI企業は、一般的にパブリッククラウドでアプリーションを稼動させることにためらいを感じてきました。しかしパブリッククラウドによる、セキュリティや規制対応、さらにFSIにとって最も重要な懸案事項であるデータ統治要件へのより優れた対応が可能になってくるにつれ、このような状況にも変化が見られるようになってきました。

クラウドサービスプロバイダー

大手のパブリッククラウドプロバイダーと、拡大を続けるクラウドサービスプロバイダー（CSP）は、分離して考えることが重要です。CSPは、独自の要件にも対応できるきめ細かなサービスの提供が可能です。FSI企業のニーズへの対応に特化したり、それを主要業務とするCSPも数多く存在します。

クラウドサービスプロバイダー

厳密な定義では、ハイブリッドクラウドサービスは、CSPやプライベートクラウドと、パブリッククラウドなど、異なるクラウドを組み合わせて利用する形態を指します。例えば、3層のアプリケーションスタックの場合、プレゼンテーションサービスをパブリッククラウドに、アプリケーションサービスをマネージド・プライベートクラウドに、そしてデータベースサービスをオンプレミスに配置するといった形態が可能です。

マルチクラウド

マルチクラウドは、ITニーズに対応するために、複数の異なるプライベートやパブリック、さらにハイブリッドクラウドを組み合わせて利用するクラウド戦略です。マルチクラウドが一般的になるにつれて、複数の異なるクラウドの効率的な管理や、アプリケーションのポータビリティの確保が新たな課題になってきています。

エンタープライズクラウド

エンタープライズクラウドは、企業固有のニーズに応えると共に、広範なワークロードの要件にも対応できるよう設計されたものです。エンタープライズクラウドには、以下が含まれます：

- 従来型のアプリケーション。
  クラウド環境では、従来の業務アプリケーションに適応できないケースがあり、大幅なコード変更が必要になる場合もあります。

- 次世代アプリケーション
  「クラウドネイティブ」なアプリケーションと呼ばれるもので、当初からクラウド環境で稼動するよう設計されたものです。

- エンドユーザーコンピューティング
  多くのFSI企業が、仮想デスクトップ（VDI）によって、顧客データのセキュリティやITの効率化が図れることを認識するようになっています。

クラウドで成功するためには

FSIのITチームが、進化し続けるクラウド環境を成功裏に導入するためには、注意深くその対応にあたる必要があります。最近のIDCのデータによれば、典型的な企業は、現在そのIT機能の約60%をオンプレミスで、40%をクラウドで稼動させています。2021年には、その比率が50:50になるだろうと予測されています。従って、オンプレミスとクラウドでの運用を上手く両立させる必要が出てきます。

このためには、オンプレミス、プライベートクラウド、CSPあるいは大手のパブリッククラウドなど、どのアプリケーションやサービスをどのクラウドで稼動させるかという明確な決定プロセスが必要になります。また業務の半分はオンプレミス側に残るため、データセンターのインフラストラクチャーを、クラウドライクな俊敏性を提供できる環境に転換させる必要があります。

クラウド環境のスマートな選択

どのクラウドモデルを使用するかは、以下のような様々な要因によって決まります：

- **価格.** 特定のサービスを事業経費（OpEx）としたり、資本支出（CapEx）としたり、さらにその組み合わせとして扱いたいと考える場合もあるでしょう。OpExの場合には、ユーティリティの価格設定を含め、様々な費用モデルに対応することができます。

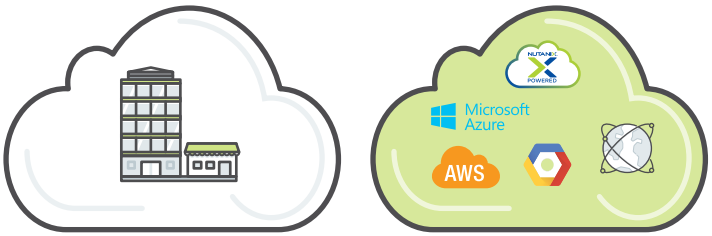
- **弾力性.** 一部のアプリケーションは、使用状況に応じて拡張や縮小が可能でなければなりません。このような拡張や縮小に向け、四半期末の処理に必要な能力などを見越すことはできますが、予期しない状況の発生による、新たなトランザクションの急増などは予測することができません。

- **セキュリティ、コンプライアンス、データ統制.** 実際の業務内容や業務の遂行場所に関わりなく、データ統制関連法に従ってデータを決まった場所に保存するなど、非常に多くの規則に従って業務を進める必要があります。クラウド環境の決定にあたっては、このような点も考慮に入れる必要があります。

- **独自のアプリケーション要件.** NoSQLデータベース、コンテナ、マイクロサービスなどを利用するクラウドネイティブなアプリケーションを構築している場合、このような要件をサポートできるインフラストラクチャーが必要になります。既存のデータセンターは、現在必要とされる様々な要件を満たし、サポートできるようにはなっていない場合があります。このため、求められる機能を追加するか、外部のプロバーダーを利用する必要があるということです。

- **アプリケーション開発の要件.** FSI企業がイノベーションを加速するためには、ソフトウェア開発においても新しいアジャイルなモデルを採用する必要があります。アジャイル開発では、セルフサービスや自動化の採用などが原則となります。

最も重要でパフォーマンス要件の厳しいアプリケーションに対しては、オンプレミスやプライベートクラウドを選択することが良いとされますが、クラウドプロバイダーの場合には、弾力的な拡張性が求められるクラウドネイティブなアプリケーションに対応することが可能です。



オンプレミスプライベートクラウド
予測可能でセキュア
パフォーマンスセンシティブ
ミッションクリティカル

サービスプロバイダーのパブリッククラウド
拡張性に優れ弾力的
クラウドネイティブなアプリケーション
企業IT、ホステッド

図1. アプリケーションの配置場所をよりスマートに決定する

最終的な目標は、アプリケーションを最適に配置し、それぞれのアプリケーションやサービスに最善となるアプリケーションスタックの提供に時間と資金を集中し、優れたカスタマーエクスペリエンスを提供することです。

個別のアプリケーションを検討する前に、何を達成したいのかという戦略的な視点で考えることが重要です。アプリケーションを稼動させる場所の決定に影響を与える、全ての要因を網羅したクラウド選定マトリックスを作成してください。

例えば：

- アプリケーションはコンテナ化可能か？
- アプリーションは弾力的なリソースの拡大や縮小が可能か、それとも定常的か？
- I/Oのパターンは？安定的か、変動的か、 高いのか低いのか？
- アプリケーションは垂直方向に拡大するのか、それとも水平方向か？

- 時間が経つにつれ、アプリケーションがコントロール不能になったり、際限なくリソースを消費するようにならないか？
- アプリケーションが他のアプリケーションのエコシステムに依存していないか？
- アプリケーションにおいて、厳しいコンプライアンス対応やデータ統制要件がないか？
- アプリケーションが停止した場合、業務に及ぼす影響は？

適切なクラウド選定マトリックスが完成したら、次にそれを使って個別のアプリケーションを評価することができます。

データセンターの変革

データセンター業務の中核に位置する従来のインフラストラクチャーは、非常に複雑で、運用コストも極めて高く、アプリケーションを特定のクラウドから別のクラウドに移すことは、困難または不可能と言えるでしょう。

データセンター業務の中核に位置する従来のインフラストラクチャーは、非常に複雑で、運用コストも極めて高く、アプリケーションを特定のクラウドから別のクラウドに移すことは、困難または不可能と言えるでしょう。運用業務からこれらの問題を取り除かない限り、デジタルトランスフォーメーションを完遂することはできず、業務目標の達成についても困難なままとなります。それでは、クラウド時代のニーズに応えるには、データセンターのインフラストラクチャーとして、どんな機能が必要となるのでしょうか？「必須項目」一覧では、以下の要素を慎重に評価する必要があります：

- **ソフトウェアデファインド.** サイロ化した専用のインフラストラクチャーや、サーバー、ストレージ、ネットワークコンポーネントを物理的に構成する方法は、既に過去のものです。
- **ハイパーコンバージド.** 従来のデータセンターのインフラストラクチャーは、Webスケールなアーキテクチャーをベースに、サーバー、ストレージ、ネットワークを統合したハイパーコンバージドインフラストラクチャー（HCI）に置き換えられつつあります。適切なHCIを導入することによって、企業が必要とする全てのタイプのワークロードを処理できるようになります。
- **容易な管理性能.** ITの成功にとって、管理の複雑さが大きな障害となっています。単一の管理インターフェースで、インフラストラクチャーからアプリケーションの導入に至るまで、全てをコントロールできることが求められます。

- **容易な自動化.** 運用効率の向上や担当者の負担軽減、さらに手作業での誤った設定によるエラーの発生を防止するためには、自動化が最善の手段となります。

- **セルフサービス機能.** セルフサービスによってITニーズを満たし、開発チームや業務担当者の生産性を向上させ、市場投入まで時間を短縮して、ITリソースの節減を図ることができます。

- **アプリケーションおよびVM単位での対応.** スナップショットやレプリケーション、クローニングといったデータ処理を、VMやコンテナなどのアプリケーションと同じきめ細かさで実施できる必要があります。

- **組み込み済みの保護機能.** データ保護やディザスタリカバリ（DR）機能は、本来データセンターが提供すべきものであり、他に依存したり別に管理すべきものではありません。

