Deloitte.
デロイト トーマツ

デジタル戦略としての全社アーキテクチャのあるべき姿

デジタル時代を勝ち抜くためのアーキテクチャの要点

デロイト トーマツ コンサルティング合同会社
テクノロジーストラテジー・トランスフォーメーション

変化の激しい経営環境において、競争優位性を持ち、持続的な成長を実現できるための企業力を持つことが日本企業の目指す姿となる

1.はじめに

再注目を浴びるエンタープライズ・アーキテクチャ

近年の経営を取り巻く環境は、VUCAと称されるように不確実性が高く、将来の予測が困難な状況下にある。VUCAとは、Volatility(ボラティリティ:変動性)、Uncertainty(アンサートゥンティ:不確実性)、Complexity(コンプレキシティ:複雑性）、Ambiguity(アンビギュイティ:曖昧性)の頭文字を並べた言葉である。この言葉が示すような変化の激しい経営環境において、経営環境は多岐にわたる改革を求められており、いつどこでも対応できる速さと、全体を統制できる力を持つことが日本企業に必要な取組みとなってきている。この取組みを進めていくためには、世の中の流れに目を向け、産業・社会・顧客に新しい価値を届けられるよう、変化に先回りする形でデジタル・クラウド活用を武器としていくことが必要となる。これを実現していく際の考え方として、「エンタープライズ・アーキテクチャ（EA）」に改めて注目が集まっている。

従来のエンタープライズ・アーキテクチャ

「アーキテクチャ」とは元々、建築の領域において建造物や建築様式を指す言葉で、転じて、IT領域においては技術の設計思想を指す言葉として、広く用いられている。また、「エンタープライズ・アーキテクチャ（EA）」という用語は、2000年代前半に登場した用語で、ビジネスとITの接点における「企業の情報システム全体像のデザイン」を指し、ビジネスをサポートするシステムの全体最適化を目指して用いられる検討のフレームワークである。検討のフレームワークとしての「EA」には、以下の検討領域が含まれる。

【業務機能領域】

- BA（Business Architecture）：政策・業務の内容、実施主体、業務フロー等について、共通化・合理化など実現すべき姿を体系的に示したもの。

【IT／デジタル機能領域】

- AA（Application Architecture）：業務処理に最適な情報システムの形態（集中型か分散型か、汎用パッケージソフトを活用するか個別に開発するか等）を体系的に示したもの。
- DA（Data Architecture）：各業務・システムにおいて利用される情報（システム上のデータ）の内容、各情報（データ）間の関連性を体系的に示したもの。
- TA（Technology Architecture）：実際にシステムを構築する際に利用する諸々の技術的構成要素（ハード、ソフト、ネットワーク等）を体系的に示したもの。

2000年代からこれまでの日本企業においては、このフレームワークの下、最適化と言いながらITコスト抑制のみを主目的としてしまっているケースが多い。例えば、IT部門管理下にある既存ITの標準化や統廃合のみが検討テーマになっていることや、IT環境を管理・統制するために、重厚なドキュメントを整備することに時間と労力を費やしてしまっている実態がある。本来、アーキテクチャに関する検討は企業経営全体に影響を及ぼすものであるにもかかわらず、技術者・IT部門中心に進められてきてしまっており、あるべき検討ができていないことがほとんどだ。

デジタル時代のエンタープライズ・アーキテクチャ

経産省やデジタル庁などによれば、アーキテクチャとは、変化に先回りする形で多様かつ身近なテクノロジーやデジタル活用を武器に、産業・社会・顧客に新しい価値を届けるための考え方や構造として定義されるものと述べられている。このことからもわかるように、デジタル時代において考えるべきアーキテクチャは、従前の考え方や取り組みの範疇を大きく超える概念へ変化してきている。従来のアーキテクチャは先に述べたように標準化や規定定義を軸にコスト削減を目指すものであったが、今求められるアーキテクチャはトランスフォーメーションの概念を取り入れたものとなる（図1参照）。

重要なことは、アーキテクチャは、技術者やIT部門に閉じた話ではなく、企業経営の在り方・組織文化の在り方そのものであり、企業が目指すゴール・世界観との直結が求められ、経営者が理解し責任を負うべきアジェンダであり、全社的に取り組むべき課題へとシフトしてきていることである。

Traditional		Digital
ITシステムの整備	目的	市場価値創出・変化への追随
テクノロジーの統合・標準化	ミッション	トランスフォーメーションとイノベーション
テクノロジ領域	視点	企業全体
IT専門チーム	パラダイム	デジタル変革プログラムのコア
標準・規定文書ベースの厳密な管理	ガバナンス	最小限のガバナンスと最大限のサポート
業務要件のHeavy Analysis &One Way	アプローチ	問題解決アプローチ・Agile型
不明瞭、個別運用	役割・責任	明瞭、コラボレーションによる創造的な活動
コスト最小限を志向	インパクト	効果最大化を志向

