クラウドコンピューティング
に関する考察

２０１２年３月２９日

企業内 ITC・IT ガバナンス研究会

はじめに

IT 業界を覆うクラウドコンピューティング（Cloud Computing）熱には、もはや“流行”を通り越したものすら感じる昨今である。

世界全体が未曾有の経済危機に陥ったことで、大規模なシステム受注が望めない現状にあって、IT ベンダーは、このコンピューティング・モデルに一縷の望みを託しているようだが、ユーザー企業にとっても、クラウドモデルは、コスト削減や開発期間短縮といった面から、今後の IT 戦略上、無視できない存在となっていくと思われる。

我々は、クラウドコンピューティングをどうとらえ、いかに採用に備えるべきかの指針を考え、クラウドコンピューティングの最適利用を導きたい。

2012年3月

執筆者　一同

【執筆メンバー　ITガバナンス研究会（アイウエオ順）】

坂本　徳明　　（0064952006C）
滝沢　　康　　（0012552001C）
千枝　和行　　（0029302004C）
古川　正紀　　（0005462001C）
牧田　一雄　　（0052712005C）

目次

2011 年度研究レポート

NIST によるクラウドコンピューティングの定義とリファレンスモデルの紹介

牧田　一雄

1. はじめに

クラウドコンピューティングという名前がよく耳にし、使われるようになってから数年が経過した。クラウドコンピューティングにおいては、ハイプ曲線の局面にとしては、黎明期を過ぎ、流行期に入った。昨年から今年にかけて、クラウドコンピューティングの大規模ユーザである米国政府においても、これまでの経過と、そこでの検討をもとにNIST(National Institute of Standards and Technology)から標準となる文書の公開に向けて、ドラフトが公開されている。このレポートでは、IT コーディネータが活動の参考になると思われる 2 つのドラフトを紹介する。

2. NIST によるクラウドコンピューティングの定義

クラウドコンピューティングが常に進化している中で、この定義はクラウドコンピューティングの重要な側面を特徴付けている。それはクラウドサービスと展開戦略の広範囲な比較の手段を支援し、何がクラウドコンピューティングを最良に使用するかを議論するベースラインとして提供される。

この文書は、当初 MS Word で作成された非常に短い非公式な文書として作成され、クラウドコンピューティングの浸透の経過に伴い、適切な定義になるように何回かの改変が繰り返された。この文書は現在、「The NIST Definition of Cloud Computing」のタイトルで、NIST Special Publication 800 Series のドラフトとして 2011 年初めに公開され、2011 年中に正式な文書に予定である。

この定義は、クラウドコンピューティングに関連する各種ガイドラインなどで一般的に使用されており、この定義を適切に理解し共通に使用することが重要である。この定義の概要は以下のとおりである。（なお、翻訳は IPA（独立行政法人情報処理推進機構）から公開されているものを利用した）

2.1. 定義

クラウドコンピューティングは、共用の構成可能なコンピューティングリソース（ネットワーク、サーバー、ストレージ、アプリケーション、サービス）の集積に、どこからでも、簡便に、必要に応じて、ネットワーク経由でアクセスすることを可能とするモデルであり、最小限の利用手続きまたはサービスプロバイダとのやりとりで速やかに割当てられ提供されるものである。このクラウドモデルは 5 つの基本的な特徴と 3 つのサービスモデル、および 4 つの実装モデルによって構成される。

2.2. 基本的な特徴

- オンデマンド・セルフサービス(On-demand self-service)
  ユーザは、各サービスの提供者と直接やりとりすることなく、必要に応じ、自動的に、サーバの稼働時間やネットワークストレージのようなコンピューティング能力

を一方的に設定できる。

- 幅広いネットワークアクセス(Broad network access)
  コンピューティング能力は、ネットワークを通じて利用可能で、標準的な仕組みで接続可能であり、そのことにより、様々なシンおよびシッククライアントプラットフォーム（例えばモバイルフォン、タブレット、ラップトップコンピュータ、ワークステーション）からの利用を可能とする。
- リソースの共用(Resource pooling)
  サービスの提供者のコンピューティングリソースは集積され、複数のユーザにマルチテナントモデルを利用して提供される。様々な物理的・仮想的リソースは、ユーザの需要に応じてダイナミックに割り当てられたり再割り当てされたりする。物理的な所在場所に制約されないという考え方で、ユーザは一般的に、提供されるリソースの正確な所在地を知ったりコントロールしたりできないが、場合によってはより抽象的なレベル（例：国、州、データセンタ）で特定可能である。リソースの例としては、ストレージ、処理能力、メモリ、およびネットワーク帯域が挙げられる。
- スピーディな拡張性(Rapid elasticity)
  コンピューティング能力は、伸縮自在に、場合によっては自動で割当ておよび提供が可能で、需要に応じて即座にスケールアウト／スケールインできる。ユーザにとっては、多くの場合、割当てのために利用可能な能力は無尽蔵で、いつでもどんな量でも調達可能のように見える。
- サービスが計測可能であること(Measured Service)
  クラウドシステムは、計測能力を利用して、サービスの種類（ストレージ、処理能力、帯域、実利用中のユーザアカウント数）に適した管理レベルでリソースの利用をコントロールし最適化する。リソースの利用状況はモニタされ、コントロールされ、報告される。それにより、サービスの利用結果がユーザにもサービス提供者にも明示できる。

2.3. サービスモデル

- ソフトウェア・アズ・ア・サービス（サービスの形で提供されるソフトウェア）
  SaaS(Software as a Service)
  利用者に提供される機能は、クラウドのインフラストラクチャ 2 上で稼動しているプロバイダ由来のアプリケーションである。アプリケーションには、クライアントの様々な装置から、ウェブブラウザのようなシンクライアント型インターフェイス（例えばウェブメール）、またはプログラムインターフェイスのいずれかを通じてアクセスする。ユーザは基盤にあるインフラストラクチャを、ネットワークであれ、サーバーであれ、オペレーティングシステムであれ、ストレージであれ、各アプリケーション機能ですら、管理したりコントロールしたりすることはない。ただし、

ユーザに固有のアプリケーションの構成の設定はその例外となろう。

- プラットフォーム・アズ・ア・サービス（サービスの形で提供されるプラットフォーム）PaaS(Platform as a Service)
  利用者に提供される機能は、クラウドのインフラストラクチャ上にユーザが開発したまたは購入したアプリケーションを実装することであり、そのアプリケーションはプロバイダがサポートするプログラミング言語、ライブラリ、サービス、およびツールを用いて生み出されたものである 3。ユーザは基盤にあるインフラストラクチャを、ネットワークであれ、サーバーであれ、オペレーティングシステムであれ、ストレージであれ、管理したりコントロールしたりすることはない。一方ユーザは自分が実装したアプリケーションと、場合によってはそのアプリケーションをホストする環境の設定についてコントロール権を持つ。
- インフラストラクチャ・アズ・ア・サービス（サービスの形で提供されるインフラストラクチャ）IaaA(Infrastructure as a Service)
  利用者に提供される機能は、演算機能、ストレージ、ネットワークその他の基礎的コンピューティングリソースを配置することであり、そこで、ユーザはオペレーティングシステムやアプリケーションを含む任意のソフトウェアを実装し走らせることができる。ユーザは基盤にあるインフラストラクチャを管理したりコントロールしたりすることはないが、オペレーティングシステム、ストレージ、実装されたアプリケーションに対するコントロール権を持ち、場合によっては特定のネットワークコンポーネント機器（例えばホストファイアウォール）についての限定的なコントロール権を持つ。

2.4. 実装モデル

- プライベートクラウド(Private cloud)
  クラウドのインフラストラクチャは、複数の利用者（例：事業組織）から成る単一の組織の専用使用のために提供される。その所有、管理、および運用は、その組織、第三者、もしくはそれらの組み合わせにより行われ、存在場所としてはその組織の施設内または外部となる。
- コミュニティクラウド(Community cloud)
  クラウドのインフラストラクチャは共通の関心事（例えば任務、セキュリティの必要、ポリシー、法令順守に関わる考慮事項）を持つ、複数の組織からなる成る特定の利用者の共同体の専用使用のために提供される。その所有、管理、および運用は、共同体内の 1 つまたは複数の組織、第三者、もしくはそれらの組み合わせにより行われ、存在場所としてはその組織の施設内または外部となる。
- パブリッククラウド(Public cloud)
  クラウドのインフラストラクチャは広く一般の自由な利用に向けて提供される。そ

の所有、管理、および運用は、企業組織、学術機関、または政府機関、もしくはそれらの組み合わせにより行われ、存在場所としてはそのクラウドプロバイダの施設内となる。

- ハイブリッドクラウド(Hybrid cloud)
  クラウドのインフラストラクチャは二つ以上の異なるクラウド・インフラストラクチャ（プライベート、コミュニティまたはパブリック）の組み合わせである。各クラウドは独立の存在であるが、標準化された、あるいは固有の技術で結合され、データとアプリケーションの移動可能性を実現している（例えばクラウド間のロードバランスのためのクラウドバースト)。

3. NIST によるクラウドコンピューティング・リファレンス・アーキテクチャ

米国政府へのクラウドコンピューティングの適合と、その導入は、多種多様の技術的、非技術的な要素に依存している。NIST によるクラウドコンピューティングの定義は、政府全域で使用できる全体フレームワークを記述するために必要とされた。そして、この文書はクラウドコンピューティングのコンポーネントと提供を高い精度でコミュミケートする NIST によるクラウドコンピューティング・リファレンス・アーキテクチャを提示する。

この文章は、「Overview」と「Architectural Components」の 2 つの章から構成されている。「Overview」は、リファレンス・アーキテクチャの 5 つの主要な登場人物、そしてそれらは役割と責任分担をもっている、について述べている。また、「Architectural Components」は、サービスの展開と組み合わせの重要な側面をのべている。

NIST によるクラウドコンピューティング・リファレンス・アーキテクチャは、クラウドサービスが提供する「what」への要求に焦点を当てている。ソリューションを設計し、導入するかの「how to」ではない。リファレンス・アーキテクチャは、クラウドコンピューティングにおける operational intricacies の理解を促進することに注力されている。