- **分散とエッジ機能.** 企業は、以前にも増して業務の現場に近いセカンダリおよびエッジロケーションにインフラストラクチャーを配備し、データをローカルで収集して処理するという必要に迫られています。

- **本質的なマルチクラウド対応.** スマートな企業は、オンプレミスでの運用と複数のクラウドプロバイダーで稼動するアプリケーションおよびサービスを組み合わせて利用しています。皆様のデータセンターのインフラストラクチャーも、ハイブリッドな運用モデルを採用すべきです。

クラウドの時代において、ITサービスに対する期待値は根本から変わりました。開発チームやITサービスを利用する社内や社外の利用者は、パブリッククラウドが提供する俊敏性や拡張性を求めています。

次世代のインフラストラクチャーを構築する際には、レガシーなアーキテクチャーの先を見据えた、クラウドに対抗できるデータセンターを作り上げる必要があります。それでは、この新しいITスタックとはどのようなもので、最新のイノベーションをどうやってデータセンターで活用し、どんなクラウド戦略を実行に移せばよいのでしょうか？その答えとなるのは、エンタープライズクラウドによって重要なリソースに対するコントロールを失うことなく、パブリッククラウドのような俊敏性を提供できると考える金融サービス企業がますます増えているという事実です。

02

金融サービスにおけるサイバーセキュリティ

金融サービスは、世界的に見ても最も規制の厳しい業界と言えますが、それには相応の理由があります。米国だけで、金融機関を対象にした法律や規制が無数と言えるほど存在します。例えば、グラム・リーチ・ブライリー法（GLBA）や、サーベンス・オクスリー法（SOX）、PCIデータセキュリティスタンダード（PCI DSS）、ドッド＝フランク・ウォール街改革・消費者保護法などが良く知られています。

個人を特定することが可能な情報（PII）のエクスポージャー拡大に対応する、新たな規制も増え続けています。また欧州では、EU一般データ保護規則（GDPR、補足記事参照）が、2018年5月より施行され、世界の企業に大きな影響を与えています。

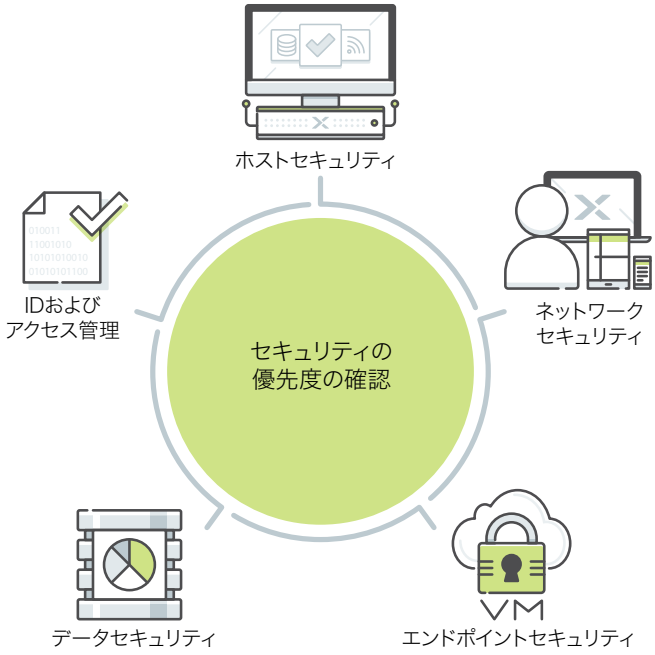
しかし残念なことに、これらの規制要件に従うことと、優れたセキュリティを担保することは全く別の話なのです。大手の消費者信用報告会社が被害を受け、広く報道されているような攻撃がますます増えています。Financial Threats Review 2017によれば、金融機関を標的とする攻撃や、それによる金銭的被害額は、2016年から2017年にかけても増え続け、止まる気配を見せません。

金融サービス企業がデジタルトランスフォーメーションを加速させるにつれ、プライベートクラウドによるオンプレミスか、サービスプロバイダーか、あるいはパブリッククラウドかを問わず、あらゆるアプリケーションやサービスにおいて、サイバーセキュリティが重要な懸案事項となってきています。

GDPRへの準備はできていますか？

欧州連合（EU）は、市民の個人データを保護するためのフレームワークを導入しました。EU一般データ保護規則（GDPR）は、データ保護の強化と統一を目指したものです。GDPRは、2018年5月25日に施行されました。

これは、機密性の高い個人データやID、遺伝子や生体情報、さらに匿名データといった個人情報を自身でコントロールできるという意味で、EUの市民にとって前向きな一歩となっています。GDPRは、企業における業務の在り方を変革しています。GDPRは、EUに拠点を置く企業だけでなく、EUの市民に帰属するデータを取り扱う全ての企業に対して適用されます。もしITチームが、まだGDPRへの準備ができていない状況であれば、本書はその着手のための最適な手引きとなるはずです。



セキュリティの優先度の確認

サイバーセキュリティの成功には、5つの幅広い分野での継続的な対応が必要です。

- サーバーへの攻撃に対する防御力を高めるために**ホストセキュリティ**を強化
- 企業のファイアウォールによって、外部および内部からの侵入を防ぎ、**ネットワークセキュリティ**を確保
- 企業ネットワークの内部や企業のリソースにリモートからアクセスすることが可能な、増加し続けるエンドユーザーデバイスなどを保護し、**エンドポイントセキュリティ**を確保
- 安全なキー管理による強力な暗号化によって重要なデータを保護し、**データセキュリティ**を確保
- ホスト、ネットワーク、エンドポイントの組み合わせや、アクセスコントロールを使ったデータ保護機能によって、アプリケーションや情報へのアクセスを制限する**IDやアクセス管理**機能を実装

ホストセキュリティ

対象環境が、物理、仮想、オンプレミスあるいはクラウドのいずれであっても、数十あるいは数百ものサーバーのセキュリティを管理することは、決して容易ではありません。ホストやVMのセキュリティ確保にあたっては、様々な対応が必要になります：

- 必要なポートだけをオープンし、必要なサービスだけを稼動させて、アクセスをコントロール
- マルウェアやウィルスのスキャン
- 全てのセキュリティや関連する管理イベントのロギングと監視
- データの暗号化
- データ保護の実施

1台のホストにおいて、ただ1つの見落としや設定ミスがあるだけで、サイバーセキュリティの攻撃対象となる脆弱性を発生させることになります。

ネットワークセキュリティ

これまでネットワークセキュリティと言えば、高度なファイアウォールを使用して、企業ネットワークを外部の侵入から守ることを意味していました。しかし、金融サービスのデータセンターの場合には、仮想マシン間で発生する非常に多くのトラフィックもこれに含まれる状態になっています。これは、従来のデータセンターを出入りする「垂直方向（north-south）」のトラフィックパターンと比較し、「水平方向（east-west traffic）」のトラフィックと呼ばれています。

このような内部のフローは、境界線セキュリティで捉えて監視することが出来ないため、保護においてギャップが生じることになります。異常なパターンや異常値を特定するためには、ネットワークトラフィック全体の可視化が必要となります。さらに、それぞれのアプリケーションやサービス、グループが定められた境界線内に確実に止まるようにするためには、マイクロセグメンテーションが必要になります。

エンドポイントセキュリティ

エンドポイントのセキュリティ対象には、エンドユーザー（従業員と顧客）がネットワークやアプリケーション、そしてサービスにアクセスするためのエッジデバイスやデバイスセットが含まれます。エンドポイントのセキュリティの重要性は、商用クラウドアプリケーションの導入や、BYODの普及、自宅やリモートでの業務実施ニーズなどの拡大などに伴い、ここ数年でさらに高まってきています。今やエンドポイントは、サイバー犯罪者が好んで標的とする侵入口になっています。

エンドポイントのセキュリティを強化するためには、従業員のデバイスを常にアップデートし、フィシングやマルウェア攻撃から保護することが重要です。従来のデスクトップデバイスの管理でさえ面倒な作業となることを考えれば、デバイスの持ち込みは、とても厄介な問題なのです。

デスクトップやアプリケーションの仮想化ソリューションを導入して、エンドユーザーのエンドポイントにおけるセキュリティに対応しようという、一歩進んだ金融サービス機関も増えています。このようなテクノロジーによって、デスクトップやエンドユーザーアプリケーションを、ソフトウェア環境やアクセスをコントロールできるデータセンター内でホストすることが可能となります。データへのアクセスや確認は可能ですが、ローカルデバイスに保存されることがないため、個人を特定することが可能な情報（PII）をリスクに晒す機会を減らすことができます。

データセキュリティ

サイバーセキュリティの最終的な目的は、不正なアクセスの防止や、価値ある情報の盗難を避けることです。そのため、暗号化は最初で最後の防衛線となります。全てのPIIが、暗号化された状態で保存および転送される必要があります。セキュリティを確保し、データが適切な認証を受けた場合にのみアクセスできること保証するためには、堅固なキー管理が必要になります。