図 1　デジタル時代のアーキテクチャ

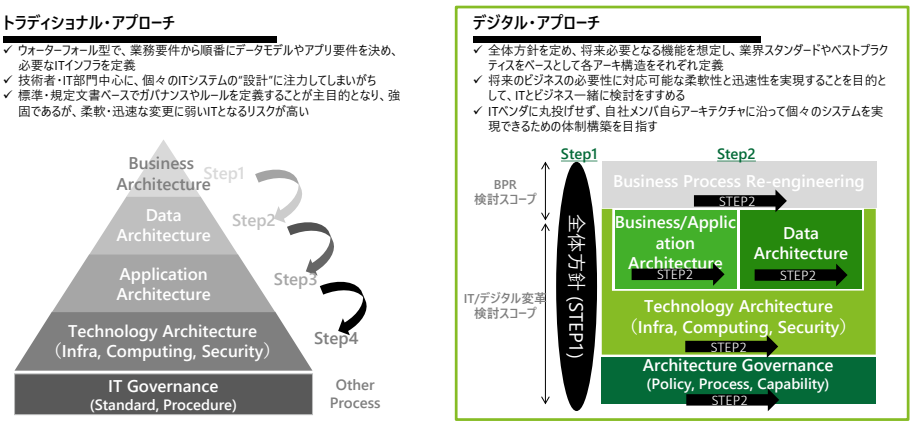

図 2　アーキテクチャ検討のアプローチ

デジタル時代のアーキテクチャ検討アプローチ

アーキテクチャ検討のアプローチ自体もデジタル時代に合わせたものへシフトしている。従来は、ウォーターフォール型で、業務要件から順番にデータモデルやアプリ要件を決め、必要なITインフラを定義するという、アプローチで進めることが多く、結果として得られるアーキテクチャについては強固であるが、柔軟・迅速な変更に弱いITとなるリスクが高いものであった。一方、デジタル時代においては、全体方針を定め、将来必要となる機能を想定し、業界スタンダードやベストプラクティスをベースとして各アーキ構造をそれぞれ定義していくというアプローチが求められる（図2参照）。

本稿では、デジタル時代を勝ち抜くためのアーキテクチャの要点について、アプリアーキ、データアーキ、インフラアーキ、コンピューティングアーキ、セキュリティアーキという5つの領域で述べる。

自社のリソースをノンコアプロセスからコアプロセスへ集中できるよう、世の中のベストプラクティスを自社に取り込み追随可能なアーキテクチャ（仕組みと体制）を手にする

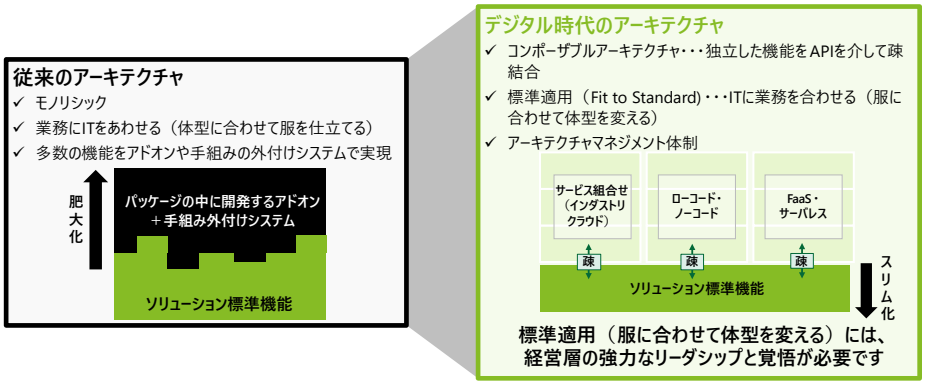

図 3　ビジネス/アプリケーションアーキテクチャ

2.ビジネス/アプリケーションアーキテクチャ

事業変革を阻害する従来のモノリシックなアーキテクチャ

ビジネスの変化に適切に対応していくためには、ITを迅速かつ柔軟に組み替えできるように準備しておくことが望ましいということは想像に難くない。しかし、現実の世界においては、度重なる機能追加や改修により、構造が肥大化・複雑化してしまったり、設計書の保守が徹底されていなかったり、システムの全容を理解しているIT要員が社内に存在しなかったりするため、ITを迅速かつ柔軟に組み替えて新規ビジネスチャンスに対応していくということができなくなってしまうという状況に陥っていることがよくある。

このような状況が生まれる要因の一つとして、従前からのシステム構造として主流と言える"モノリシックな（一枚岩の大きな塊）アーキテクチャ"がある（図3の左部参照）。モノリシックなアーキテクチャで構築されたシステムは、クラッチやアドオン開発のプログラムが多量となりやすく、開発するプログラム間が相互に連携する密結合となり一部を修正する際の影響範囲を特定することが難しいため、ビジネスロジックの頻繁な変更や、先進技術の部分的な追加実装には適していないものとなる。
また、モノリシックなアーキテクチャを採用している業務システムは大規模なシステムであることが多く、個別ユーザ要件を取り込んで現状の業務にITをあわせる、言わば、体型に服を合わせていくという進め方を取っているため、ユーザにとっては利便性が高いため数十年に渡り利用されるシステムとなる。この使いやすいシステムは大幅な業務改革を強いるようなシステム刷新を取りづらく、ユーザが同じ業務を長年繰り返すことに慣れていき、変化をしないということそのものが企業文化となってしまう原因を生み出している。