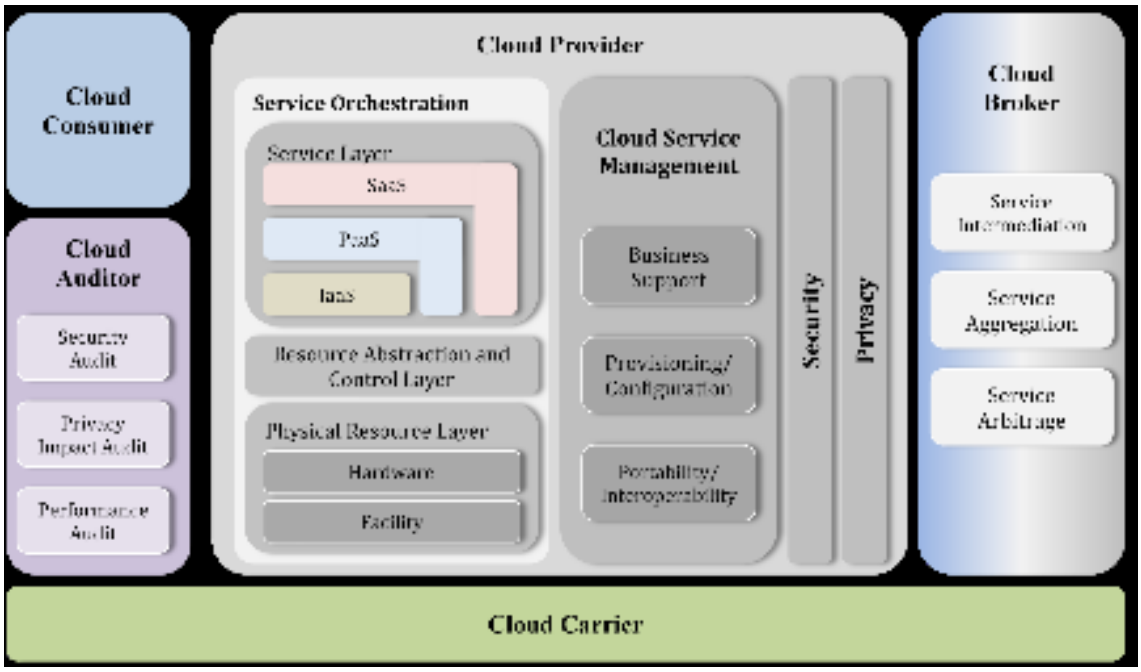
この文書は現在、「NIST Cloud Computing Reference Architecture」のタイトルで、NIST Special Publication 500 Series として 2011 年中に正式な公開される予定である。

なお、以下は著者による翻訳のため、誤訳や意味の取り違いの検証、および用語統一は十分になされていない。

3.1. 概要(Overview)

3.1.1. 概念リファレンスモデル

次の図は、「The NIST cloud computing reference architecture」の概要を表し、それらのクラウドコンピューティングにおける主な登場人物と、それらの動きと機能を示している。この図は汎用的なハイレベルなアーキテクチャを描いており、クラウドコンピューティングの要件、使用、特性と標準について理解を援助することを意図している。



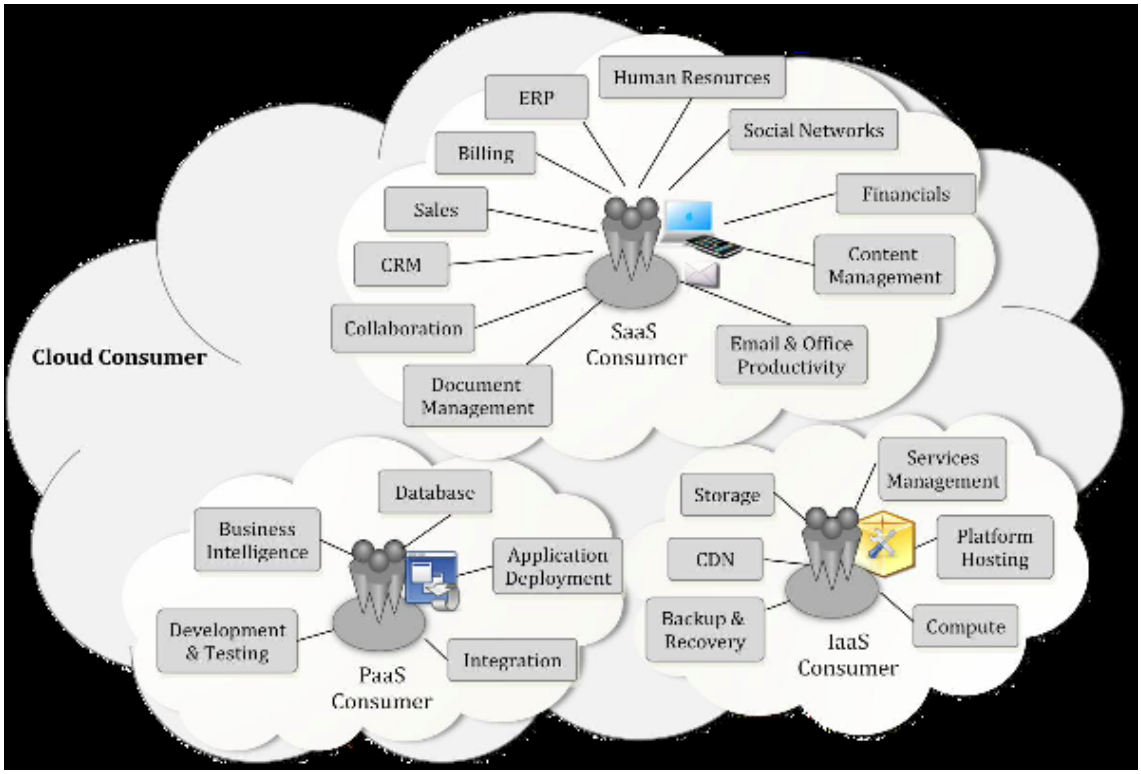
Cloud Consumer：ビジネスの関係を維持する人物、または組織、Cloud Provider からのサービスを使用する。

3.1.2. クラウド利用者(Cloud Consumer)

クラウド利用者は、クラウドコンピューティングサービスの主要なステークホルダーである。クラウド利用者は、クラウド提供者と取引関係を維持し、サービスを利用する人または組織である。クラウド利用者は、クラウド提供者からのサービスカタログを見て廻り、適切なサービスを要求し、クラウド提供者とのサービス契約を準備して、そしてサービスを利用する。クラウド利用者は、供給されたサービスに対する請求され、、それに従って支払いを手配する必要がある。

クラウド利用者は、クラウド提供者によって実現される技術的な性能要件を指定するための SLA が必要である。 SLA は、サービス品質、セキュリティ、性能障害に対する改善に関する条件をカバーすることができる。 また、クラウド提供者は、クラウド利用者が受け入れなければならい制限および義務のような、利用者に明確にすることができない約束の集合を、SLA の中にリストするかもしれない。クラウド利用者は、より良い価格設定とより有利な条件があるクラウド提供者を、自由に選ぶことができる。 通常、クラウド提供者の価格設定方針および SLA は交渉することができない。もし、利用者が多量の使用を予測し、より良い契約のための交渉をしようとしないかぎり。

要求されたサービスによって、活動および使用のシナリオは、クラウド利用者の中で異なる。 図はクラウド利用者に利用可能なクラウドサービスのいくつかの例を提示する。



クラウドの中の SaaS アプリケーションは、ネットワークを通してクラウド利用者へアクセスできる。 SaaS 利用者は、ソフトウェアアプリケーションへのアクセスをメンバーに提供する組織、ソフトウェアアプリケーションを直接使用するエンドユーザ、またはエンドユーザのアプリケーションを構成するソフトウェアアプリケーション管理者がなれる。SaaS 利用者は、エンドユーザの数、使用時間、利用されたネットワークの帯域幅、保存されたデータの量または保存されたデータの期間に基づいて請求される。

PaaS のクラウド利用者は、クラウド環境の中にホストされたアプリケーションの開発、テスト、配布および管理のために、クラウド提供者によって提供されたツールや実行資源を使用することができる。PaaS 利用者は、アプリケーションソフトウェアを設計し、導入するアプリケーション開発者、クラウドベースの環境の中でアプリケーションを実行し、テストするアプリケーションテスター、クラウドの中にアプリケーションを発行するアプリケーション配布者、およびプラットフォーム上でアプリケーションの実行を構成し、監視するアプリケーション管理者がなれる。PaaS 利用者は、PaaS アプリケーションによって使用される処理、データベース・ストレッジおよびネットワーク資源、そしてプラットフォームの使用期間に従って請求される。

IaaS の利用者は、彼らが任意のソフトウェアを配備し実行できる仮想コンピュータ、ネットワーク経由アクセス可能ストレッジ、ネットワーク・インフラストラクチャ・コンポーネント、およびその他の基本的なコンピューティング資源にアクセスを持っている。IaaS の利用者は、IT インフラストラクチャの運用のためのサービスの作成、導入および監

視に関心を持っているシステム開発者、システム管理者、および IT マネージャがなれる。IaaS 利用者は、これらのコンピューティング資源にアクセスする能力が提供され、仮想コンピュータによって使用された CPU 時間、保存されたデータの量と期間、使用されたネットワーク大域幅、ある期間に使用された IP アドレスの数のような、使用した資源の量および期間に従って請求される。

3.1.3. クラウド提供者(Cloud Provider)

クラウド提供者は人あるいは組織であり、それは利害関係者に利用可能なサービスの作成に責任を持っている実体である。クラウド提供者は、サービスを提供するために必要なコンピューティングインフラストラクチャを取得、管理し、サービスを提供するクラウドソフトウェアを実行し、そしてネットワークアクセスを通してクラウド利用者に対するクラウドサービスを提供するための手配をする。

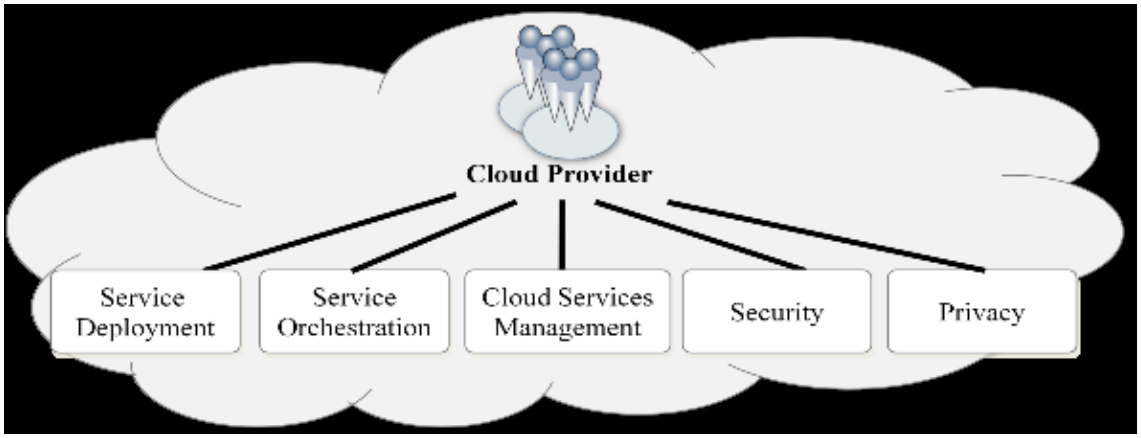
SaaS に関しては、クライド提供者は、クラウド利用者が期待するサービスレベルでサービスが提供されるように、クラウドインフラストラクチャの上でソフトウェアアプリケーションの運用を展開、構成、維持、そして更新する。SaaS の提供者は、アプリケーションとインフラストラクチャの管理と制御における責任の大部分を引き受ける。一方、クラウド利用者はアプリケーションの限定された管理のコントロールを持っている。