IDおよびアクセス管理

IDおよびアクセス管理（IAM）は、アクセス認証を受けたユーザーだけが、サービスや情報にアクセスできるようにするためのプロセスであり、それ以上でもそれ以下でもありません。問題は、顧客や従業員に煩わしさを感じさせずに、不正利用者を締め出すIAM手法を構築できるかどうかにあります。多くの金融サービス機関は、2要素認証とデバイス認証を組み合わせることで、顧客に多くのストレスを与えることなく、アクセスにおけるセキュティ向上を図っています。

セキュリティ自動化の重要性

大規模なIT運用では、あらゆる局面での大幅な自動化なくして、セキュリティ対策が上手くいくことは望めません。

- 手作業によるセキュリティ設定では、必ず人的ミスが発生し、それが攻撃の標的となる脆弱性を発生させる要因となります。適切なセキュリティ設定は、自動的に行われる必要があります。

- セキュリティ設定を行ったシステムやソフトウェアが、事前定義したセキュリティ設定から乖離していないことを確認できる必要があります。乖離があればそれを特定し、自動的に修正できなければなりません。

- 高度なデータ侵害手段では、修正が可能にもかかわらずパッチが適用されていない既知の脆弱性を狙い撃ちします。新しい脆弱性が見つかったシステムやソフトウェアに、最小限の時間差でパッチを適用するようなプロセスを実装する必要があります。

セキュリティ要件が特に厳しい環境に対するセキュリティの設定や監査を容易にすることを目的に、複数の組織が立ち上げられています。Center for Internet Security（CIS）は、「サイバー攻撃防御のためのベストプラクティス・ソリューションの定義、開発、検証、促進および維持」を目的とした組織です。CIS Benchmarksは、ITシステムセキュリティのための基準とベストプラクティスを提供します。米国国防総省（DoD）では、主要なオペレーティングシステムやソフトウェア向けに、セキュリティ技術導入ガイド（STIGs：Security Technical Implementation Guides）を策定しました。一般的にSTIGsは、CISベンチマークよりも厳しい内容となっています。CISベンチマークとSTIGsは、セキュリティ自動化や監査の基礎となるものですが、それ自体が自動化機能を提供するものではありません。

より優れたセキュリティの選定

言うまでもなく、金融サービスのITチームは、セキュリティを最優先事項として意思決定を行う必要があります。セキュリティを真剣に考慮に入れているベンダーやパートナーを選択します。当初からセキュリティ機能を考慮に入れて設計せず、ソリューションを補完するために後付けで対応する形では、セキュリティを確保することができません。

クラウド時代では、セキュリティ機能が前面に現れないとしても、インフラストラクチャーに完全に統合されている必要があります。セキュリティ機能が製品文化として組み込まれ、セキュリティが製品開発に不可欠な要素になってこそ、金融サービス企業の厳しい要件に対応することができるのです。また、インフラストラクチャーのセキュリティ維持に向け、広範な自動化機能が取り入れられることで、リスクを低減しながらシームレスな拡張を行うことが可能となります。

ブロックチェーンとは?
ブロックチェーンをご存知の方なら、ビットコインにおける暗号化通貨としての役割も理解されていることでしょう。ビットコインをどう考えるかは別にして、FSI企業がブロックチェーンに注目し、導入を行っていることには相応の理由があります。最近のHarvard Business Reviewの記事では、このテクノロジーについて次のように説明しています:

ブロックチェーンは、二者間の取引を効率的かつ検証可能で永続的に記録できるオープンな分散型の台帳です。台帳それ自体が、自動的に取引を発生させるようにプログラミングすることもできます。ブロックチェーンを使用することで、取引データにデジタルコードを埋め込み、削除、改ざん、変更が不可能な透過的で共有可能なデータベースに格納することができます。これによって、全ての取引や処理、タスク、そして支払にデジタルレコードと署名が付与され、それぞれを特定し、検証、保存、共有することができるようになります。法律家や銀行のような仲介者は、もはや不要になります。個人、組織、機械、そしてアルゴリズムが相互に妨害し合うことなく、自由に取引を行うことができます。
– HARVARD BUSINESS REVIEW


NODE 01
NODE 04
NODE 05
NODE 03
BLOCK 01
BLOCK 01
NODE 01
NODE 02

03

DevOpsと金融サービス

「金融サービス機関は、大きな課題に直面しています...
その多くは、オンライン化に取り組むことなく、現在のデジタル世代をサポートするために、バックエンドのプロセスやシステムの近代化に注力してきました。レガシーなシステムやコードに加え、セキュリティや規制に対するコンプライアンスの強化やガバナンス要件への対応といった課題を抱え、これら全てがソフトウェア改革を複雑で遅々として進まないものにしているのです。そう思われませんか」
– TECHBEACON

今現、在金融サービス業界に最も影響を与えているのが、金融テクノロジーあるいはフィンテックと呼ばれる存在です。フィンテックの新興企業が、2017年だけで170億ドルもの資金をベンチャーキャピタルから調達しており、銀行や資本市場企業といった既存の金融サービス機関もフィンテックが創出するメリットを追い求めています。

暗号化通貨やブロックチェーン（補足説明参照）という言葉が、著名な報道の一面を飾る一方で、フィンテックでは、次のようなテクノロジーを採用しています：

- 個人と企業間の支払をシンプル化する合理的なペイメントテクノロジー
- FSI企業の規制やコンプライアンス対応を支援するRegTech
- 保険市場の効率改善のためのInstruTech
- アルゴリズムとAIを使って投資アドバイスを提供するRobo-Advisor
- 複数の金融機関から提供されたデータを、サードパーティーのアプリを使って集約・分析するためのAPIを備えたオープンバンキング
- 売り手と買い手の契約を、コンピューターを使って迅速かつ容易に実行する、スマートコントラクト (Smart Contract)
- 企業や個人（特に以前の金融市場では投資を受けることができなかった）が資本市場にアクセスするための新たな手段を提供する、クラウドファンディングとマイクロ投資 (Microinvesting)

前述のように、既存の金融サービス企業は、新興のフィンテック企業に追い着けるよう動いており、自社の改革を進めています。DevOpsは、FSI企業が直面する問題を解決するソリューションと成る得るものです。Electric CloudのCEO、Steve Broodie氏は、TechBeaconに次のように書いています：

金融サービス業界は、まだ時流に追い着いていないどころか、アジャイルや継続的デリバリ（CD: Continuous Delivery）、DevOpsといった最新の手法を使ったデリバリのスピードアップやイノベーションへの取り組みを開始したばかりです。

この保守的な業界のエグゼクティブは、DevOpsがより迅速かつ効率的に、そして安全な形で市場に価値を提供するための手段だと考えています。金融サービスは、DevOpsによってアプリケーションのリリース頻度や品質を高められるだけでなく、ガバナンス、リスク、セキュリティ、コンプライアンスといった戦略にも対応できるようになります。

デジタルトランスフォーメーションとフィンテックは、金融サービスのITチームや開発チームをDevOpsモデルへと誘導する、かつてないほどのビジネス変化をもたらしています。

DEVOPSとは

DevOpsは、開発と運用チーム間のギャップを埋め、両者の摩擦を取り除いて、新しい機能やサービスの提供を加速するために、ITの文化やテクノロジーを変革する手法です。

従来のエンジニアリングチームやツールは、それぞれがサイロ化され、非生産的な状態が続いてきました。「自分のラップトップでは動く」「それは自分の問題ではない」あるいは「私はやらない」といった言葉が現れたら、それはDevOpsを必要とするサインです。長期的なリリースサイクル、リリース期限を守れない運用、低品質な製品等は、DevOpsを導入すべき、さらなるサインと言えるでしょう。

DevOpsは、組織間のギャップを埋め、内部や外部の利用者により優れた価値を提供します。DevOpsによって責任範囲の厳密な区分を取り払い、コラボレーションや自動化を可能にすることで、以下のようなメリットを創出します：

- 迅速なリリース. ソースコードのチェックインから顧客へのリリース、そして実際の利用に至るまで、ソフトウェアのテストやリリースを自動化して、その提供を加速化することができます。

- フェールファストとフィックスファスト. 自動導入（および復帰）戦略によって、リスクを低減しながらリリースの短縮化を図ることができます。

- クローズドループの設計とテスト. 全ての変更は学習や実験の機会であり、全てのギャップや誤りはテスト、実装、自動化を改善するための機会となります。自動運用によって、システムを監視して修正を促すことができるようになります。

アプリケーションの開発、導入、利用において実際に起っていることを確認し、システム全体をより効果的かつ効率的にして、無駄を省く方法を明らかにします。
– INFORMATION WEEK.
DEVOPSに移行するための8つのステップ

- アクセスやセルフサービスの民主化. 開発やテスト環境を、開発者やテスト担当者、そして運用担当者がアドホックに構築できるようにします。

既に説明したように、セキュリティやコンプライアンス対応にあたっては、自動化が重要となります。高度な自動化を実現することで、DevOpsによって、開発に費やす努力をより確実に製品に結び付けることができます。

インフラストラクチャーとDEVOPS

DevOpsプロセスでは、インフラストラクチャーにおけるアジリティ（俊敏性）が重要になります。開発と運用の統合がどこまで進んでいるかに関わらず、インフラストラクチャーが果たす役割は大きなものです。適切なインフラストラクチャーによって、目標の達成が遙かに容易なものになります。

オンプレミスを担当するIT部門からの応答の遅さに耐えかねて、開発チームがパブリッククラウドに移行してしまう場合もあります。しかしこのような対応は、複雑な事態を発生させることにも繋がりかねません。