グローバルのベストプラクティスを取り込むためのデジタル時代のアーキテクチャ

これからの時代において、ビジネスの変化に適切に対応していくためには、柔軟性と迅速性というものを獲得して行くことが不可欠となる。これを実現するためのアーキテクチャとして重要な考え方は、コンポーザブルなアーキテクチャ、標準適応Fit to Standardという2つの考え方である（図3の右部参照）。
これは、ある業務や事業を実現するにあたり、ソフトウェアアズアサービス（SaaS）と呼ばれるクラウド上で提供されるパッケージ機能のようなものを複数組み合わせ、かつ、SaaSに業務を合わせていくことを示しており、いわば、洋服に体型を合わせていくと言うことを示している。
特にSaaSについては、社内ワークフローなど業界非依存で共通のニーズを満たすソフトウェアとして活用することが大半ではあるが、インダストリクラウドと呼ばれるような、各業界や業種固有の戦略や、事業運営のニーズを満たすことのできる業界固有SaaSが次々に生まれてきており、よりSaaS活用が進めるべき流れが生まれてきている。

得られる価値

このアーキテクチャの考え方により得られる価値は以下の通りである。

- 疎結合された小さな機能群単位で導入・展開が可能となるため、アジャイルな導入が可能となる。これにより、既存システムに大きな変更を加えることなく、特定のサービス（業務プロセス）のみを対象として、最新技術による業務への適用を試すと言ったことも容易に行えるようになる
- この世の中の既にクラウド上で提供されるSaaS（インダストリクラウド）は様々な企業のベストプラクティスが取り込まれた状態になっているため、そのベストプラクティスに自社のアーキテクチャを合わせていくことで自社の業務や事業に世の中のベストプラクティスを取り込むことができる

こうした考え方は、外資系企業では既に当たり前となっており、例えばグローバル企業でデファクトスタンダードとなっているERPの導入を例にとると、短ければ3カ月、長くとも1～2年程度で実装が済むケースがほとんどである。一方で、日本企業においては導入そのものが5年越しのプロジェクトになることも珍しくない。これは、長年培われた部門固有の業務プロセス・便利な機能に固執し、追加開発にて組み込もうとすること（体形に合わせて服を仕立てるアプローチ）で検討が長期化する傾向があることが原因である。しかし、基幹系システムの導入に数年単位の遅れをとっていては、ITを梃としてビジネス面での競争優位性を獲得するなど望むべくもないので、従来型の考え方にたつ日本企業は、デジタル時代のアーキテクチャの考え方である、コンポーザブル、かつ、Fit to Standardへ舵を切るべきときに来ている。

ここで重要なことを1つ上げておく。標準適用、つまり服に合わせ体型を変えていくアプローチは、かなり困難を伴うものとなるため、最初の掛け声だけで終わってしまわぬように、経営層の強力なリーダーシップと覚悟が必要となることを認識しておいてほしい。

企業内外のデータを活用し先を読みアクションを取ることができるようにするためのアーキテクチャ（仕組みと体制）を手にする

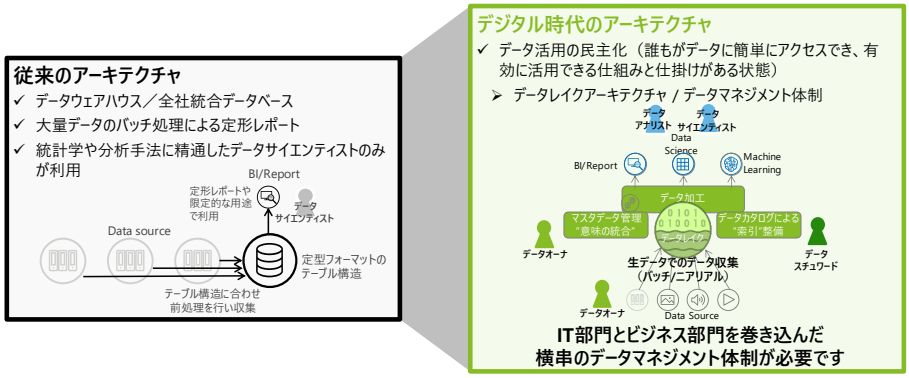

図 4　データアーキテクチャ

3.データアーキテクチャ

データ活用を阻害する従来の柔軟性のないアーキテクチャ

データ活用が企業の盛衰を決定するものとなってきており、業務、事業、経営、あらゆるレイヤにおいてデータ活用の仕組みと能力を持つことが、強さとスピードの実現につながる時代となってきているが、現実的には、以下のような問題が山積している。

- 計画を実行へ落とし込むことや、その計画に対する実績のモニタリングや分析ができていない
- 一部の事業部や本社のみの活動履歴しか追えないため、グループ全体でのポートフォリオが把握できず、タイムリーに適切な意思決定ができてない
- コーポレートが、グループ子会社や事業部からデータを収集・分析する仕組みがない
- 業務とシステムの個別最適化となり、全社横断的な視点でデータを捉えることができない
- 業務の属人化によって集計作業に時間が掛かりタイムリーなレポーティングができない

このような課題により、日本企業においてデータの利活用が限定的となっているということが明らかとなってきている。

このような状況が生まれる要因の一つとして、古いアーキテクチャの考え方が挙げられる（図4の左部参照）。データ基盤を保持しているという日本企業のほとんどにおけるアーキテクチャは、全社で巨大なデータベースを保持し、そこに複数のシステムのデータをひたすら集めていく、構造化のためのテーブル設計を行い、そのテーブル構造に合わせて事前処理を行ってからデータを投入するという、従来型のアーキテクチャとなっている。これは、オンプレミスにおいて巨大なストレージを持ち、データ基盤を構築している企業のことのみを指すのではなく、クラウド上のDWHサービスを使っていたとしても、アーキテクチャの考え方が従来型の考え方のままであることがほとんどである。