PaaS に関しては、クラウド提供者はプラットフォームのためのコンピューティングインフラストラクチャを管理し、プラットフォームのコンポーネントを提供するクラウドソフトウェアを実行します。実行時ソフトウェアの実行スタック、データベースおよびその他のミドルウェアコンポーネントのような。PaaS クラウド提供者はまた、通常、提供されたツールによる開発、展開およびプロセスの管理を支援する。統合開発環境(IDEs)、クラウドソフトウェアの開発用バージョン、ソフトウェア開発キット(SDKs)、展開および管理ツールのような。PaaS クラウド利用者は、アプリケーションとホストティングの環境設定のおそらくいくつかのコントロールを持つ。しかし、ネットワーク、サーバ、オペレーティングシステム(OS)、またはストレージのようなプラットフォームの基礎となるインフラストラクチャへはアクセスできないか、または限られたアクセスを持つ。

IaaS に関しては、クラウド提供者は、サービスの基礎となる物理的なコンピューティング資源を取得する。サーバ、ネットワーク、ストレージ、およびホスティング・インフラストラクチャを含んで。クラウド提供者は、サービス・インタフェイスとコンピューティング資源の抽象概念の集合を通して、IaaS クラウド利用者にコンピューティング資源を利用可能にするのに必要なクラウドソフトウェアを実行させる。仮想マシン、仮想ネットワーク・インターフェイスのような。向きを変えて、IaaS クラウド利用者は、彼らの基本的なコンピューティング・ニーズのために、これらのコンピューティング資源を使用する。仮想コンピュータのような。 SaaS と PaaS のクラウド利用者と比較して、IaaS クラウド利用者はコンピューティング資源のより基本的な形態にアクセスする。そしてその結果、

近づく手段を持っていて、その結果、OS やネットワークを含めてアプリケーションスタックの中のより多くのソフトウェアコンポーネントのコントロールを持つ。他方では、IaaS クラウド提供者は、これらのインフラストラクチャ・サービスの提供を可能にする物理的なハードウェアとクラウドソフトウェアのコントロールを持つ。たとえば、物理的なサーバ、ネットワーク機器、記憶装置、ホスト OS および仮想化のためのハイパバイザ。

クラウド提供者の活動は、5 つの主要なエリアで説明される。クラウド提供者はサービス展開、サービスオーケストラ編成、雲のサービス管理、セキュリティ、およびプライバシーのエリアでそれの活動を主導する。セクション 3 で詳細について議論する。



3.1.4. クラウド監査者(Cloud Auditor)

クラウド監査者は、その結果で意見を表明する目的で、クラウドサービスの統制に関する独自の検査を実施するこができる関係者である。監査は、客観的証拠の検証を通して、規格への適合について検査するために実行される。 クラウド監査者は、セキュリティ・コントロール、プライバシー影響、性能などの点から、クラウド提供者によって提供されるサービスの評価をおこなうことができる。

監査は、連邦政府機関に対しては特に重要である。「政府機関は、クラウド提供者のセキュリティ・コントロールを評価するために第三者を可能にする契約条項を含むべきである」なので。セキュリティ・コントロールは、システムとそれの情報の秘密性、完全性、および可用性を保護するために組織内の情報システムの中で使われる管理、運用、そして技術的な安全装置または対策である。セキュリティ監査のために、クラウド監査者は、情報システムのセキュリティ・コントロールの評価を作成することできる。コントロールが、正しく導入され、意図したように運用し、システムに対するセキュリティ要件に関係する望ましい成果を生産していることの程度を決定するために。また、セキュリティ監査は、規則とセキュリティポリシーへのコンプライアンスの検証を含むべきである。 例えば、監査者は、管轄の関連する規則に従ってデータの保持に正しいポリシーが適用されることを保証することを課される。監査者は、確定された内容が変更されていないこと、法的およ

びビジネスのデータの公文書の要件を満たしていることを保証するだろう。

プライバシー影響監査は、個人のプライバシーを統治する適用可能なプライバシー法と規則の遵守することため、そして開発と運用のすべての段階で個人情報の秘密性、完全性、および可用性を保証することを、連邦政府機関を助けることができる。

3.1.5. クラウド・ブローカ(Cloud Broker)

クラウドコンピューティングの発展として、クラウドサービスの統合はクラウド利用者にとって管理するにはより複雑になりすぎる。クラウド利用者は、直接クラウド提供者に接触する代わりに、クラウドブローカにクラウドサービスを要求するかもしれない。クラウド・ブローカは、クラウドサービスの使用、性能、および配送を管理する実体であり、クラウド提供者とクラウド利用者の間の関係を交渉する。

一般に、クラウド・ブローカは 3 つのカテゴリーのサービスを提供できる。

- サービスの仲介：クラウド・ブローカは、何らかの特定の能力の改善やクラウド利用者への付加価値サービスの提供により既存のサービスを強化する。改良は、クラウドサービスへのアクセス管理、ID 管理、性能報告、強化されたセキュリティなどである。
- サービスの集合：クラウド・ブローカは、複数のサービスを 1 つまたはそれ以上の新しいサービスに結合し統合する。ブローカーは、クラウド利用者と複数のクラウド提供者の間のデータ統合をしたり、安全なデータ移動を保証する。
- サービスの仲裁：サービスの仲裁は、集められるサービスが固定されないことを除いて、サービスの集合に類似している。サービスの仲裁は、ブローカは複数の機関からサービスを選択する柔軟性を持っていることを意味する。例えば、クラウド・ブローカは、最も良いスコアを持っている機関を測定し選択するために、信用スコアを使用することができる。

3.1.6. クラウド・キャリア(Cloud Carrier)

クラウド・キャリアは、クラウド利用者とクラウド提供者の間の接続性とクラウドサービスの輸送を提供する仲介者として行動する。クラウド・キャリヤは、ネットワーク、電気通信、および他のアクセスデバイスを通して利用者へのアクセスを提供する。 例えばクラウド利用者は、コンピュータ、ラップトップ、携帯電話、モバイルインターネットデバイス(MIDs)などのようなネットワークアクセスデバイスを通してクラウドサービスを得ることができる。クラウドサービスの配布は、通常、ネットワークと電気通信のキャリヤ、または輸送機関によって提供される。そこで輸送機関は、大容量ハードドライブのような記憶媒体の物理な輸送を提供する企業を参考にしている。 クラウド提供者は、クラウド利用者へ提示されるＳＬAs のレベルと一致したサービス提供するためにクラウド・キャリアと SLA を設定するだろう、そしてクラウド利用者とクラウド提供者との間の専用で安全な

接続の提供をクラウド・キャリアに要求するかもしれないことを注意する。

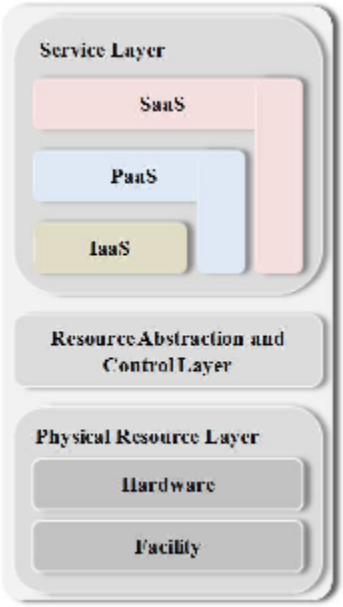
3.2. アーキテクチャ・コンポーネント(Architectural Components)

3.2.1. サービスの展開

NIST クラウドコンピューティングの定義で特定されるように、クラウド・インフラストラクチャは次の展開モデルのひとつで運用されるだろう：パブリッククラウド、プライベートクラウド、コミュニティクラウド、またはハイブリッドクラウド。 違いは、コンピューティング資源がクラウド利用者にどのような排他性が作られるかに基づいている。

3.2.2. サービスの組み合わせ(Service Orchestration)

サービスの組み合わせは、クラウド利用者へクラウドサービスを提供するために、コンピューティング資源の手配、調整および管理におけるクラウド提供者の行動を支援するためのシステム・コンポーネントの構成を参照する。図 15 は、クラウドサービスの提供を支えるこの構成の一般的なスタック・ダイアグラムを提示している。



この表現の中では 3 層モデルが使用されている。クラウド提供者は彼らのサービスを提供するために構成することが必要である、システム・コンポーネントの 3 つのタイプのグループを表現している。

この図が示しているモデルの中で、上位は *Service Layer* で、ここではクラウド提供者が、クラウド利用者がコンピュータ・サービスへアクセスするためのインタフェースを定義している。 3 つのサービスモデルのそれぞれのアクセス・インタフェースは、この層で

提供される。 SaaS アプリケーションは PaaS コンポーネントの上位に構築でき、PaaS コンポーネントは IaaS コンポーネントの上位に構築できるといことは可能であるが、必ずしも必要ではない。SaaS、PaaS、および IaaS コンポーネントの中の任意の依存関係は、お互いの上で積み重ねられるコンポーネントとしてグラフィカルに表現される。 一方、コンポーネントの釣りは、サービス・コンポーネントのそれぞれが、それ自体によって成り立っていることを表現している。例えば、SaaS アプリケーションは、IaaS クラウドからの仮想マシンの上に実装され、ホストされる。または、IaaS の仮想マシンの使用無しに、クラウド資源の上位に直接実装される。