- アプリケーションをクラウド上で開発しても、稼動させるオンプレミスの環境は異なります。従来型の多くのアプリケーションはクラウドで稼動するようには設計されておらず、仮に動いた場合でも、それは満足できる状態ではありません。

- ITチームが、データセキュリティを直接コントロールすることができなくなります。
- クラウド関連の費用は、すぐに管理できない程急増します。

「世界の1/3の消費者は2つ以上のフィンテックサービスを利用し、顧客の84%はフィンテックを知っていると回答しています」
– CNBC

開発環境を（適正な費用の範囲内で）より実際の業務環境に近づけ、リリース前にバグを発見できるようにする必要があります。しかし、オンプレミスで開発を行おうとすると、新たな課題が浮上します：

- 開発環境が急速に拡大している場合、アプリケーションに必要なリソースが存在することを、どうやって担保したらよいのでしょうか？
- 用するリソースや負荷が想定できない場合、どうやって新しいアプリの開発計画を立てたらよいのでしょうか？

多くの企業が、既に存在するインフラストラクチャーを使ってDevOpsに取り組んでいます。このような対応は論理的であるように思われますが、もしインフラストラクチャーが旧態依然としたものであれば、その著しい複雑さが進捗を阻害し、生産性を低下させ、達成すべき成果に影響を与えることになります。クラウドでアプリケーションを開発してオンプレミスで稼動させる場合、環境を変えてもアプリケーションが正しく機能することを、どうやって担保すればよいのでしょうか？

インフラストラクチャーの断片化

複数のプラットフォームや不安定な複数の管理ツールで構成されたDevOpsインフラストラクチャーは、インフラストラクチャーのサイロ化を招き、DevOpsプロセスの進行を阻害し、膨大な時間や費用の無駄を招きます。断片化したインフラストラクチャーは：

- 自動化が困難。わずかな変更にも、大変な労力を要することになります。
- 複雑な監視やトラブル対応。ネットワーク、サーバー、ストレージおよび仮想化など、それぞれに対して専門家が必要になります。
- 保護やセキュリティ確保が困難。開発環境の可用性がクリティカルパスとなって、企業データが攻撃を受ける可能性もあります。
- メンテナンスやアップグレードが困難。アップグレードに6ヶ月も必要となったり、システム停止が必要だとしたら、DevOpsを果たして進めることができるのでしょうか？

遅々として進まない非効率なプロビジョニング

DevOpsを実現できるかどうかは、自動化処理を活用して開発やテスト環境を迅速に構築したり削除できるかどうかにかかっています。従来のインフラストラクチャー環境におけるプロビジョニングは、非常に多くの時間を要し、効率的な拡大には多くのストレージが必要となる複雑で負荷の大きな処理でした。このような俊敏性におけるギャップを埋めるため、多くの開発チームがパブリッククラウドに移ろうとしますが、それによって開発側と運用側の会話が減ることになり、DevOpsの本来の趣旨にまったく反するものになります。

開発やテスト環境で使用する業務データのコピーは、コードの品質を確保するために、出来る限り最新の状態である必要があります。何ヶ月も前のデータセットを使用したテストは、障害発生の原因となります。例外は常に付きものですが、出来る限り最新のデータセットとインフラストラクチャーを使って開発チームが作業できるようにすることが重要です。どんなに差異を縮小しても、開発環境から業務環境にコードを移した場合には、不安定な動作や予期しない障害が発生するものです。

DEVOPSの実施

効果的なDevOpsを目指すFSI企業にとっての処方とは：

- クラウドライクなインフラストラクチャーモデルを使って、データセンターインフラストラクチャーをシンプル化および最新化すること
- チーム横断的、あるいはオンプレミスとクラウド環境を横断する形での運用統合を実現する自動化機能を追加すること

そのために組織的にも大幅な変更が必要となる場合があります。
この問題については、後の章で説明します。

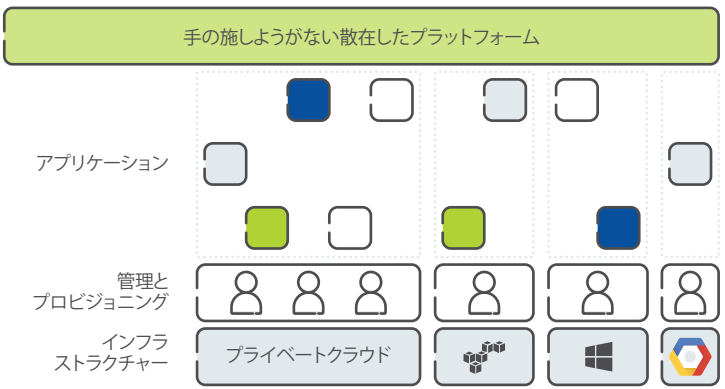


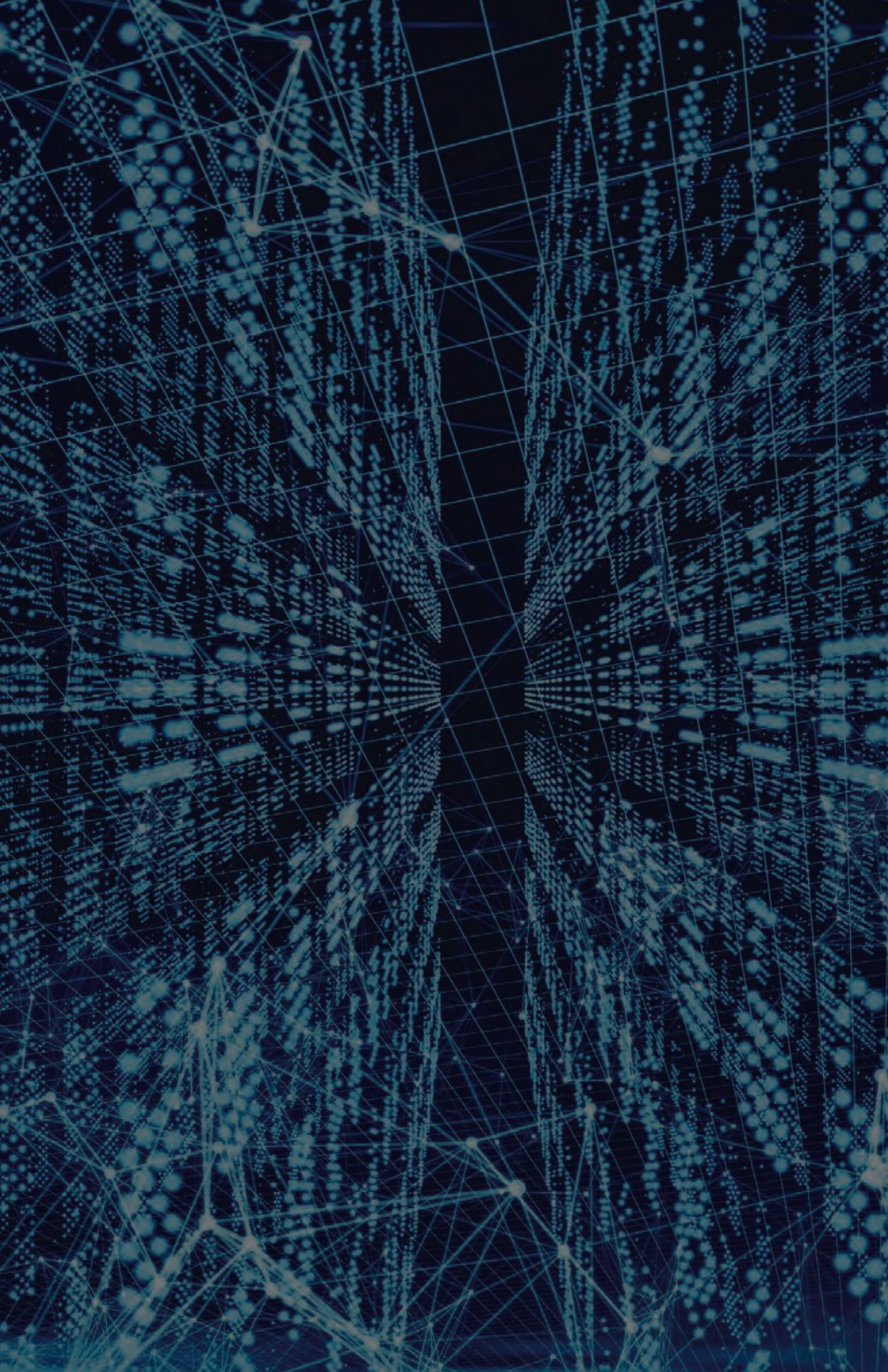
図2. クラウドへの拡張を行うと、DevOpsの実現はいっそう困難になります。

FSIにおけるDEVOPSの課題

第2回目となるDevOps Enterprise Summit in Europeを解説するInfo-Queueの最近の記事には、このように書かれています：

「大手金融機関には共通した課題があります。法律、コンプライアンス、セキュリティに関する要件への対応、そして、支配的かつ官僚的なサイロ化した組織文化です。

このような課題の解決方法には、共通したものがあります。自動化された持続的なデリバリー、無駄のないアプローチ、価値を基準にした組織間のアラインメント、テストの自動化、コンプライアンスやセキュリティチェックの自動化、そして法務部門やコンプライアンス部門の密接な連携です。アウトソーシングをやめてインソーシングに切り替えている企業もあります」