これにより、以下に示すような弊害が生まれる。

- 特定の定形レポートや、集計軸での分析しかできない
- 新たな観点で分析したいとなったら、都度テーブル設計やBI画面の開発が必要となってしまうため、必要なときに必要なデータ活用ができない
- システムごとに異なるデータの意味定義を解消できないため、大量のデータは集めてきたはずなのに何も活用できない
- 個別システムからは、登録用のテーブル構造に合わせて、連携用のバッチ処理を回した集計結果のみ連携されるので、詳細分析ができない

多種多様なデータを経営判断に活かすためのデジタル時代のアーキテクチャ

これからの時代において、柔軟性と迅速性というものを獲得していくためには、一貫性のあるデータの横串連携を可能とし、誰もがデータに簡単にアクセスでき有効活用できるデータの民主化のためのアーキテクチャとしていく考え方が必要となる（図4の右部参照）。このアーキテクチャにおいては具備すべきサービス機能として主に4つの機能が挙げられる。

- 構造化データだけでなく非構造化も保持可能なデータレイク機能
- データの意味定義を整理する「メタデータ」情報を管理可能なデータカタログ機能
- 分散配置されたデータを連携するためのデータ連携機能
- マスタデータを管理するための機能

得られる価値

このアーキテクチャの考え方により得られる価値は以下の通りである。

- データレイクの仕組みにより、種類によらず、大量のデータを高速処理し、利用に向けて下準備する事が可能となる。いわゆるリレーショナルデータベースの構造データだけでなく、テキストや画像、動画、音声といった膨大な量の非構造データを保持でき、リアルタイムデータの活用が可能となる
- データカタログの仕組みにより、どこにどんな意味合いのデータを保有しているかというデータの全体像を把握することが可能となる
- データ連携の仕組みにより、コンポーザブルで疎結合化となるアプリケーションに分散配置されたデータをAPI連携し、データ活用につなげることが可能となる
- マスタデータ管理の仕組みにより、マスタデータは企業で一元管理できるようになる

なお、データ活用については、基盤があればそれで全て解決とはならず、企業内に蓄えられたデータを管理／統制（マネジメント／ガバナンス）するための、いわゆるデータマネジメントの体制も不可欠となる。データオーナ、データスチュワードといったロールをデータマネジメント体制の中で持たせて、全社横串の活動としてデータ整備を進めていく取り組みが必要となることを認識しておいてほしい。

仮想化技術としてのクラウド活用ではない、真のクラウド活用により業務や事業が必要とする機能を提供できるアーキテクチャ（仕組みと体制）を先回りして準備する

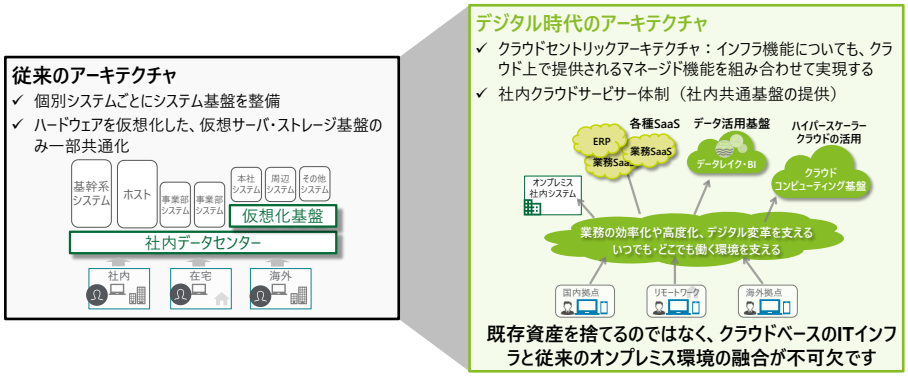

図 5　インフラストラクチャアーキテクチャ

4.インフラストラクチャアーキテクチャ

デジタル・クラウド活用を後回しにしてしまう従来の硬直的なアーキテクチャ

インダストリクラウド活用や、クラウド活用を目指す際、日本企業の現状のIT環境では大きな問題に直面する。ITインフラ領域において従来の仕組みを変えることなく、先に述べたアプリケーションアーキテクチャやデータアーキテクチャ変革を行う際、増加するクラウドへのアクセスのキャパシティを処理できないといったことや、セキュリティ対策がクラウドに対応できていないなどの理由から、十分に活用できない状況に陥ってしまうリスクが高い。

このような状況が生まれる理由としては、従来のオンプレミスをベースとしたITインフラ環境そのものが挙げられる（図5の左部参照）。現在の国内企業のITインフラ環境は、巨大なデータセンターがあり、様々な機器を配置し、社内ネットワーク境界でセキュリティ対策をする構成となっていることがほとんどである。基本的にはITインフラは個別システムごとにサイロ型で構築され、共通基盤化している場合であってもサーバやストレージなどのハードウェアを仮想化した、仮想サーバ・ストレージ基盤のみ一部共通化するのみとなっていることがほとんどである。
このような従来型のITインフラ環境においてキャパシティ増加に対応するためには、事前にハードウェアリソースの増強などの対応が必要となるものであり、スピードや柔軟性の欠如したITインフラと言わざるを得ない。