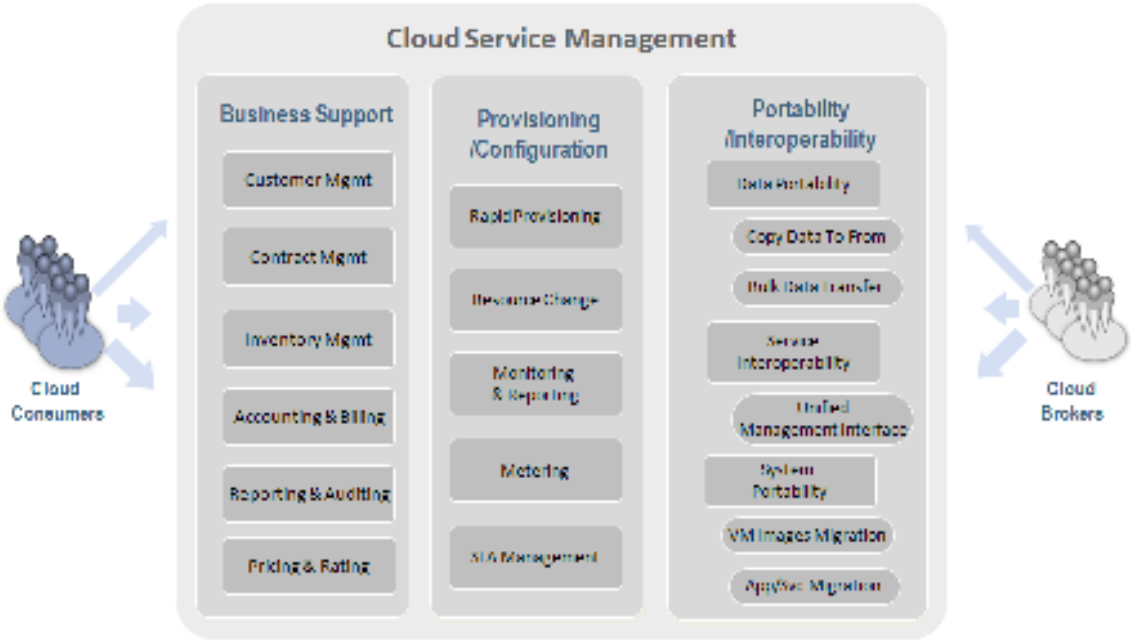
モデルの中間の層は、*Resource Abstraction and Control Layer* である。この層は、クラウド提供者がソフトウェア抽象化を通して物理的なコンピュータ資源へのアクセスの提供と管理のために使用する、Resource Abstraction コンポーネントの例としては、ハイパーバイザ、仮想マシン、仮想データストレージおよび他のコンピューティング資源の抽象化のような、ソフトウェア要素を含んでいる。資源の抽象化は、基礎となる物理的な資源の効率的で、安全で、信頼できる使用を確実にするために必要である。仮想マシン技術はこの層で一般的に使用される一方、必要なソフトウェアの抽象化を提供する他の手段もまた可能である。 この層の Control の面は、資源配分、アクセス・コントロール、使用状況の監視に責任を持つ、ソフトウェア・コンポーネントに関係する。これは、多数からなる基礎となる物理的な資源と、リソースプーリング、動的割当て、および測定サービスを可能にするソフトウェアの抽象化を相互に結びつける、ソフトウェアの構造である。様々なオープンソースと独占販売のクラウドソフトウェアは、このタイプのミドルウェアの例である。

スタックの最下位の層は、*Physical Resource Layer* である。それは、すべての物理的なコンピューティング資源を含んでいる。この層は、ハードウェア資源を含んでいる。コンピュータ(CPU とメモリ)、ネットワーク(ルータ、ファイアウォール、スイッチ、ネットワークリンク、およびインタフェース)、ストレージコンポーネント(ハードディスク)および他の物理的なコンピューティング・インフラストラクチャの要素のような。また、それは、施設の資源を含んでいる。加熱、換気、空調(HVAC)、電源、通信、および物理的な施設の他の面のような。

システム・アーキテクチャ・コンベンションに続いて、すなわち、水平位置調整、モデルにおけるレイヤは依存関係を表す。上位の層のコンポーネントは、機能するために隣接している下位の層に依存する。 Resource Abstraction and Control Layer は、Physical Resource Layer の上位で仮想クラウド資源をさらし出す。そして、クラウド・サービス・インタフェースがクラウド利用者にさらし出される場所である Service Layer を支援する。一方、クラウド利用者は、物理的な資源への直接的なアクセスを持っていない。

3.2.3. クラウドサービス・マネジメント(Cloud Service Management)

Cloud Service Management は、サービスに関連する機能のすべてを含んでいる。それは、クラウド利用者に要求または提案されたそれらのサービスの管理と運用のために必要である。図 16 で説明されるように、Cloud Service Management は、*Business Support*、*Provision and Configuration*、そして *Portability and Interoperability* の観点の要件を記述される。



3.2.3.1. Business Support

Business Support は、クライアントとの取引し、プロセスをサポートするビジネスに関連したサービスの集合を伴う。 それはクライアント面であることであることである営業活動を実行するのに使用されるコンポーネントを含んでいます。

- *Customer manegrment* : 顧客のアカウントを管理する、アカウントのオープン／クローズ／終了、ユーザープロファイルの管理、連絡窓口の提供と顧客の問合せと問題の解決による顧客との関係の管理など。
- *Contract management* : サービス契約を管理する。契約の準備／交渉／クローズ／終了など。
- *Inventory Management* : サービスカタログの準備する、管理する、など。
- *Accounting Billing* : 請求情報を管理する、請求書を送る、受け取った支払いを処理する、送り状を追跡する、など。
- *Reporting and Auditing* : ユーザの運用をモニターする、レポートを生成する、など。
- *Pricing and Rating* : サービスを評価し、価格を決定する、販売促進やユーザーの

履歴に基づく価格設定の規則を取り扱う、など。

3.2.3.2. Provision and Configuration

- *Rapid provisioning* : 要求されたサービス／資源／能力に基づいて、クラウドシステムを自動的に配備する。
- *Resource changing* : 修理、増強、クラウドへの新しいノードの結合のための構成や資源割当てを調整する。
- *Monitoring and Reporting* : 仮想資源の状況を知り、モニターする、クラウドの運用と事象をモニターする、そして性能レポートを生成する。
- *Metering*:サービスのタイプを充当された抽象化のあるレベルにおける能力の計測結果を提供する。(例えば、ストレージ、処理、帯域幅、および活動中のユーザアカウント)。
- SLA Monagement : SLA の契約の定義（QoS パラメタによる基本的スキーム)、SLA のモニター、定義されたポリシーに従う SLA の実施を包含する。

3.2.3.3. Portability and Interoperability

クラウドコンピューティングの増殖は、技術的なインフラストラクチャおよびより速いソフトウェアの更新においてコストの節減を約束する。他の潜在的クラウドコンピューティング顧客と共に、米国政府はクラウドへの移行に強い関心を持っている。 しかし、クラウドコンピューティングの採用は、クラウドがセキュリティ、移植性、および相互運用性に関するユーザの心配をどのように処理できるかに、大いに依存している。このセクションは、移植性と相互運用性のための要件について簡潔に論じる。セキュリティは、別のセクションで扱われる。

移植性について、見込み客は、彼らは彼らのデータまたはアプリケーションを、少ない費用と最少の混乱で、複数のクラウド環境に跨って移動できるかどうか知ることに関心をもっている。相互運用性の関連では、ユーザは、複数のクラウドの間、または中で交信する能力について心配している。

クラウド提供者は、データ移植性、サービス相互運用性、およびシステム移植性を支援する仕組みを提供しなければならない。 データ移植性は、データ・オブジェクトをクラウドの中へ、または外へコピーするための、または大量のデータ移送のディスクを使用するためのクラウド利用者の能力である。サービス相互運用性は、統一された管理インタフェースを使用して、複数のクラウド提供者を跨って、彼らのデータとサービスを使用するためのクラウド利用者の能力である。システム移植性は、完全停止した仮想マシン・インスタンス、またはマシン・イメージを、ある提供者から他の提供者へ移行することを許す。または、アプリケーション、サービスおよび彼らのコンテンツを、あるサービス提供者から他へ移行する。

数多くのクラウドサービス・モデルは、移植性と相互運用性に関連する異なった要件を持っているかもしれないということに注意しなければならない。例えば、IaaS は、新しいクラウドにテーダを移行することやアプケーションの実行する能力が必要とする。従って、仮想計算機のイメージをキャプチャし、異なった仮想化技術を使用しているかもしれない新しいクラウド・プロバイダに移行することが必要である。 VM イメージへのいかなるどプロバイダ固有の拡張は、除去される必要がある。移植するのに移されるか、または記録される必要があります。 一方 SaaS ではデータの移植性に焦点が当てられ、その結果、標準フォーマットでのデータの抽出とバックアップを実行するのが重要になる。

3.2.4. セキュリティ

セキュリティが、規範モデルのすべての層の向こう側にわたるアーキテクチャの十字を切る局面であると認めるのは、重要です、物理的なセキュリティからアプリケーションセキュリティまで及んで。 したがって、また、Cloud Providers が唯一範囲の下にあるのではなく、クラウドコンピューティングアーキテクチャ関心におけるセキュリティはあります。

Consumers と他の関連俳優を曇らせてください。 雲のベースのシステムは、まだセキュリティが認証や、承認や、有用性や、秘密性や、アイデンティティ管理や、保全や、監査や、セキュリティモニターや、インシデントレスポンスや、安全保障政策管理などの必要条件であると扱う必要があります。 これらのセキュリティ要件が新しくない間、私たちは助けへの特定の見解が雲系でセキュリティを議論して、分析して、実装する雲について議論します。

3.2.4.1. クラウドサービス・モデルの展望

NIST のクラウドコンピューティング定義で特定された 3 つのサービスモデル、すなわち、SaaS、PaaS および IaaS が、異なったタイプのサービス管理の運用を利用者に提示し、そしてクラウドシステムへの異なったエントリーポイントを露出させる。そして、それは敵のために異なった攻撃する面を作る。したがって、クラウドサービス・モデルの影響とセキュリティの設計と実装におけるそれらの異なる課題を考慮することが重要である。 例えば、SaaS は、ネットワークの接続を使用して、クラウドの提供へのアクセスで利用者に提供される。通常インターネット上で、ウェブブラウザを通して。SaaS クラウドシステムのセキュリティの課題では、ウェブブラウザのセキュリティが強調される。 IaaS のクラウド利用者は、ホストのハイパーバイザの上で実行される仮想マシン(VMs)が提供される。したがって、VM 分離を達成するためのハイパーバイザのセキュリティが、仮想化技術を使用する IaaS クラウド提供者のために広範囲にわたって研究されてきた。

3.2.4.2. クラウド展開モデルの含意（言外の意味）

前出のセクションで議論したクラウド展開モデルの種類は、重要なセキュリティの含意がある。 展開モデルの展望からセキュリティ含意を見る 1 つの方法は、展開モデルでのテナントの排他性の異なりのレベルです。プライベートクラウドは、1 つの利用者の組織に専用に提供される。一方、パブリッククラウドは、予測できないテナントが相互に共存することができる。従って、ワークロード分離は、パブリッククラウドよりプライベートクラウドがセキュリティの関心はより少ない。 クラウド展開モデルのセキュリティの影響を分析する別の方法は、アクセスの境界の概念を使用することである。例えば、オンサイト・プライベートクラウドは、クラウド利用者の組織のネットワークの境界内にプライベートクラウドをインサイトにホストされた時、クラウドの境界で追加の境界制御装置が必要かもしれないし、そうでないかもしれない。一方、外部にソースされたプライベートクラウドは、クラウドの境界で境界線保護の確立を要求する傾向がある。