データセンターにおけるインフラストラクチャーのシンプル化と最新化

ITインフラストラクチャーを最新化し、現状の複雑さや多様性を低減することで、自動化が容易になります。DevOpsに理想的となるインフラストラクチャーソリューションは、以下のような特性を持っています：

- **ソフトウエアデファインド**. ソフトウェアデファインドなインフラストラクチャーは、コードアプローチのインフラストラクチャーにとって非常に重要です。構成作業において物理的な対応が必要となる専用のサイロ化したサーバーやストレージ、ネットワークコンポートネントやインフラストラクチャーは完全に撤去すべきです。

- **ハイパーコンバージドを超えて**. サーバー、ストレージ、ネットワーク機能を、REST APIやプログラミングインタフェースと共にシンプルなソフトウェアデファインド・ビルディングブロックに統合したハイパーコンバージドインフラストラクチャーは、シンプルでクラウドライクな環境を提供し、全てのDevOpsタスクをシンプル化します。

- **高可用性**. インフラストラクチャーは、最大限の可用性を提供できるよう構成されている必要があります。ソフトウェアやファームウェアの定期的なアップデート、ハードウェアの追加といった作業を、迅速かつシンプルに実施することが可能で、システム停止が必要だったり、他の運用に影響を与えないことが必要になります。

- **容易な管理**. 1つの管理インターフェースによって、プライベートやパブリッククラウドを横断する形で、全てのインフラストラクチャーや仮想化タスクを管理できる必要があります。一般的に、インフラストラクチャーの管理が容易であるほど、タスクの自動化もシンプルにすることが可能になります。

- **容易な自動化**. 全てのインフラストラクチャー管理タスクが、既に自動化されているか、またはプログラミングインタフェースを使って容易に自動化できる必要があります。

- **柔軟性と順応性**. 全てのインフラストラクチャーやツールは、既存のソリューションとの連携が可能で、新しいツールやテクノロジーの導入が容易に行えなければなりません。.

プライベートクラウドやパブリッククラウドを横断する形での自動化の統合とシンプル化

現在、DevOpsの自動化問題に対応する様々なソリューションが存在していますが、多くのソリューションは部分的な対応に留まっているだけでなく、あくまでも現状のデータセンターの状況を前提としたシンプル化を目的としています。FSI企業が必要としているのは、新しいIT全体

像の構築に向けた課題解決に役立つソリューションです。そのためには、現状を脱却し、あるべき姿への転換を助け、プライベート（オンプレミス）やパブリッククラウドを横断した形での自動化を可能にするソリューションである必要があります。

完全なDevOps自動化ソリューションは、次のような機能を提供します：
モデルベースの自動化. モデルは、スキルセットに関わらず誰でも容易に理解することが可能で、アプリケーションやサービスの様々な依存関係を説明する抽象化された定義体です。ポリシーベースのアプローチは、モデルベースの自動化を補完するものです。モデルは、サービス設定を抽象化し、ポリシーは管理上の懸念を具体的な設定から切り離します。

ワークフロー駆動型のオーケストレーション. 現在のDevOpsは、不安定なスクリプトや面倒な手作業によるプロセスを強いる場合が多くあります。ワークフロー駆動型のオーケストレーションの場合、全てのオーケストレーションは事前定義済みのワークフローに従って実施され、タスクを集中的に管理します。

ワークフロー駆動型のライフサイクル管理. サービスのライフサイクルは、その「導入から廃止まで」の全体アクティビティの集合と考えることができます。適正なDevOpsソリューションは、ライフサイクル全体を通じたアプリケーションの管理と維持が可能なプラットフォームを提供します。これによって、アップグレード、移行、そして廃止といった複雑な機能の自動化が可能になると共に、離散的なサービスの相互の依存関係を説明することができます。

既存の自動化の再利用. IT部門は、これまでツールだけでなくカスタムのスクリプトやコーディングなど、自動化に向け多大な投資を行ってきました。DevOps自動化ソリューションは、このような既存のソリューションと連携したり、適切なタスクで活用できるようになっている必要があります。

単一のインターフェースを使った管理と運用. DevOpsは、全てのワークフローの定義、管理、監視、共有を、集中的に実施できる必要があります。現在は、非常に多くの異なる環境や自動化のためのツールが散在しているため、DevOps担当者が、IT全体を包括的に見渡すことができるケースは非常に稀です。理想的なDevOps自動化ソリューションは、包括的なビューを提供し、全ての管理対象となるアプリケーションやサービスに対して、コラボレーションや共通の視点を提供します。

04

デジタルトランスフォーメーションと組織構造

「多くのFSI企業が、製品やその提供機能を拡張するためにデジタルテクノロジーを利用する一方で、組織の業務や運用、さらにカスタマーモデルをデジタルモデルに合わせるための見直しについては、その対応を怠っています」

– DELOITTE CENTER FOR FINANCIAL SERVICES

現代の金融サービス業界においてテクノロジーの重要性が高まる中、デジタルトランスフォーメーションを成功させるためには、企業文化や管理体系の大幅な変更もまた不可欠です。例えば、McKinsey & Companyでは、オランダの大手銀行であるINGによるアジャイルな組織へのアプローチは、GoogleやNetflix、Spotifyのような成功企業をモデルにしていると説明しています。

INGでは、この組織転換に向け、企業文化の大幅な見直しが必要だということに気づいています。金融サービスのデジタルトランスフォーメーションについて、最近のレポートでは、次のように説明されています：Deloitte Center for Financial Servicesでは、企業のDNAを見直すために、FSI企業が「デジタルDNA」を組織全体に浸透させる必要性と、FSI企業がデジタルトランスフォーメーションを成功させるための特定の要因について説明しています。

企業全体の文化や組織構造の変革は、本書の範囲を超えたテーマですが、それがIT部門や開発チームにもたらす影響や機会について説明したいと思います。IT部門や開発チームは、他部門に対する触媒的な役割を果たします。

これまでの章で、データセンターの変革とクラウドの導入を合わせて考えることが、新しいアプリケーションやサービスの提供や、カスタマーエクスペリエンスの向上において重要であることを説明してきました。新しいデジタルアプリケーションやサービスの提供を進める過程で、従来のウォーターフォール型の手法は、アジャイルな開発方法に置き換わっていきます。開発者とIT運用部門の力関係のバランスを、この新しい現実に合わせて変えていく必要があります。

これを推進するためには、データセンターの変革や、クラウドサービスプロバイダーおよびパブリッククラウドプロバイダーが提供するサービスを確実に導入するのための計画が必要になります。これによって予算や担当者を、アプリケーションスタックやDevOpsへの移行に集中させることができます。

データセンターの変革によるリソースの解放

従来のITインフラストラクチャーは、デジタルのニーズに対応できる十分な柔軟性や拡張性を備えていません。ITチームは、システムを動かし続けるために、日常的な管理タスクに非常に多くの時間を費やしていますが、それはビジネスを一歩先に進めるための仕事ではありません。

IT予算の80%を占めるなど、日々の運用にIT予算の多くが割かれ、イノベーション向けに残されているのは予算は20%だけです。データセンター変革の目的は、この割合を 50/50 に近づけ、予算や担当者の時間を新しいプロジェクトに割り当てられるようにすることです。

アプリケーションスタックにフォーカス

断片化したインフラストラクチャーの管理には、ストレージやネットワーク、仮想化などの専門スキルを持ち、必然的に発生するトラブルへの対応が可能で、相互間のギャップを埋めることができる「インフラストラクチャーのスーパースター」が必要になります。このような人材を確保することは非常に困難で、膨大な費用がかかります。運用が拡大すると、専門家の追加が限界を迎え、スーパースターに依存し続けることが不可能になります。極端な場合、インフラストラクチャーの変更による影響を理解し、複雑な変更を施せるエンジニアが数名しか存在しないというケースさえあります。

データセンターの変革によって、このようなスペシャリストへの依存度を下げ、ITのジェネラリストでもインフラストラクチャーに対応できるようにすることで、サーバー、ストレージ、ネットワークおよび仮想化チーム間に存在するIT運用上の壁を低くすることができます。インフラストラクチャー対応の負荷を低減することで、DevOpsへの重要なステップとなる、アプリケーションスタックやアプリケーション開発にチームを集中させることができるようになります。

結果として、このようなインフラストラクチャーは、開発チームにとって遙かに理解しやすく受け入れやすいものになります。ソフトウェアデファインドインフラストラクチャーによって自動化が可能となり、開発と運用、両方のチームがインフラストラクチャーを直接計画できるようになります。これは「IaC: Infrastructure as Code（コードによるインフラストラクチャー構成管理）」と呼ばれることもあります。

DevOpsへの移行

合理的なインフラストラクチャーがあれば、開発と運用の距離を縮め、前章で説明したように、DevOpsへの移行を加速することができます。しかし、そのためにはまず、多くの組織的な課題に備える必要があります。