ビジネス変革を後押しするデジタル時代のアーキテクチャ

デジタル時代に求められるITインフラ環境は、業務や事業が必要とする機能をすぐ提供できる、柔軟性や迅速性の高いITインフラ環境であり、全社ITインフラ環境をクラウド化、すなわち、クラウド上で提供される複数の機能を組み合わせたITインフラ環境が必要である。具体的には、ゼロトラストと呼ばれる新しいセキュリティの考え方を中心とし、コミュニケーション基盤に加えて、ネットワーク基盤や認証基盤、セキュリティなどを含むITインフラ機能を、クラウド上で提供される複数の機能を組み合わせたアーキテクチャとしていくことが必要となる（図5の右部参照）。
ここで1つ注意点を述べておくと、この取組みは、現在の資産となるオンプレミス上の様々なITを捨てて全てをクラウドで作り直すということを意図していない。クラウド上で提供されるSaaSやデータレイクを活用できるようにするための変革の取り組みであり、クラウドベースのITインフラと従来のオンプレミス環境を融合した、ハイブリッドなITインフラ環境を実現することを意図している。
拠点だけでなく、今までアーキテクチャの中心となっていたオンプレミスデータセンターもエッジの一部とするよう配置し、コミュニケーションやクラウドコンピューティング基盤だけでなく、端末管理、ネットワーク、セキュリティ機能についてもクラウド機能で実現することで、SaaS活用やPaaS/FaaS等のサーバレス活用を実現する構成を示す。
従来のネットワークセキュリティの置き換えではなく、インフラ各コンポーネントそれぞれでゼロトラストを加味したセキュリティを実現することとなる。

得られる価値

クラウドベースのアーキテクチャへ社内ITインフラを転換することで、最先端テクノロジーを迅速に活用し、利便性とセキュリティ高度化を両立できるようになるため、安心安全にSaaS活用やデータ活用を推進できるようになる。
具体的には、企業のDX推進や、働き方改革のためクラウド活用を推進しやすくなるほか、クラウド活用により社内ネットワーク内外へ偏在することとなる企業の情報資産を守るゼロトラストの実現へつなげることができるようになる。

この新しいITインフラの実現にあたっては、クラウド上で提供される機能の「組合せ」が重要であり、これまでのように個別機能ごとに設計開発を進めては実現することはできない。特に、クラウド上で提供されるIT基盤にかかるテクノロジーは互いに関連しあっているため、テクノロジーの関連する領域全体を俯瞰したアーキテクチャ（構成）の検討が不可欠であり、全体をデザインする目利き力が肝となる。従来、日本企業が頼りしているSIerや製品ベンダは個別領域しか検討できず個別最適になりがちのため、今までとは異なる観点のパートナーとして全体デザインする目利き力のあるアーキテクトを獲得していくことが何よりも重要な取り組みであることを認識しておいてほしい。

従来の技術とは大きく異なるハイパースケーラーの特徴を踏まえ、スピードと統制の両立ができるようになるアーキテクチャ（仕組みと体制）を手にする

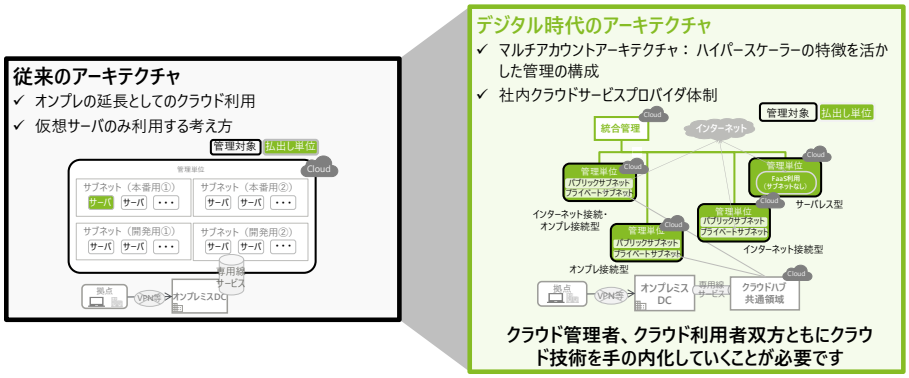

図 6　コンピューティングアーキテクチャ

5.コンピューティングアーキテクチャ

オンプレ再現を目的とし、ハイパースケーラー活用のメリットが得られないアーキテクチャ

先に述べた社内ITインフラをクラウドベースのアーキテクチャへ転換するための取り組みを既に進めている企業も複数あると想定されるが、以下のような課題に直面していることが、様々な企業において発生していることをよく耳にする。

- オンプレミス環境のサーバ・ストレージ基盤の老朽化に合わせて、データセンター機能をクラウド化し、プライベートクラウド環境を構築したが、プライベートクラウド環境の構築自体に2年近くを要した
- 既存システムを順次クラウド化（仮想サーバーのみクラウドへ移設する単純リフト化）をした結果、既存のオンプレミス環境における維持コストより高コストとなってしまった
- プライベートクラウド事業者のクラウドサービスを利用していたが、当該クラウドサービス提供が終了してしまうことになり、クラウド環境を更に別のクラウド環境へ移設することが必要となってしまった

このような状況が生まれる理由としては、従来のオンプレミスをベースとしたコンピューティング環境をクラウド環境上で再現したような、オンプレミスの延長としてのクラウド利用が挙げられる（図6の左部参照）。

コンピューティング環境のクラウド化については、導入までのリードタイムを小さくすることや、変更への柔軟性を上げること、利用料金の重量課金化によるコスト削減、クラウド上で提供される最新テクノロジーが利用できることなど、クラウド利用におけるメリットを享受できるアーキテクチャとしておくことが不可欠であるものの、オンプレミスにおける知識のみでクラウドコンピューティング環境を利用しようとしてしまうと、これらのメリットはほとんど得られない。