3.2.4.3. 共有されたセキュリティ責任

前出のセクションで議論したように、クラウド提供者とクラウド利用者は、クラウドシステムの中のコンピューティング資源に対して統制の異なる程度を持っている。伝統的な IT システムと比較して、そこでは 1 つの組織がコンピューティング資源の集積全体とシステムのライフサイクル全体に対して統制を持っている、クラウド提供者とクラウド利用者は、協力してクラウドベースのシステムを設計、構築、展開、運用する。統制の分割は 、双方の組織がクラウドベースのシステムに適切な保護を提供する責任を共有（分担）することを意味する。セキュリティは共同責任である。セキュリティ統制は、つまり、保護を提供するために使用される測定は、どちらの組織が実装のためにより良い位置にいるか判断するために分析される必要がある。どこの分析は、サービスモデルの展望からの考慮を含む必要がある。そしてそこでは、異なったサービスモデルがクラウド提供者とクラウド利用者の間の統制の異なった程度度合いを暗に意味している。例えば、IaaS シナリオの初期のシステム特権ユーザのためのアカウントマネジメント統制は、IaaS 提供者により通常実行される。一方、IaaS 環境で展開されたアプリケーションのためのアプリケーションユーザアカウント管理は、通常プロバイダーの責任ではない。

3.2.5. 個人情報保護

クラウド提供者は、クラウド内での個人情報(PI)と個人識別情報(PII)の確実で、適切で、一貫した収集、処理、コミュニケーション、使用および状態を保護しなければならない。連邦政府 CIO カウンシルによると、連邦政府の重要業務命令の 1 つは、集めた個人識別情報の個人情報保護を確実にすることである。PII は、個人を識別し追跡するために使われる情報である。 名前、社会保険番号、生体記録のような。単独または他の個人や識別情報と結合した時、特定の個人に連係、または連係可能となる。誕生日、出生地、母親の旧姓のような。クラウドコンピューティングは共用資源、ソフトウェアおよび情報の自由度のあ

る解決法を提供するが、それはまた、クラウドを使用する利用者への追加の個人情報保護の挑戦を引き起こす。

4. まとめ

このレポートでは、NIST から公開された「NIST によるクラウドコンピューティングの定義」および「NIST によるクラウドコンピューティング・リファレンス・アーキテクチャ」を紹介した。現在多くのクラウドサービスが、IT ベンダーやプロバイダから提供している。IT コーディネータがクライアントの経営課題の解決を支援するために必要な IT 戦略を適切に計画し、確実に実施するための選択肢としてクラウドコンピューティングは必ずスコープに入ってくる。この状況において、IT コーディネータが適切な助言をクライアントに提供するために、当レポートが役に立てば幸いである。

● 参考文献

- ◆ The NIST Definition of Cloud Computing
- ◆ NIST によるクラウドコンピューティングの定義
- ◆ NIST Cloud Computing Reference Architecture

ＩＴガバナンスからみたクラウドコンピューティングの研究
～　ビジネスリスクに対応するために　～

ＩＴガバナンス研究会
千枝　和行

１．はじめに

既にわが国においてもクラウドコンピューティングのビジネスが活発化してきている。

東日本大震災の被災地では、基幹業務のサーバーが何らかの被害を受けて使用不能になったり、情報の利用が困難になったりして、情報資産のダメージを生じるケースが多数発生し、改めてビジネスリカバリー対策として注目されている。クラウドであれば、ネットワークさえつながればすぐにでも再利用が可能で、ビジネスの立ち上がりが早いことが期待できるからである。当然サービスを提供するメーカーやベンダーもビジネスチャンスと捉え、売り込みに躍起になっている。

情報システムの技術は、１９９０年代半ばにはビジネス上必要な技術が確立したため、１０数年間大きな進展が見られなかった。そのため、ＩＳＭＳや個人情報保護法などに代表される様に、セキュリティポリシーやリスク対策などの分野にシステムビジネスの方向がフォーカスされていた。

クラウドコンピューティングは数万台を連結した大容量サーバー群にソフトウェアを搭載し、利用形態に従った従量制の課金で利用者にシステム環境を開放する仕組みである。技術としては既に開発されていたが、使われていなかった技術を集積して「規模の経済」を実現することができた。そのことによって、新しいビジネス分野が開拓され、普及し、ビジネスが活性化されることへの期待感が大きい。

クラウドコンピューティング特徴をＱＣＤ（早い、美味い、安いの吉野家）的に表現すると、

①早い　　・システム立ち上げの短縮化
②美味い　・業務の可視化（モニタリング）
　　・ソフトの柔軟化（選択肢）
　　・ビジネスの安全化
　　・品質チェックの義務化（不味い）
③安い　　・費用のスケーラブル化

そして

④新しい　・コンピュータ資源（業務規模）のスケーラブル化

である。

一方、利用する企業側は新技術といえど経営統制（ガバナンス）の一環として機能していなければビジネスリスクを負うことになり、それが実際に発生した場合には経営上のインパクトが大きいことが想定される。

本稿は、前年度の研究に引き続きＩＴガバナンスとビジネスリスクの観点から論ずることとする。

２．経営上のＩＴガバナンスとしてのポイント

（１）経営上のＩＴとリスクマネジメント

東日本大震災を初めとして、日本における経営環境は今まで以上に速いスピードで変化が進んでいる。ＩＴの効率的な利用と同時に、今回は事業継続（ＢＣＰ） に対して十分な対策を取っていなかった企業が大きな痛手を受けることになった。現状の評価を行いながら、効果的な投資と同時に経営によるガバナンスが必要とされる。

①不確実な経営環境の中で（ＩＴ）投資効果とリスクのバランス点を模索。

外部環境としては、長期的に人口動態の変化による国内経済のＧＤＰの減少予測、中国への企業進出の成熟化と消費のバブル化、東南アジアへ企業進出のシフト化、広域経済圏の推進などが経営環境として発生しており、より一層の効率化と投資の効果を求めなければ経営基盤を大きく損ねかねない。

内部環境としては、ＢＣＰ対策の遅れ、商品ライフサイクルの短縮化、部品調達の停滞、モチベーション低下などが問題となる。

これらの急激な環境変化に対応するために、全社的なリスク分析を行い、補強すべき分野を特定し、優先順位をつけて投資を行うことになる。

それに伴ってＩＴ投資も同様に十分なリスク分析を行い、限られた予算の中から効果的かつ効率的な投資を行わなければ、他社に遅れをとる要因になりかねない。

②受容できる経営上のリスクレベルを決定。

リスク分野特定とリスクの大きさの特定ができたら、経営上の許容できるリスクレベルを項目ごとに決定していく。

リスクを無くすか、低減するか、回避するか、さもなくば許容することを項目ごとに決め、経営者の承認を得ておく。

決定したリスク対応は、全社に公開され周知されなければならない。

③リスク低減の為、どのＩＴ分野に投資を行なうかを選択。

ビジネスリスクの大きさに従って、リスクを低減しなければならない項目に関し、対象とする分野と優先順位付けの整理を行う。

その中でＩＴ投資によって改善できる項目は、関係者が同様に分析・整理を行い、全体との整合性を取りながら改善提案する。

④適切なセキュリティとコントロールが存在することを証明。

計画に従って実行策を実施し、結果を注視する。ＩＴを使ったリスク低減のためのプロセス改善やリスクの低減効果については、経営レベルの管理指標としてＫＧＩを設定し、稼動後はモニタリングを行う。

モニタリング結果を初期の目標値と照らし合わせ、そのコントロールによる目標の達成度合いの評価を行い、達成していない項目に関しては、改善策を検討する。

以上の内容は経営者に答申し、承認を貰っておく。

（２）ＩＴを使用してビジネス目的を達成

ＩＴを使用してビジネス目的を達成していくことは、継続作業である。中長期的な目標とＩＴのアーキテクチャを設定し、毎年ローリングしながら推進しなければならない。

ビジネスとＩＴを融合させるには、ビジネス要件に基づいたＩＴのアーキテクチャを構築しておく必要がある。

しかもただ単に構築されているだけではなく、ＩＴがもたらすビジネス上の改善が経営目標の改善と一致していることを説明する指標（ＫＧＩ）が設定され、アーキテクチャの中に組み込まれ、測定され、評価されるＰＤＣＡが存在し、経営者に報告され、評価されていることが必要である。

経営者の評価と意思決定のため、指標設定とモニタリングが行なわれ、評価される仕組みが存在する必要がある。

（３）ＩＴガバナンス

ＩＴが利用され効果を発揮していることを経営的な管理の下に行われていることを証明するためには、ＩＴガバナンスが存在することを証明しなければならない。

まず、経営戦略に基づいてＥＡ（エンタープライズアーキテクチャ）の設計・構築が行われ、ＥＡに基づいて各業務プロセスを改善する業務システムが稼動されている必要がある。

業務システムが初期の性能を発揮することを確認するには管理指標（ＫＰＩ）を設定

し、システム上にモニタリング可能な機能を組み込み、モニタリングし、結果を収集・分析評価し、初期目標との乖離度を評価する。

評価に当たっては、ベストプラクティス等の外部の客観的データと照合して行うことが望ましい。

評価結果は経営者に報告され、その評価を受けておく。

経営者の承認の元、改善のための是正措置・予防措置を実施し、更にモニタリングを継続する。

このようなＩＴに関するＰＤＣＡの流れを確立し、モニタリングと改善の業務プロセスを通して、ＩＴガバナンスが存在することを立証することができる。

３．クラウドコンピューティングのＩＴ統制

（１）ＩＴ基本戦略の見直し

クラウドコンピューティングは、従来のＩＤＣやＡＳＰとは少し違った側面を持っているので、その特性を十分研究し、ＩＴ戦略の中に取り入れていかなければならない。

①ＩＴ統制ポリシーの見直し。

ＩＴを統制するためのポリシーは、ＩＴ環境の変化によって当然見直さなければならない。

クラウドコンピューティングの場合は、自社の重要情報が丸ごと外部の管理に委託される場合もあり、統制項目にしたがって見直しをする必要がある。

特に、従来は自社内若しくは協力会社との関係までを考慮すればよかったのが、システムの受託者の規範や管理水準にまで踏み込まなければならないので、場合によっては内容に大幅な修正を加えなければならないケースも想定される。

②ＩＴが達成すべき機能を経営者からのステートメントとして見直し。

従来の自社内、もしくは協力会社むけの内容だけではなく、受託者に要求すべき内容を経営者のステートメントとして、ステークホルダーに対して明確に示しておく必要がある。

③ＩＴを統制する組織体と意思決定方法を見直し。

ＣＩＯ（情報システム担当役員）を中心に、ＩＴをコントロール組織が構築されているのが望ましいが、クラウド化するということは更に企業情報の管理を外部に委託することになるので、意思決定方法を見直す必要がある。

特にインシデントが発生した場合のエスカレーション方法・レベルについては、リスクのケースに従ってし細かく設定しておく必要がある。

（２）ＩＴ統制組織体（委員会）による統制

先に述べたとおり、ＣＩＯを中心にＩＴをコントロール組織が構築されているのが望ましいが、情報喪失・情報漏洩の重要性に鑑み、委員会による統制をより明確にしておく必要がある。

①ＩＴ基本戦略の見直し。

クラウド化することによる競争相手への差別化の方法は、その企業の業界・業態によって異なる。

クラウドの特性である「システム立ち上げの短縮化」、「業務の可視化（モニタリング）」、「ソフトの柔軟化（選択肢）」、「費用やＩＴ規模のスケーラブル化」などを取り入れて差別化を図ることが重要である。