最初に、エグゼクティブレベルを巻き込むことが重要です。他の変革と同様、DevOpsには相応の予算が必要であり、定着するまでの間、生産性が低下する場合もあります。

次に、業務要件に合った組織構造を決定する必要があります。組織構造は、IT部門を超えたものとなります。INGのCOOであるBart Schlatmann氏は、次のように述べています「重要なのは『エンド・ツー・エンド』の原則に従って、マーケティングの専門家、商品や販売の専門家、ユーザーエクスペリエンスデザイナー、データアナリスト、ITエンジニアなど、多岐の分野にわたるチームが協力し合いながら、クライアントのニーズへの対応に焦点をあて、同じ成功の目標に向かって一致団結してきたことです」

DevOpsの成功に向け、特に決まった組織構造が存在するわけではありません。WebサイトのDevOpsテクノロジーの場合、それに適した9つの組織構造タイプと、避けるべき7つの組織構造があります。

最後に、組織構造がどうであれ、開発や運用チームが相互に機能し、新しい責任を全う出来るよう、トレーニングに対して投資を行う必要があります。どんな試みの場合でも、その成功は施策に携わる人間が成功するか（あるいは失敗するか）どうかに依存しており、特定チームがどんなに熱心にヒーローとしての努力を払っても、成功は長続きするものではありません。

05

金融サービスにおけるNutanix Enterprise Cloud

「核となるインフラストラクチャーを、Nutanixベースのソリューションに移行する判断を下して、本当に良かったと思います。企業はデジタルエコノミーへと移行しつつあり、これまでのIT産業化の時代から、デジタルと物理的世界を融合した新しいビジネスモデルを持つデジタル化時代に入ろうとしてます。これまでのビジネスモデルには、かつてないほどの変化や破壊が起っています。しかしその一方で、これがITサービスへの新たな期待や要件を生み出しています。インフラストラクチャーや運用の責任者には、TCOをコントロールしながら、業務の拡大を可能にする新しいテクノロジーやアーキテクチャーの枠組みの採用が求められています」

EMPIRE LIFE、エンタープライズサービスおよびテクノロジー担当VP

KEVIN J. ARBOUR氏

金融サービス機関にとって、今ほど多くの課題とビジネスチャンスが目の前に置かれている時代はありません。顧客中心のサービス提供にフォーカスするリテールバンクか、競争優位性を狙う資本市場企業か、あるいは分析モデルの向上を図る保険会社なのかに関わらず、Nutanix Enterprise Cloudは、業務課題の解決に必要なセキュリティやアジリティを提供すると共に、従来の業務アプリケーションと次世代のアプリケーションのいずれについてもサポートすることが可能です。

NutanixのWebスケールなソリューションによって、運用のシンプル化と加速化を図り、新しいサービス提供までの時間を短縮して、ビッグデータの分析に取り組んだり、データベースやVDIを効率的に導入することができるようになります。Nutanixによって、データセンターをクラウド環境まで安全に拡張したハイブリッドIT環境の基盤を構築することができます。

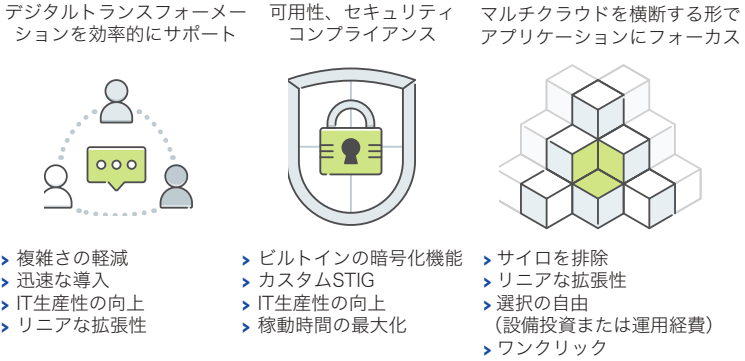


図3. Nutanix Enterprise Cloudが、FSIの課題を解決

エンタープライズクラウドアーキテクチャー

ハイパーコンバージェンスの原則に従ったNutanix Enterprise Cloudは、FSIの課題解決に必要となる柔軟なプラットフォーム機能を提供します。サーバー、ストレージ、セキュリティ、データ保護機能、仮想化、ネットワークを統合したそのアーキテクチャーによって、ワンクリックでの運用やアプリケーションの完全な自動化、マルチクラウドの管理、さらにFISデータセンターに最適となるソリューションを提供することができます。

参考資料

- 20 Top Enterprise Cloud Questions Answered
- Real Data Center Modernization Requires Best-of-breed IT

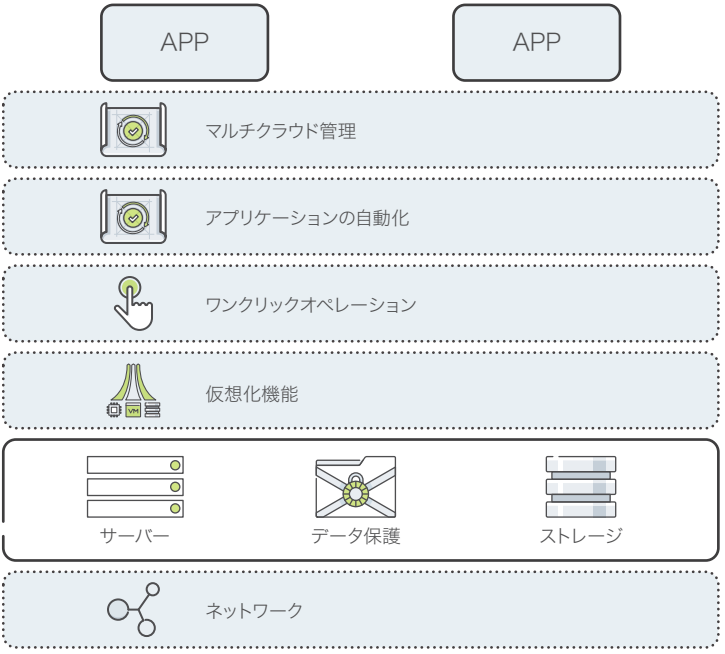


図4. Nutanix Enterprise Cloudには、インフラストラクチャーに求められる一般的な機能が全て含まれています

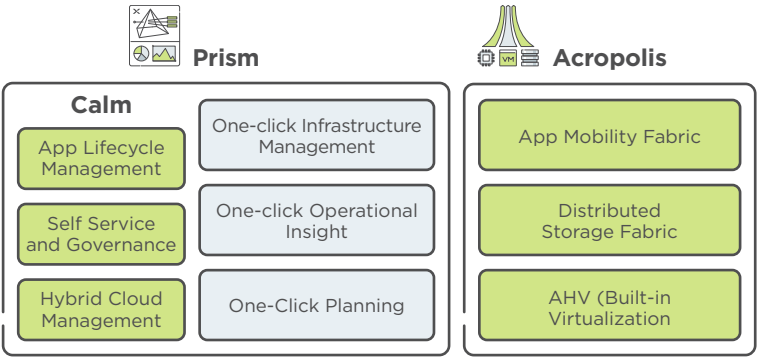


図5. Nutanix Prismは、全ての管理機能を提供します。Acroplisは、高度なインフラストラクチャーとデータ管理機能をサポートしています。

コンパクトかつシンプルなリモート管理が可能なNutanix Enterprise Cloudは、セカンダリデータセンターやディザスタリカバリサイト、さらにブランチロケーションにも最適することが可能です。インフラストラクチャーや業務全体のアプリケーションを、Nutanix Prismという単一のインターフェースで管理することができます。

Nutanix Enterprise Cloudでは、従来のインフラストラクチャーに見られる推測による対応や制約を排除することで、短期間でシステムを稼動させ、システムを停止する必要なく拡張し続けられるようにします。Nutanixによってフラグメント化したインフラストラクチャーを排除し、使用率を上げ、拡張性や可用性を大幅に向上させながら、コストを削減することが可能です。ITチームは、管理作業の削減や排除が可能となったことで、アプリケーション機能の向上や新たなサービスの提供により多くの時間を割けるようになります。

セキュアな設計

レガシーなインフラストラクチャーソリューションは、セキュリティを最優先に考えて設計されたものではありません。Nutanixのアーキテクチャーでは、様々なビルトイン機能を備え、優れた防御機能を発揮する、セキュリティファーストのアプローチを取っています。

セキュリティ開発ライフサイクル

Nutanixは、独自のセキュリティ開発ライフサイクル（SecDL）を使用して、設計から開発、テスト、そして機能強化に至るまで、全てのソフトウェア開発プロセスでセキュリティ機能を取り入れています。Nutanixソリューションは、確実なコンプライアンス対応を実現するため、政府、金融サービス、ヘルスケアなど、幅広い業界での評価プログラムの認定を受けています。この結果、攻撃対象範囲を大幅に縮小し、機密データが侵害を受ける機会を低減させています。

- 連携. セキュリティは、製品開発の全ての段階に織り込まれ、ストレージ、仮想化、管理機能を含むハイパコンバージドインフラストラクチャースタック全体をカバーできるようになっています。

- 自動テスト. SecDLテストは完全に自動化され、セキュリティに関連したコード変更は、リスクを最小限に抑えるためにマイナーリリースの間で行われるようになっています。

- 脅威モデリング. 全てのコード変更に関連して想定されるリスクを評価し、緩和措置が取られます。

「当社の（全てのハードウェアシステムとOSを管理する）ITインフラストラクチャーチームと、（最大のSplunkユーザーであり、大規模なデータ保存とパフォーマンス要件に対応する）セキュリティチーム、そしてSplunkを実際に管理しているツール担当チーム全員が、意思決定に関与しています。この3つのチーム全てが、Nutanix Enterprise Cloudプラットフォームは、当社の要件にあった最高のソリューションだったという意見に同意しています」