ビジネスの効率化や高度化のために、ノンコア業務については、Fit to Standardの方針に則りインダストリクラウドと呼ばれるSaaS活用を拡大していくことを狙いつつ、コア業務については、企業の差別化につながる領域であることから、必ずしもSaaSが存在せず、スクラッチで対応していくことが求められ、それを実現可能とするコンピューティング基盤が不可欠となる。しかし、従来の知識に立脚した、仮想サーバーを立てて必要な製品をひとつひとつインストールしていくようなコンピューティング基盤を利用し、従来の仕組みを変えることなく差別化領域に注力しようとした場合、開発効率が悪く、素早いビジネスの変化に対応できないほか、クラウドでサービス提供されるような最新テクノロジーが活用できず、十分に競争力を獲得できない。

ハイパースケーラーの特徴を踏まえたデジタル時代のアーキテクチャ

デジタル時代にふさわしいクラウドコンピューティングアーキテクチャというのは、迅速性・柔軟性の高いハイパースケーラーと呼ばれるクラウドサービスを活用できる環境であることが不可欠である。仮想サーバーを利用するというIaaS利用だけでなく、クラウドプロバイダーが用意するPaaSやFaaSの機能を組み合わせて1つのシステムを実現していける管理基盤を具備していくことが必要となる（図6の右部参照）。

デジタル時代では、ビジネス変革のスピード（アジリティ）が重要となっていくため、ハイパースケーラーは新たなサービス開発をより迅速に行い、かつ、他のシステム環境に影響を及ぼさずに安心してスピーディに試行錯誤もできるようにするために、管理単位でシステムを完全に分離するマルチアカウント構成を基本的な考え方とする。そして、野良クラウドを回避し個々のシステムへきちんと統制をかけるため、ハイパースケーラーにおける自由度の境界を担保し、かつ共通の統制をかけられる仕組みを用いた管理の方法とする。
また、ハイパースケーラーにて具備されるランディングゾーンの仕組みを用いて、個々のシステムそれぞれ分離したクラウド環境に対して共通要素となる基礎構成や最低限遵守すべきガバナンスルールを自動的に適用させる仕組みとする。

得られる価値

ハイパースケーラーと呼ばれるクラウドプロバイダーが用意するPaaSやFaaSの機能を組み合わせて1つのシステムを実現していける環境を整備することで、ビジネスプロセスのデジタル化やITシステムの導入におけるの迅速性・柔軟性を実現できるようになる。特に、個々のシステム同士の環境をクラウド上で完全分離する仕組みとしておくことで、個々のシステム担当者側で、クラウド上のサービスを利用することに足枷がなく自由にサービスを選んで組み合わせを試行錯誤しつつ、その影響を一切他のシステムへ影響させないということを実現できるだけでなく、個々のシステム担当者が勝手にクラウド環境を利用する野良クラウド化を回避するための仕組みも同時に整備することができるようになる。

ここで重要となる考え方は、クラウド＝従来のインフラ管理者が全てハンドリングするべきと思い込んではいけない、ということだ。迅速性・柔軟性を確保するために個々のシステム担当者へ裁量を与えること（＝個々のシステム管理者へ、各クラウドサービスの利用権限を渡すこと）を仕組みで実現し、クラウド管理者、クラウド利用者双方ともにクラウド技術を手の内化していくということが何よりも重要となる。

高度サイバーセキュリティへの対処と同時に、事業や業務の効率化・高度化など、デジタル化・クラウド化を加速するアーキテクチャ（仕組みと体制）を手にする

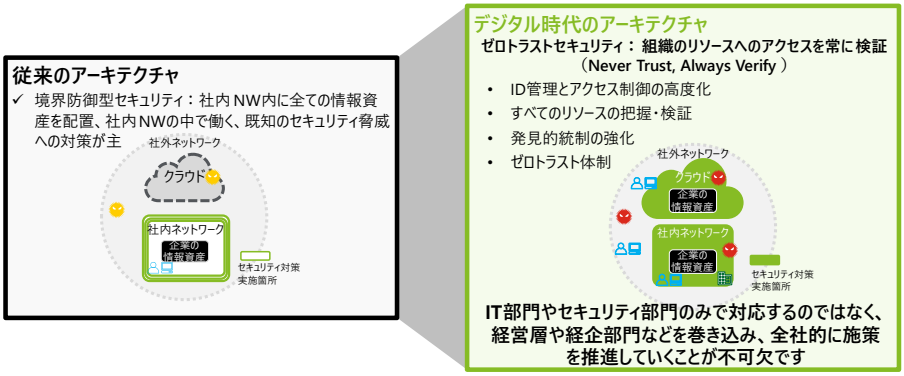

図 7　セキュリティアーキテクチャ

6.セキュリティアーキテクチャ

高度サイバー攻撃を防げない従来の境界防御型アーキテクチャ

従来のセキュリティの考え方は、境界防御型のセキュリティと言われるもので、社内と社外を区別し社内を信頼するという考え方にたちセキュリティ対策をするというものである。例えば会社の情報資産は、社内NW（オンプレミスDC内）に全て配置することが前提であり、社員も社内NWの中で働くことが前提となり、社内NWにアクセスする際に認証などのチェックをするが、一度社内NW内に入ったら特段チェックされないというものとなる（図7左部参照）。