例えば、一時的に大量のＣＰＵ資源を使って研究するなどの場合、一時的なプロジェクトなどでは、自社でＩＴ資源を保有せずクラウドを利用して対応するほうが、トータルコストは安くて済む。

企業環境の変化の認識、従来の戦略からの相違点の調査、改善すべきプロセスの選定などを行って戦略の見直しを行う。

②ＥＡ（企業全体のＩＴ／ビジネス構造）の見直しと設計。

企業環境の変化に基づいて、ＥＡの見直しも行われなければならない。ＥＡは経営コントロールとＩＴコントロールを結びつける重要な機能を持っているので、慎重に再検討される必要がある。

③ＩＴ構成とプロセスの再評価。

自社のシステムの構成要素の洗い出しと整理が行われている必要がある。

通常の企業であれば、２０００年問題やアウトソーシング検討時に洗い出しが行われいるはずである。

これらの情報を元にクラウド化すべき分野の特定と選定を行い、委員会で検討され承認されておく必要がある。その際、具体的なビジネスリスクやビジネスインパクトが考慮されていることが望ましい。

④長期ＩＴ投資計画の立案と予算化。

クラウド化を含めたＩＴの投資計画に関し、短期のみならず長期計画をローリングで立案し、予算化しておく。

⑤計画の実施と結果の評価。

ビジネスリスクを回避し、競合他社への差別化を図るため、ＩＴ投資の実施を行い、それをモニタリングし、予め設定したＫＰＩと比較しながら評価し、委員会の承認を経て経営者に報告する。

必要に応じて是正措置、予防措置を行う。

（３）ＩＴ計画の実施

クラウドコンピューティングを自社内のＩＴ構成に取り入れるためには、以下の手順で推進する必要がある。

①コンピュータシステムの環境情報の整理。

クラウドシステムを利用するには、利用すべきシステム選定の判断が必要であり、そのためにはシステム環境の洗い出しとマッピングが行われている必要がある。

それらは、

・２０００年問題対策検討時のシステムの洗い出し

・システムのアウトソーシング利用のため、ＳＬＡ設定時のシステム毎の洗出し

・システム更新計画のためのＥＡ的なシステムグランドデザイン設計時

などを検討した際に、既に終了しているはずである。

これらの情報を元に検討を進め、クラウド化できそうな部分の候補を選定する。

その上で、設計図を描いた後にクラウド化の検討を進める。

上記の様なプロセスを経ていない場合、現状の洗い出しを行い、

・基幹システム（会計、生産、物流、営業、社外ＨＰなど）

・研究開発システム（特許、研究、開発など）

・間接業務システム（秘書、人事、資産管理、会議室予約、災害安否確認など）

・オフィスシステム（メール、文書作成、グループウェア、など）

・支援システム（マスター配信、セキュリティ、ｅ－ラーニングなど）

を明確化して、システムと優先順位のランク付けのマッピングを実施しておく必要がある。

②コンピュータシステムの資産情報の整理。

クラウドシステムを利用するにはコスト管理が必要であり、そのためには自社のシステム構成がデータベース等で管理されている必要がある。

通常ＴＣＯ測定を行っている企業であれば、コストの算定は容易に行えるが、行っていなければ、以下の情報を明確にする必要がある。

・ハードウェア構成（サーバーの種類、利用目的、台数、資産価値など）。

・データベース構成（データベースの種類、利用目的、個数、資産価値など）。
・ソフトウェア構成（アプリケーションの種類、利用目的、資産価値など）。
・ネットワーク構成（ルータの種類、台数、資産価値など）。
・外部利用回線（回線の種類、利用経費など）。
・固定資産（コンピュータルーム、ラック室、分電版、テーブルなど）。
・管理費（システム管理人件費、外注費、利用者の人件費など）。
等々・・・。

これらの資産の取得時期、年間固定費、年間経費、更新予定などを算定しマッピングし管理する必要がある。

③コンピュータシステム運用組織とプロセスの整備。

コンピュータを運用するためには組織とプロセス、すなわち「運用統括組織」、「ヘルプデスクサービス」、「ユーザサービス（駐在サービス）」、「保守サービス」、「エスカレーションフロー」などが機能している必要がある。

現在ではＩＴＩＬなどで定義された機能を必要に応じて組織化し、プロセスとして確立すればよく、十分な機能が無い場合は、見直しと改善提案を行う。

④クラウド化した場合の影響の調査。

クラウド化した場合に、どのような影響がもたらされるのかを事前に調査しておく必要がある。

調査の範囲と内容は、
・現状で利用者に提供されているサービスの全体
・自社が利用できそうな外部サービス内容
・クラウド化した場合の利用者の利用形態や、運用管理者の業務形態
・利用に際してのネットワーク環境
・同業他社のクラウド化の動向
・今後新たに発生しそうなサービス

であるが、できれば既にクラウドシステムを取り入れている企業と情報交換し、その長所・短所、導入による業務の変化などを適切に把握・分析しておくことが望ましい。

⑤改善のためのプロセスの存在（予防的、保全的）。

コンピュータシステムの維持向上には、改善のためのプロセスの存在（予防的、保全的）と、それを裏付ける予算的措置が必要である。

これらのＰＤＣＡプロセスと予算については、事前に委員会の審議と経営者の承認を得ておく必要がある。

⑥クラウド化の経営者への説明。

クラウドシステムを導入するには、経営者の決済が必要である。

そのために、事前にクラウドシステムの概要を経営者に説明しておく。

ＣＩＯが設定されている場合には、経営トップへの話しが通しやすくなる。ＣＩＯへの報連相として、
・上司に対するレポートラインが確立
・週報・月報などで頻繁に報告することが可能
・重要ポイントについては直接面談して説明することも可能

などが実現され、スムーズに推進しやすい。

ＣＩＯが設定されていない場合には、情報システム部門が定期的に経営者に報告する機会があれば計画的に説明するが、その様な機会が無い場合、理解を得ることは困難が予想される。

場合によってはクラウド化もコストメリットという点で、経営インパクトありという認識を共有する必要で、単独で応じてもらえない場合は、経理責任者などと協議し共同説明したり、外部の権威を借りて説明する機会を設定したりする必要があ

る。
⑦クラウド化するコンピュータシステムの方針・範囲・利用形態の決定。
クラウドシステムを利用する方針･範囲･利用形態などを決定する必要があるが、これらの決定は経営者の決済が必要である。
経営者を交えた検討委員会で決定するが、検討に当たっては、
・クラウド化の方針
・クラウド化するシステムの範囲、利用形態
・クラウド化することへのメリット・デメリット
・クラウド化した場合の構成と数年間のコストの見通し
・クラウド化の阻害要因や問題が発生した場合の回避策
・クラウド化できない場合の代替案
・クラウドシステム利用の同業他社の動向と利用の実態
などを項目に織り込む。
それとは別に利用者の代表との運営委員会を開催して状況を説明する。
⑧クラウド化の後のモニタリングと評価。
クラウド化した後は、モニタリングと評価を行う。
モニタリングはクラウド提供者が測定したデータ以外に、システム内に組み込んだモニタリング項目で測定したデータも合わせて評価する。
また、定点観測として、導入前と導入後にＴＣＯ測定を行い、コスト的な側面を測っておくことが望ましい。
ＴＣＯ測定には、
１）コンピュータ資源の管理面
・調達に係るコスト。（ＰＣ，ハード、ソフトネットワークなど）
・システム資源管理に係るコスト。（同上）
・ライフサイクル管理に係るコスト。（同上）
②人件費の管理面
・ＥＵＣコスト。（処理マクロの作成、社内ソフト流通、利用時間など）
・システムの導入・更新に係るコスト。（要件定義、受入テストなど）
・トラブル対応に係るコスト。（ヘルプデスク、エスカレーションなど）
を測定項目に含めておくことが望ましい。
モニタリングの評価結果はＫＰＩ・ＫＧＩ、更にはベストプラクティスとの比較においてなされるのが望ましく、結果は委員会を通じて経営者に報告する。
⑨是正的措置と保全的予防措置の実施。
モニタリング評価結果に基づいて是正措置を行うが、予算的な制約もあり、緊急性を要する項目を第一に、重要な項目を第二にするのが望ましい。
是正措置から漏れたものについては、予算を計上し、保全的予防措置として実施されるの望ましい。

４．クラウドコンピューティング導入とビジネスリスク

クラウドコンピューティング導入の際に、検討しなければならないビジネスリスクを以下に例示する。

・経営環境面

ビジネスインパクト	ビジネスリスク	ビジネス課題
固定費から変動費へ	事業者撤退のリスク	事業方針への適合性
主要システムの費用化	事業停止のリスク 法的堅牢性崩壊のリスク	事業方針への適合性
ＩＴ投資の弾力性	想定外の費用発生	事業方針への適合性
システム要員の配置転換	技術喪失リスク	人事統制への適合性
ＩＴのＢＣＰ対策実現	事業者撤退のリスク	リスク委員会の統制
ビジネス拠点整備の容易性	セキュリティリスク	
ＩＴ資産の所有から利用へ	監査への適合性	費用のトレードオフ
ビジネス連携の容易性		事業戦略への適合性
ビジネス規模の自由度設定	統制外の事業発生	ＩＴ統制方法

・情報環境面

ビジネスインパクト	ビジネスリスク	ビジネス課題
基本マスターの整備	不整合の存在のリスク	全社協力体制
企業情報統制の機会	非協力部門のリスク	全社協力体制
情報連携による活用	ノウハウ不足のリスク	「見える化」の統制

・システム環境面

ビジネスインパクト	ビジネスリスク	ビジネス課題
集中管理から分散管理へ	データ不整合性リスク	システム方針整備
開発期間の短縮	ニーズ欠如のリスク	
サービスの組合せ利用	利用度低下のリスク	システム方針整備
フロントエンド処理の存在	コストが減らないリスク	運用見直し
クリティカルシステム保持	費用削減対象外	費用効果トレードオフ
検索エンジンによる検索	機密情報漏洩のリスク	ＡＣＬの設定
シンクライアントの安全性		
クライアント配置工数削減		
コスト管理の継続	コストが減らないリスク	事業方針への適合性
モニタリングによる統制	フィードバック不足	統制方法の見直し

・利用環境面

ビジネスインパクト	ビジネスリスク	ビジネス課題
ユビキタスの実現	労務管理の困難性	労務管理方針適合
使い勝手はＳＬＡ依存	二重投資のリスク	費用効果トレードオフ
オンラインリテラシー教育	普及しないリスク	教育方法の見直し

以上

2011 年度成果物

古川正紀

中堅・中小企業のためのクラウド活用の手引き

はじめに

今年度は、中堅・中小企業でも上場最大手企業と同様の IT 環境を用いて、IT 経営を安くスムーズに高度化しやすいと言われる、クラウドコンピューティングの活用のあり方を、解説致したい。