– NASDAQ、グローバルシステムおよびストレージ担当シニアディレクター JAKE YANG氏

システムレベルのセキュリティ機能には、2要素認証やクラスタロックダウン、ソフトウェアまたはハードウェアベースの保存データの暗号化機能、そして堅牢なキー管理機能などが含まれています。

セキュリティの自動化

Nutanixは、米国国防総省の認定に要する時間を短縮するため、独自のセキュリティ技術導入ガイド（STIG）を導入し、Nutanixシステムの安全なインストレーションや保守を可能にすると共に、認定に必要な時間を数ヶ月から数分にまで短縮しました。

- **迅速なベースラインの確認と検証.** NutanixのSTIGは、自動評価ツールと互換性を維持するため、XCCDFフォーマットで記述され、SCAP標準をサポートしています。

- **自動構成管理.** 自動セキュリティ構成管理（SCMA: Security Configuration Management Automation）によって、ストレージやビルトインの仮想化機能など、Nutanix STIGに記載された800のセキュリティ項目を効率的に確認することができます。

高度なマイクロセグメンテーション

多くの業界で規制が強化されていることで、マイクロセグメンテーションに対する要望が急速に高まっています。Nutanixのマイクロセグメンテーションによって、極めて粒度の高いネットワークコミュニケーションポリシーをDMZに提供することが可能になります。Nutanixカテゴリーは、ポリシーの定義と管理をシンプル化します。VMが定義済みカテゴリーに追加されると、自動的に適切なポリシーが継承されます。また、包括的な仮想化によって、容易にルールを作成することができます。

広範におよぶネットワークセキュリティパートナー

拡張性に優れたNutanixアーキテクチャーは、広範なセキュリティパートナーのエコシステムと連携するためのAPIを提供しています。検証済みの共同ソリューションは、ネットワークやデータ、エンドポイントなど、あらゆる階層に柔軟なセキュリティ機能と確かなサポートエクスペリエンスを提供します。Nutanixでは、SIEMやファイアウォール、その他のセキュリティアプリケーションを、WebホストやDMZサービスと同じ共有のインフラストラクチャー上に構築することができます。

参考資料

- Information Security with Nutanix

ワンクリックアップグレード

多くのサイバー攻撃は、まだパッチが適用されていないインフラストラクチャー上の既知の脆弱性を探し出そう試みます。Nutanixが提供する、システムを停止することなくワンクリックで実施できるアップグレード機能によって、インフラストラクチャーソフトウェアにパッチを適用する際の手間を省き、遙かに容易にDMZのセキュリティ設定を最新の状態に保つことができます。

Nutanix CalumによるITの自動化

Nutanix Enterprise Cloudは、定常的な管理や最適化といった作業を不要にし、ITインフラストラクチャーを実質的にインビジブルなもの、つまり普段意識する必要がないものに変えます。また、アプリケーションライフサイクル管理における固有な課題への対応や、プライベート、パブリック、分散クラウドを横断する形でのIT運用環境の包括的な自動化を実現できます。さらに、単一の管理インフラストラクチャーを通して、マルチクラウド環境のインフラストラクチャーやアプリケーションを管理することもできます。

Nutanix Calmは、モデルベースのワークフローを使って、DevOpsの導入に不可欠な自動化や、ネイティブなアプリケーションのオーケストレーション、さらにライフサイクル管理といった機能をNutanix Enterprise Cloudに提供します。

アプリケーションライフサイクル管理

Calm　では、アプリケーションを完全なエンティティとして扱うことで、アプリケーションの作成から使用、そして管理方法に至るまでをオーケストレーションします。Calmは、プライベートクラウドやパブリッククラウドなど、様々なクラウド環境におけるアプリケーションのシンプルで再生可能な自動管理を可能にします。

Calmは、関連するVM、設定内容、バイナリなど各アプリケーションの全ての要素を取り込むことによって、カスタムアプリケーションの設定や管理をシンプル化し、自動化や繰り返し実行が可能な共通アプリケーションの導入およびライフサイクル管理を可能にします。

互いに共通の言語を用いた1つの柔軟な枠組みを提供することで、チーム間のコラボレーションを向上させ、開発と運用の間で齟齬が生じることを避けることができます。

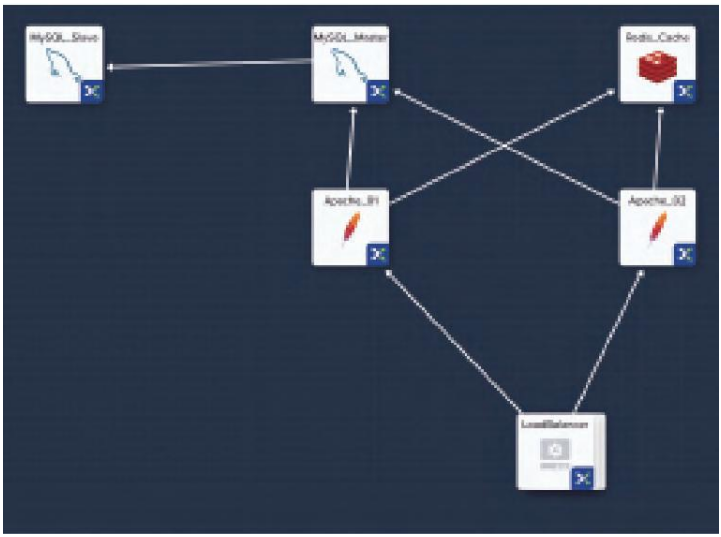


図6. Calmブループリントには、カスタムアプリケーションの導入と管理に必要となる全ての要素が盛り込まれています。

セルフサービスとガバナンス

Nutanix Marketplaceは、Nutanix Enterprise Cloud環境に対して完全なセルフサービス機能を提供します。ユーザーは、事前に組み込み済みのブループリントや、マーケットプレイスで提供するカスタムのブループリントを利用することができます。アプリケーションのオーナーや開発者は、ITサービスをリクエストし、即座にサービスの提供を受けることができます。

ロールベースのガバナンスによって、ユーザーの操作を指定された許可範囲内に限定することができます。包括的なトレーサビリティや問題の排除のため、インフラストラクチャースタック全体における全てのアクティビティや変更をロギングし、セキュリティチームにとって重要なコンプライアンス対応を支援します。部門およびグループ単位でのチャージバックやコスト管理が可能で、パブリックやプライベートクラウドを横断する形でIT関連費用を注意深く監視することができます。

参考資料

- Nutanix Calm: Application Automation
- DevOps and the Enterprise Cloud

「私たちが納期を守ることができる大きな要因は、複雑なインストレーションが不要であり、他のベンダーのように様々なスキルセットを用意する必要もないためです。また、当初の想定よりも遙かに少ない要員で管理することもことが可能で、ストレージに特化したスペシャリストを採用する必要もありませんでした」