しかし、現実には、既にコミュニケーションツールやSaaSなどを用いることで、企業の情報資産は社外環境でデータ保持する事となり、既に前提が崩れているほか、在宅勤務やテレワークなどの新しい働き方に対応できなかったり、社内NW内に侵入後にランサムウェアを仕掛けるなどの高度標的型攻撃等、新たなセキュリティ脅威に対応できないといったように、課題が山積みとなっている。

これらの原因は、ゼロトラストという、新しい考え方が欠如していることに起因する。ゼロトラストとは、全ての要素を対象とし、エンドツーエンドで要素間の通信と状態を可視化・監視し、ポリシーとコンテキストに基づいて動的に制御するという考え方であり、デジタル活用・クラウド活用にあたっては、ゼロトラストの考え方をベースとして検討を進めることが不可欠となっている。

ゼロトラストを実現するデジタル時代のアーキテクチャ

デジタル・クラウド活用が求められる現在においては、“ゼロトラスト”という考え方を実現していくことが目指す姿であり、“Never Trust, Always Verify”という、何も信頼しないという考え方に立脚し、組織のリソースへのアクセスを常に検証し続けるという仕組みを実現することが重要である。企業内外のどこからアクセスが発生しても安心安全に企業リソースを用いることができるというアーキテクチャを実現することが求められる。（図 7 の右部参照）

NIST 800-207 では、7つのゼロトラストアクセス原則が定義されているが、ここでは、ゼロトラストアーキテクチャ構築に必要となる大きな考え方を4点紹介する。以下の仕組みや体制を整備していくことが、セキュリティアーキテクチャの目指す姿となる。

1つ目は、ID管理とアクセス制御の高度化である。認証やアクセス制御の処理を、動的かつトランザクションごとに制御し、組織の保有するリソースに対するアクションは、セッション単位でアクセス許可の制御を実施するほか、動的なポリシーベース・コンテキストベースでの制御を実施する。

2つ目は、全てのリソースの把握・検証である。全てのリソース（データソースとコンピューティングサービス等）は全て守るべきリソースと見なし、状態を把握し、ロケーション（ネットワークの場所）に関係なく、全ての通信を保護するというものである。

3つ目は、発見的統制の強化である。ネットワークと通信の現在の状態について可能な限り多くの情報を収集し、包括的なログ管理を実施した上で、組織の保有する全リソースに対し、正しくセキュリティが保たれるよう継続的に監視するというものである。

4つ目は、ゼロトラスト体制の構築である。ゼロトラストはセキュリティソリューション導入だけでは実現できず、セキュリティ組織に加えて、企業組織全体で取り組むことが必要となる。

得られる価値

ゼロトラストアーキテクチャがある程度進んだ状態においては、従来の環境に比して、ネットワークやセキュリティのコストが削減できるようになった、データ流出リスク軽減といったセキュリティレベルが向上した、リスクを把握し対策の見直しができるようになった、生産性が向上した、といった成果が得られるようになる。

ただし、これはセキュリティツールを導入して即得られるものではなく、長期にわたった取り組みとして得られる成果となるものである。このため、ゼロトラストアーキテクチャの実現においては、情報システム部門やセキュリティ部門のみで対応するのではなく、経営層や経営企画部門、監査部門などを巻き込み、全社的に施策を推進していくゼロトラスト体制を構築していくことが不可欠である。

7.おわりに

これらのアーキテクチャを実現するには、3つの課題が立ちはだかかる。1つ目は、新しいデジタル・クラウドテクノロジーの知識がないことにより、従来とは異なる考え方を取り入れられず検討が進められないという課題。2つ目は、これまで具体的な検討を全てベンダに依頼して任せていたことにより、自分たちで検討しない体質になっているという課題。3つ目は、社内でIT部門の権力が弱いことにより、全社アジェンダとしてITに係る変革をリードしていく人物がいないという課題である。

新しいデジタルやクラウドテクノロジーに対する知識がないままITベンダに検討を丸投げすることで、ITベンダの持つ新しいITソリューションが新たに導入されるだけという結果となってしまい、変革が進むどころか誰にも使われない新たなシステムが出来上がるという結果となってしまうことが想定される。

この課題を解決するためには、将来の実行フェーズにおける指針・礎となる主要な考え方をまとめ、構想としてトップダウンにて社内へ展開することと、自社でこの新しい考え方・アーキテクチャを使いこなす（＝手の内化する）ための体制をもつことが不可欠である。

デロイト トーマツでは、構想策定から、企業内にこれらを手の内化するための社内アーキテクトチームの組成まで、End to Endで支援するサービスを提供している（図8参照）。最初の6ヶ月で将来に向けた全社IT/DXアーキテクチャの目指す姿と実行計画を描いた上で統制するための体制を実現し、実行プロジェクトの統制や技術検討支援を行えるようにする進め方が地に足のついた実現性のある進め方となる。

全社アーキテクチャという、多岐にわたる検討範囲に対して全体俯瞰の視点を持ち進むというハードルを乗り越えながら進めるためには、全ての検討を自組織のリソースだけで行うことは現実的ではなく、外部リソースの活用も視野に入れて検討することも良いと考えられる。外部の支援サービスを用いつつ、それらを手の内化することを見据え、外部業者に丸投げするのではなく、伴走してもらう中でそのノウハウを自組織に貯めながら、推進していくことが重要である。迅速性・柔軟性を兼ね備えたアーキテクチャを手にし、デジタル時代を勝ち抜くために、必要な取り組みを推進していただきたい。