クラウドとは、結局何か？

テレビの CM やマスコミの記事でも、いまやクラウドという言葉が出回っているものの、実質的に中堅・中小企業の経営者は意外と無頓着だったり、言葉遊びに興じていたりするような感じがある。

業界団体や企業ごとに、クラウドについてのさまざまな定義があるが、例えば IT のビジネスモデルの総称としてクラウドと呼んでいたり、あるいは IT の利用形態の一つとしてクラウドと称していたりする。 因みに、総務省から委託されてクラウドの信頼性・安全性などの情報公開を行う NPO 法人 ASP・SaaS・クラウドコンソーシアムでは、クラウド黎明期に下記のような定義を行っている。

「クラウドコンピューティングとは、ASP や SaaS やユーティリティー・コンピューティングなど、データセンターのハードウェア・ソフトウェアの集合体のこと。」

少し難しい表現でもあるので、筆者なりに要約すると以下のとおりである。

- 自社でサーバーやお金の掛かる IT 機器・IT 資産を持たず、
- ネットの向こう側にある IT 資産やサービスを「賢く安く借りて使って」、
- 拡張性も縮小性(使わなくなればやめればいい)も備えた IT のこと

少しイメージが明確になったことと思われる。

クラウドは、ものによっては、初期費用 0 円で使った分だけ、使用する人(ID)の分だけ、お金を支払い、バージョンアップ(Office2007 から 2010 へのバージョンアップやサーバーの更新など)の維持管理も、ユーザー企業ではなくサービス提供社側が対応してくれるものもある。

「場所に縛られない IT 環境」で危機に強く、運用コストも安価なクラウド

「高度な IT は、お金も、高度な IT 要員も豊富な大企業だけのもの」というイメージが一般的であったが、クラウドは「大企業が使うのと同様の IT 環境・IT サービスを、使う人の分だけ、使う分量だけお金を支払い、面倒なメンテナンスなどは全てクラウド提供社側で代行してくれる」というものである。 つまり大企業と同様の IT 環境を「賢く安く借りて使える」仕組みだといえる。 中堅・中小企業のクラウド先行組は、十分にそのウマミを知って、クラウドのメリットを享受しているはずである。

クラウドが危機管理にも強いことを東日本大震災前から見聞されているが、クラウドは「場所に縛られない IT 環境」であり、災害にも経営効率化にも強い側面があるといえる。

これまでの IT は社内に全て買って備えて使っていたため、職場に行かなければ IT を用いた作業ができなかったのが実態であった。

しかし、クラウドを活用していくならば、営業先から営業日報を作成したり、会社のメールアドレスでスマートフォンからメールを打てたり出来る。 つまり、男女共に家庭からでも、ワークライフバランス(仕事と家庭の両立)対策として、子育てや介護などをしながら、IT を用いた仕事ができるようになるわけである。

また、おサイフにもやさしいクラウドであることは、ちょっと見積もりなんかを取ってみるとすぐに分かる。

例えば、ログ管理(ログの取得だけでなく、不正な IT 操作がなかったか、あれば是正できるようにするログの監視なども含む)システムを導入しようする場合の、従来とおりのシステムとクラウドを比較すると、以下のようになる。

■「ログ管理システム」導入検討時の見積もり例

ⓐ従来どおりのシステム	サーバー代＋ログ収集ツール代＋ログ管理ツール代 ＝初期費用 1,200 万円～ ＋メンテナンス費用
ⓑクラウドを用いたシステム	上記一式そろえて、初期費用約 75 万円 ＋サービス利用料
ⓐとⓑの初期費用の差額	1,200 万円－約 75 万円＝約 1,125 万円 ※クラウドのランニング費用は比較対象外。

結局、この例では大幅に初期費用を削減しつつ、IT 戦略の一環として、不正対策ツールで初期費用が浮いた分、営業管理や顧客管理システムを同じく安く使いやすいクラウドで導入して、攻めと守りを今までの IT システム一つ分で充実させるという方法も選択できるのである。

セキュリティー面からの安全性

また、危機管理上は、これまでは情報漏洩リスクにおびえ過ぎて、以下の見方があった。

「クラウドって、システムやデータがインターネットの向こう側にあるので、セキュリティー上危ない。 だから、当社は賢く安全策に徹するから、クラウドは使わない！」

しかし、東日本大震災にて IT 環境が全滅するリスクを肌で感じられた多くの企業は、本社や事業拠点そのものが地震で倒壊したり、津波で町ごと流されたりするという苦い経験から、既に「オンプレミス安全神話」が崩壊した(つまり、自社内に IT 資産を全て囲い込む方が安全だという考えが覆された)ということを理解されている。

結局、IT リスクを考える際も、リスク管理の基本的な考え方として、どっちのリスクが重いか、という観点が肝要である。

既に大手企業がハッカー対策や情報漏洩対策として、クラウド化を加速させ、クラウド提供社の高度な IT セキュリティー要員が管理する IT 環境を築こうと躍起になっている。 つまり、クラウドは、もはや、情報漏洩や不正アクセスのリスクを理由に敬遠されるべきものではない。

安全を求めるなら、災害で自社ビルや工場自体が全壊した場合のリスクを避ける意味でも、大切なデータはネットの向こう側のクラウド内に置いておく。このようなリスク管理対策としてもクラウドが注目されている。

しかしながらただ単に、安さだけを求めてクラウド化を急ぐとリスクもある。 自治体クラウドで問題のあった例は、セキュリティー対策を怠った契約でクラウドを活用したものであった。 安心して任せられる、実績も能力もあるクラウド提供社を選ぶべきである。（ここにITコーディネータの活躍の場がある。）

3タイプあるクラウドの整理

ちなみに、一言でクラウドと言っても、現在クラウドと呼ばれてサービス展開されているものには、大まかに3つのタイプがありる。 下表にその3つのタイプをまとめた。

中堅・中小企業で、自前のシステムをゼロから構築しないようであれば、クラウドと言った場合にほとんどが SaaS を意味していると言ってよいであろう。 専門知識は不要で、どの企業も手軽にさっと導入できるのがこのタイプである。

●SaaS/PaaS/IaaS の定義

SaaS **（Software as a Service）**	アプリケーション（ソフトウエア）をサービスとして提供する
PaaS **（Platform as a Service）**	アプリケーションを稼働させるための基盤（プラットフォーム）をサービスとして提供する
IaaS **（Infrastructure as a Service）**	サーバー、CPU、ストレージなどのインフラをサービスとして提供する

出典：総務省・スマートクラウド研究会報告書

大まかに言えば、表の SaaS が、各企業で IT の専門知識がなくても明日からすぐに導入できるお手軽なクラウドで、PaaS より下の部分が、IT 部門などを持ち、自前のシステム構築や IT 環境づくり(HaaS による IT 資産を借りた IT 環境の増強など)をするという、ちょっと高度なクラウド活用部分と言える。

ここまでクラウドのメリットを中心に触れてきたので、後段では、本当にクラウドはメリットばかりなのかどうか、世の中のクラウド化の流れとどう向き合えば良いかを見つめ、クラウドにするかどうかなどの選択肢を示したいと思う。

クラウド選択の落とし穴

クラウドのブームに翻弄されるだけだと、かえって高くつくこともある。 クラウドだから万全だとか、クラウドなら必ずどんな企業のどんなケースでも安くつくというわけではないことに留意すべきである。

実際にあったケースだが、「使った分だけ」「ID 分だけ」課金される、ということが、かえって従量制のワナにはまってしまった例があった。 その企業は多くのユーザーを抱えており、従来の IT を買い切って IT 資産を自社内に備えて使うオンプレミス対応の方が、従量制のクラウドより安かったわけである。

また、いったんクラウド化してみたのはいいものの、従来のITからクラウド化する際のデータ連携の問題やオンプレミスに戻せない設計・仕様・形式にされてしまったことで、ベンダー・ロックインされた(実質的に、あるクラウド提供社のサービスを使い続けざるを得なくなった)ケースもあった。

さらに、クラウドならではといえそうなのは、インターネットの向こう側に全ての IT 資産があって、ネットを介してクラウドを活用する上で、ネットワークが切れたらどうしようもないという問題もあり得る。 クラウドには欠かせないインターネット・各種ネットワークは、安定的に提供可能な通信会社の VPN(バーチャル・プライベート・ネットワーク)などの、クラウドを安心して使いやすい支援を受けるのが良いいのではないだろうか。

もちろん、中堅・中小企業でのクラウド採用で、上場最大手企業と同様の堅牢で便利で高度な IT 環境を、ID 分だけで賢く安く借りて使えたという例の方が、圧倒的に多いのは言うまでもない。

しかしまだ落とし穴はある。 やはり失敗例として、「クラウド」というサービスメニューを掲げている企業が、実は、小さな古い雑居ビルの一室で、4 台のサーバーを備えてクラウドサービスを提供しているだけの企業だったということもあった。

また、災害対応やバックアップ対応・セキュリティー対応も甘い小規模な「雲散霧消」してしまうクラウドだったという例もあったし、突然、クラウドのサービスを停止してしまった零細のクラウド提供社も実際に存在する。

クラウド活用においては、クラウドだから何でも良いのではなく、クラウド提供社の企業規模や経営の財務的な安定性・継続性や災害対応力なども賢く見極めておく必要があるわけである。

また、アメリカ企業がクラウド・ブームの火を付けたとはいえ、クラウド提供社が外資系だと、場合によっては日本の商習慣や日本企業の IT の使い勝手とうまく合わないケースもあり、国内のクラウドの方がしっくりくるという声もあったりする。

さらに、「The Dark Side of Cloud～クラウドの暗黒面～」という課題もある。クラウド自体は中立なものだが、クラウドを悪用する人や組織が出てきているという実態も、念のため知っておくべきであろう。

中には、個人のお小遣い程度の金額でも簡単に巨大な IT 資産を借りて使えることを良いことに、クラウド上にこれまでには成し得なかった大規模なサイバー攻撃の拠点を築く人々が出てきた例もある。 また、クラウド上からサイバー攻撃の依頼を受けて企業や公的機関に攻撃をかける「FaaS: Fraud（詐欺） as a Service」という暗黒面の「仕事人」まで登場して来ている。

クラウドの損益分岐点

クラウドを賢く安く手軽に活用して、堅牢な IT 環境や IT 経営を通じた成長力を高めるためには、てここまで述べてきた課題もしっかりと見据えておいて頂かなくてはならない。

その上で、結局当社にとって、クラウドの方が得なのか、それとも、IT 資産を買い切って使った方が得なのかを考えていこう、というのが、「クラウド損益分岐点という考え方である。

クラウドといっても従量制なのか定額制なのか、また、オンプレミスとクラウドで同じことをこなす場合に、管理会計の観点から「隠れたコスト(Hidden Costs)」を含めて、どっちがお得でより良いのかを比較しなければならない。