– LONDON CAPITAL GROUP、CIO
BLAIR WRIGHT氏

図7. Calmは、チームやアプリケーション単位で、クラウド全体の詳細なコストを提示します。

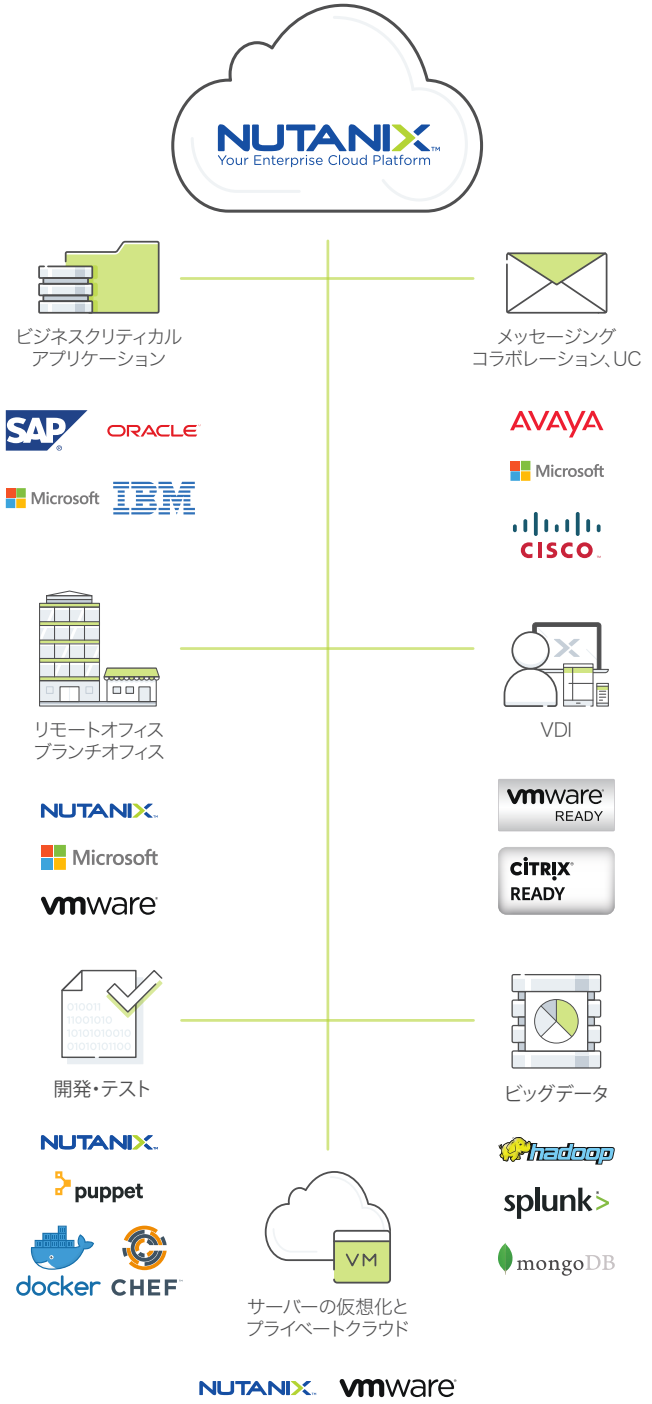
ハイブリッドクラウド管理

Calmによって、ハイブリッドクラウドアーキテクチャーのプロビジョニングを自動化することができます。複数階層で構成されたアプリケーションや分散アプリケーションを、異なるクラウド環境に導入することができます。ポリシーベースのレポーティングによって、パブリッククラウドの全体的な使用状況や、正しいコストをひと目で確認することが可能となり、アプリケーションのプロビジョニングを業務要件やコスト要件に基づいて決定することができます。

エンタープライズクラウドへのアプローチ

従来のエンタープライズクラウドアプリケーションや、エンドユーザー向けのワークスペース環境のサポートに加え、金融サービス企業では、新しいアプリケーションに対するクラウドネイティブなアプローチをさらに拡大しています。現在では、クラウドを考慮に入れた上で、オンプレミスにおけるインフラストラクチャーの意思決定を行う必要があります。複雑なインフラストラクチャーは、多くの努力を無駄にし、マルチクラウドモデルの導入にも悪影響を及ぼします。

クラウドサービスをシームレスに統合することが可能なNutanixソリューションによって、アジャイルなIT運用が可能となり、クラウドへの移行を加速することができます。Nutanix Enterprise Cloud インフラストラクチャーは、柔軟でセキュリティに優れ、管理も容易で、金融サービス企業が求める世界トップクラスのサービスとサポートを提供します。今日のIT部門は、オンプレプレミスプライベートクラウドや、Nutanix X-Poweredサービスプロバイダーがホストするプライベートクラウド、さらに様々なプライベートクラウドなど、複数のクラウド環境を横断する形でNutanix Enterprise Cloud OSのメリットを活用し、ビジネスクリティカルなアプリケーションやビッグデータ分析、次世代のクラウドネイティブなアプリケーションなど、幅広いワークロードを稼動させています。

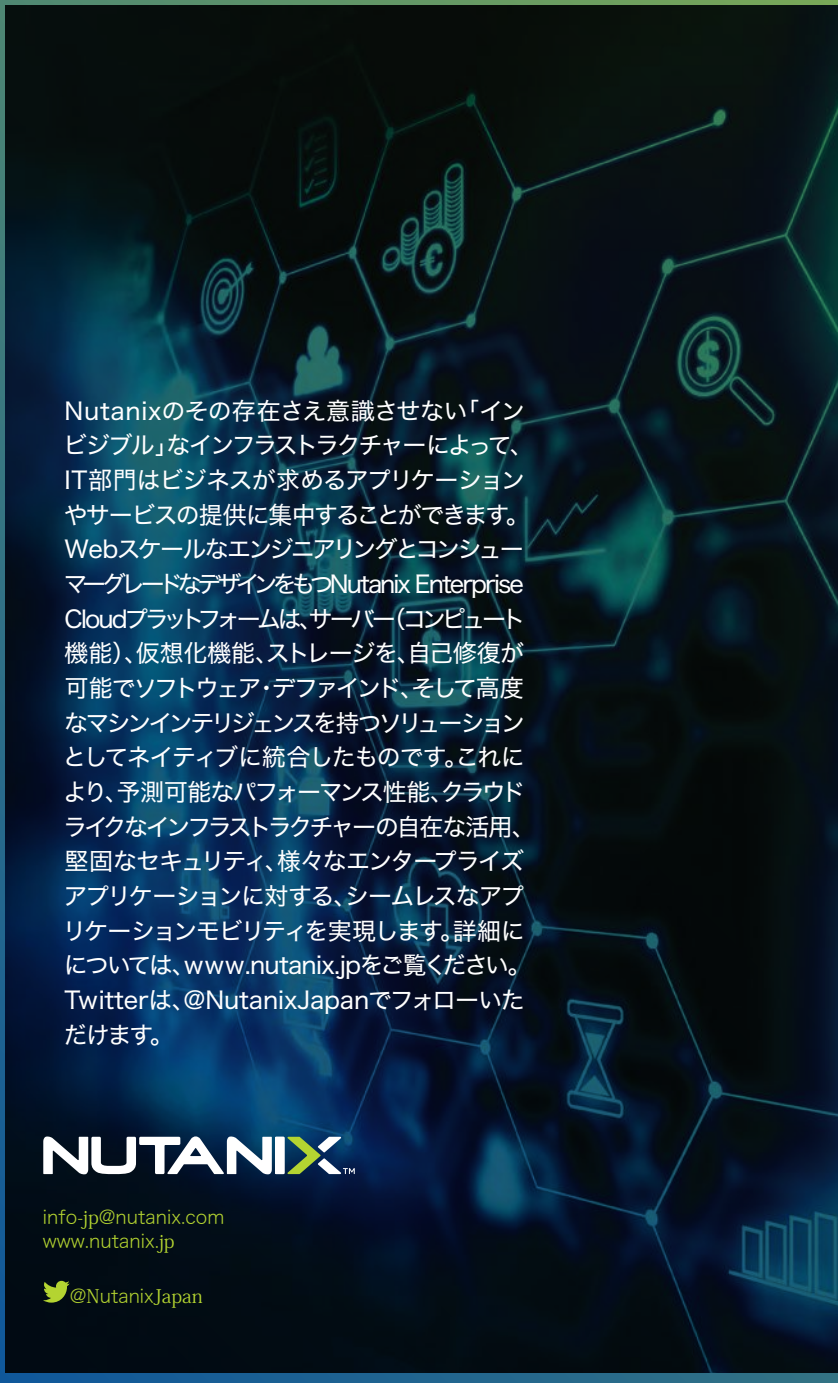

NUTANIX
Your Enterprise Cloud Platform
ビジネスクリティカル
アプリケーション
SAP
ORACLE
Microsoft
IBM
メッセージング
コラボレーション、UC
AVAYA
Microsoft
CISCO
リモートオフィス
ブランチオフィス
NUTANIX
Microsoft
vmware
VDI
vmware READY
CITRIX READY
開発・テスト
NUTANIX
puppet
docker
CHEF
ビッグデータ
hadoop
splunk>
mongoDB
VM
サーバーの仮想化と
プライベートクラウド
NUTANIX
vmware

金融サービスや保険会社のお客様は、Nutanix Enterprise Cloud OSを使って、銀行業務や保険業務固有のトランザクションシステムや分析システムに加え、セキュアなEメール、メッセージング、コラボレーションワークロード、エンドユーザーコンピューティング、VDI、ファイルストレージ、プライベートクラウドといったワークロードをサポートしています。

これらの企業は、優れたパフォーマンスやレスポンス、ITやエンドユーザーの生産性向上、アプリケーションやサービスに対する可用性の向上、さらに運用や設備コストの低減といったメリットを享受しています。このようなメリットはITに限ったものではありません。金融サービス企業は、商品の迅速な市場投入や顧客満足度の向上など、より優れたサービスを顧客に対して提供できるようになります。

Nutanixが、インフラストラクチャーやクラウドに対するIT戦略の変革をいかに支援することが可能かという点について、さらに詳しくご理解いただけます。Nutanixへのお問い合わせは、info-jp@nutanix.comまでお願いします。Twitterは、@NutanixJapanでフォローいただくことができます。また、https://www.nutanix.jp/demo/でリクエストいただければ、皆様向けにカスタマイズした説明を行なわせていただきます。

図8. Nutanixは、従来のワークロードから新しいワークロードに至るまで、
サーバーやストレージ、ネットワークに関する幅広い課題の解決を支援します。



Nutanixのその存在さえ意識させない「インビジブル」なインフラストラクチャーによって、IT部門はビジネスが求めるアプリケーションやサービスの提供に集中することができます。WebスケールなエンジニアリングとコンシューマーグレードなデザインをもつNutanix Enterprise Cloudプラットフォームは、サーバー（コンピュート機能）、仮想化機能、ストレージを、自己修復が可能でソフトウェア・デファインド、そして高度なマシンインテリジェンスを持つソリューションとしてネイティブに統合したものです。これにより、予測可能なパフォーマンス性能、クラウドライクなインフラストラクチャーの自在な活用、堅固なセキュリティ、様々なエンタープライズアプリケーションに対する、シームレスなアプリケーションモビリティを実現します。詳細については、www.nutanix.jpをご覧ください。Twitterは、@NutanixJapanでフォローいただけます。

NUTANIX™

info-jp@nutanix.com
www.nutanix.jp

@NutanixJapan