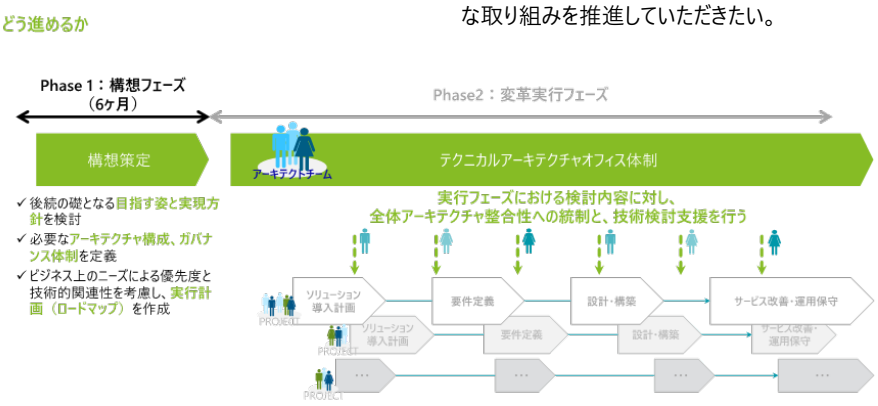

図 8進め方（例）

プロフェッショナル

佐藤 岳彦
Technology Strategy & Transformation
執行役員 マネージングディレクター

外資コンサルティングファームを経て現職。
官公庁、金融、製造業を中心に、IT構想策定、全社IT/DXアーキテクチャ策定、大規模ITプロジェクトのマネジメント等、テクノロジーコンサルタントとしてクライアントの変革を支援。
全社アーキテクチャ、クラウド、セキュリティに関するエキスパート。

メンバー

秋田 修吾
Technology Strategy & Transformation
シニアマネジャー

土田 泰徳
Technology Strategy & Transformation
マネジャー

稲葉 高洋
Technology Strategy & Transformation
マネジャー

佐藤 佑哉
Technology Strategy & Transformation
マネジャー

南野 香澄
Technology Strategy & Transformation
マネジャー

白石 智一
Technology Strategy & Transformation
マネジャー

Deloitte.
デロイト トーマツ

デロイト トーマツ グループは、日本におけるデロイト アジア パシフィック リミテッドおよびデロイトネットワークのメンバーであるデロイト トーマツ合同会社ならびにそのグループ法人（有限責任監査法人トーマツ、デロイトトーマツ コンサルティング合同会社、デロイト トーマツ ファイナンシャルアドバイザリー合同会社、デロイトトーマツ税理士法人、DT弁護士法人およびデロイト トーマツ グループ合同会社を含む）の総称です。デロイトトーマツ グループは、日本で最大級のプロフェッショナルグループのひとつであり、各法人がそれぞれの適用法令に従い、監査・保証業務、リスクアドバイザリー、コンサルティング、ファイナンシャルアドバイザリー、税務、法務等を提供しています。また、国内約30都市に約1万7千名の専門家を擁し、多国籍企業や主要な日本企業をクライアントとしています。詳細はデロイト トーマツ グループWebサイト（www.deloitte.com/jp）をご覧ください。

Deloitte（デロイト）とは、デロイト トウシュ トーマツ リミテッド（“DTTL”）、そのグローバルネットワーク組織を構成するメンバーファームおよびそれらの関係法人（総称して“デロイトネットワーク”）のひとつまたは複数を指します。DTTL（または“Deloitte Global”）ならびに各メンバーファームおよび関係法人はそれぞれ法的に独立した別個の組織体であり、第三者に関して相互に義務を課しまたは拘束させることはありません。DTTLおよびDTTLの各メンバーファームならびに関係法人は、自らの作為および不作為についてのみ責任を負い、互いに他のファームまたは関係法人の作為および不作為について責任を負うものではありません。DTTLはクライアントへのサービス提供を行いません。詳細はwww.deloitte.com/jp/aboutをご覧ください。
デロイト アジア パシフィック リミテッドのメンバーおよびそれらの関係法人は、それぞれ法的に独立した別個の組織体であり、アジア パシフィックにおける100を超える都市（オークランド、バンコク、北京、ベンガルール、ハノイ、香港、ジャカルタ、クアラルンプール、マニラ、メルボルン、ムンバイ、ニューデリー、大阪、ソウル、上海、シンガポール、シドニー、台北、東京を含む）にてサービスを提供しています。

Deloitte（デロイト）は、監査・保証業務、コンサルティング、ファイナンシャルアドバイザリー、リスクアドバイザリー、税務、法務などに関連する最先端のサービスを、Fortune Global 500®の約9割の企業や多数のプライベート（非公開）企業を含むクライアントに提供しています。デロイトは、資本市場に対する社会的な信頼を高め、クライアントの変革と繁栄を促し、より豊かな経済、公正な社会、持続可能な世界の実現に向けて自ら率先して取り組むことを通じて、計測可能で継続性のある成果をもたらすプロフェッショナルの集団です。デロイトは、創設以来175年余りの歴史を有し、150を超える国・地域にわたって活動を展開しています。“Making an impact that matters”をパーパス（存在理由）として標榜するデロイトの約415,000名の人材の活動の詳細については、（www.deloitte.com）をご覧ください。

Member of
Deloitte Touche Tohmatsu Limited

IS 669126 / ISO 27001

BCMS 764479 / ISO 22301