IT 資産を買い切って IT 環境を整える場合、雑多なメンテナンスに対応する IT 要員の人件費は、実質的に固定費として費用が掛かる。 多くの企業で、この IT のメンテナンスに掛かる人件費を検討せずにいることで、クラウド化の損得勘定を見誤っているケースが見受けられる。

損益分岐点の考え方を用いて、十分に比較検討することが肝要である。

（ここにITコーディネータの活躍の場がある。）

クラウドを活用していれば、クラウド提供社側の IT 専門家としての経験豊富な有資格者が、メンテナンスやセキュリティー対応やライセンス・バージョンアップなどを含めて対応してくれるわけである。

自社システムとクラウドにおけるバックアップの比較

また、自社の財務・人事・顧客情報などに加え、お客様からお預かりするようなデータなどが、災害や IT 事故などで消滅してしまっては、決算すらできないケースもあれば、お客様から法的問題として訴えられるケースもある。

そこで、データのバックアップが必要になってくる。 オンプレミス対応として、自社内に IT 資産を買い切って持つ場合のバックアップ対応と、クラウドを活用した場合でのバックアップ対応を比較する必要がある。

オンプレミス対応では、自社で IT 資産を買い切って備えて使うパターンであるので、この場合、バックアップはあるデータを物理的に離れた 2 拠点以上に分散して保存しなければならない。

すると、中堅・中小企業にとって、事業拠点が 1 カ所の場合は、自社の職場や工場などとは別の場所に新たに IT バックアップ用の拠点を賃貸あるいは施設を買って備えなければならないことになってしまう。 地代も掛かる上に、データをバックアップしておく IT 機器やそれを操作・メンテナンスする IT 要員も二重・三重に必要になり、無駄が多くなりがちといえる。

さらに、バックアップしたデータを、元の IT 機器で使って事業を継続できるようにするための「リストア」作業に手間暇がかかってしまいがちである。（ある企業では、IT 事故発生の際に、磁気テープからバックアップデータを元の使える状況にするまで、丸々4 日間かかった例もあった）

一方で、クラウドを活用していれば、クラウド提供社側で複数拠点に定期的にデータをバックアップしてくれるオプションサービスなどが利用できる。 また、そのようなクラウドの場合は、どこかの拠点のデータが破壊されても、別の拠点で生きているデータを使って、そのまま今までどおりの IT 作業を続けやすいため、バックアップやリストアにかかる手間暇もコストも低くなりやすいといえる。

既存の IT 運用における隠れたコスト

また、各企業の現場では、「従来どおりの IT 環境が最も良い・安全だし健全だ」と言いながら、意外と問題ある IT 運用を続けていることがよくある。

ある地方自治体では、クラウドにしておけば問題が起こらなかったのに、オンプレミス対応にこだわり、その結果、従来どおりの IT 資産が高いからと、違法コピーしたソフトを使い続けて問題になったケースもあった。

こんな IT 運用がなされるままで、無駄なのにやたら高い IT コストを垂れ流し続けていないだろうか？

例えば、サーバーを置いておくために確保している自社オフィス内のスペースが、管理会計上も IT コストとして配分すべき「地代分」の費用が掛かり続けることを忘れていないだろうか。

管理会計に「在庫金利」という言葉があるが、それに似たような状況が、サーバールームを自社内にど～んと構えることによって起こっているということを、意識していない企業が多いものと思われる。

また IT に関わるさまざまなコストや訴訟となった場合に賠償金として支払わなければならないようなリスク要因も、実は、IT 運用における隠れたコストと言える。

何をクラウド化したらいいか？　何を今までどおりにした方が良いか？

クラウドの良い面も課題も見つめてきた中で、「クラウド化にどう対応したらいいか！」が却って解りにくくなったかもしれません。

ではどうすればいいんだ…、ということになるが、以下に纏めたい。

先ずは優先順位付けであるが、一番解りやすいのは「クラウド化しやすい業務から並べてみる」である。

クラウド化しやすい支援業務系の IT 資産から始め、次第にクラウド化しにくくなる業界特殊業務系の IT 資産という順に書き上げてゆく。 次に「リスク指数」と「重要度指数」を付加し、それを掛け合わせて、得点の高い順に並べ替えてみる。

漠然とクラウド化にどう向き合うかを悩む暇があったら、いったん自社の IT 資産棚卸しをしてみて、クラウド化においてリスクの重要度も低めでクラウド化しやすい IT 資産からクラウド化していけば良い、という「システマチックに悩む」ようにしてはいかがであろうか。

全てをクラウド化する必要はないし、クラウドの発展途上ではまだまだ業界特殊業務系の IT 資産がクラウド対応され尽くしていないこともある。 そのような場合は、これまでどおりのオンプレミス対応で良い、といった判断を下せば良いのである。

最終的に、棚卸しをしてみた自社の IT 資産のクラウド化におけるリスク判定についてまとめておけば、説明責任を果たしやすく、自社内での検討・提案・稟議などに活用しやすいであろう。

結論として

クラウドについて中堅・中小企業がどう向き合い、何に気を付け、どう判断すべきかをまとめさせていただいた。 最初に防災・危機管理対策について、また、次にバックアップや災害対応について少し述べておいた。 最後には、何をクラウドに乗せるべきかの判断手法を述べている。

不況で大変な世の中であるからこそ、リストラすべきは無駄な IT 投資や IT 資産である。 多様性あふれる成長戦略を実践していく上でも、クラウドの活用を真剣に考えるべきである。

以上

Google Appsを使用した
安否確認システムの構築について

ITコーディネータ(認定番号0012552001C)
滝沢　康

2010/07/05

1

背景

- 「事業継続計画;
  BCP (Business Continuity Plan)」
  への取り組みを実施
- 災害発生時の事業継続にためには初動体制を
  早期に整えることが重要
- その対策として安否確認の迅速化が求められる

2

目的

- 災害発生時でも利用可能なシステムとすること
- 災害発生時に社員の安否確認を迅速に把握することを可能とすること
- 安否確認を迅速に行い、事業再開への初動体制構築を支援すること

3

機能要件

- ユーザ登録機能
  - 事前に安否確認対象者を登録しておく機能
- 一斉送信機能
  - 安否確認対象者へ一斉に連絡を行う機能
- 安否報告機能
  - 対象者が自身の安否を報告する機能、または代行者が登録を行う機能
- 安否確認集計機能
  - 安否報告の結果を集計、参照を行う機能

4

システム構成

- 災害時でもシステムが稼動している必要がある

- クラウドサービスであるGoogle Apps上に構築を行う
  - サーバは世界中に分散しているため、日本が災害にあっても、システムがダウンすることはなく、インターネットに接続さえできれば使用可能であると考えられる
  - Googleのインフラを使用するため、サーバやネットワーク環境を用意する必要はない
  - Google Appsの標準機能で構築可能であるため、構築コストを抑えることが可能

5

システムの利用形態

6

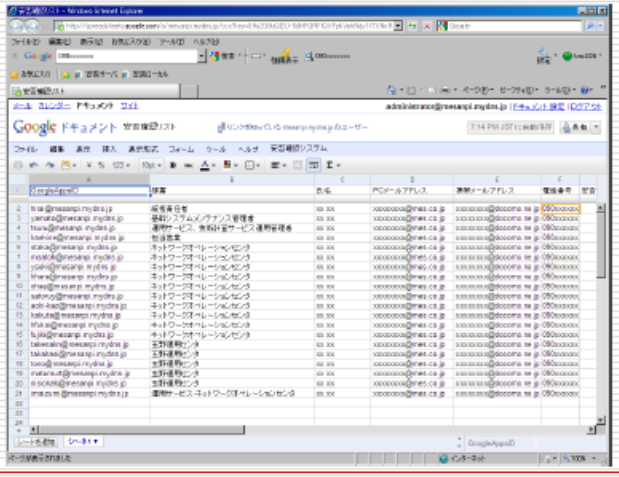
システムの利用方法

- 安否確認メールの一斉送信
  - メール送信処理を手動で実行する
- 安否報告
  - メールを受け取ったら、PCまたは携帯より、Google Apps上のサイトへ自身の情報を登録する。
  - 登録結果はGoogle Appsのスプレッドシートへ反映される
- 安否確認
  - 手動で集計処理を実施する
  - サイト内で集計結果の参照を行う

7

システム利用イメージ1

- 安否確認対象者のメンテナンス



Googleドキュメントのスプレッドシート機能を利用

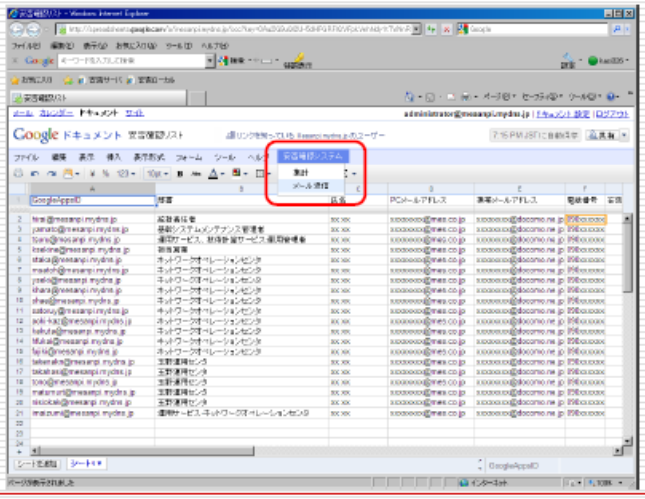
ブラウザ上でExcelのように編集が可能

※Googleドキュメント：
ブラウザ内で動作するオフィスソフト
データはGoogleのサーバ上に保管される

8

システム利用イメージ2

□ メールの一斉送信



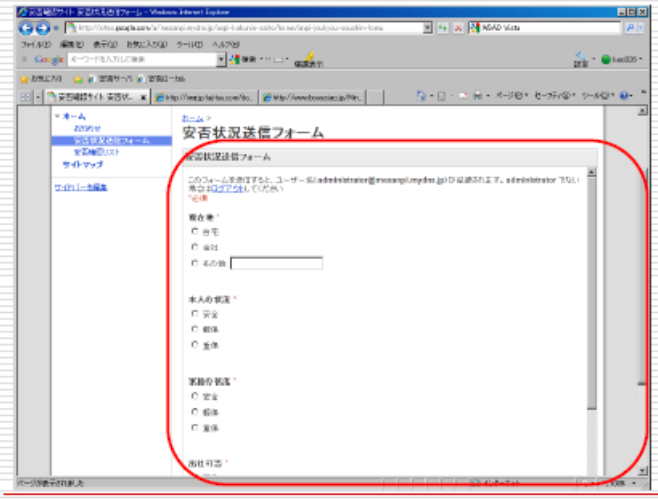
スプレッドシートのスクリプト機能を利用してメールの送信が可能

※Excelのマクロのよう機能

9

システム利用イメージ3

□ 安否情報の登録



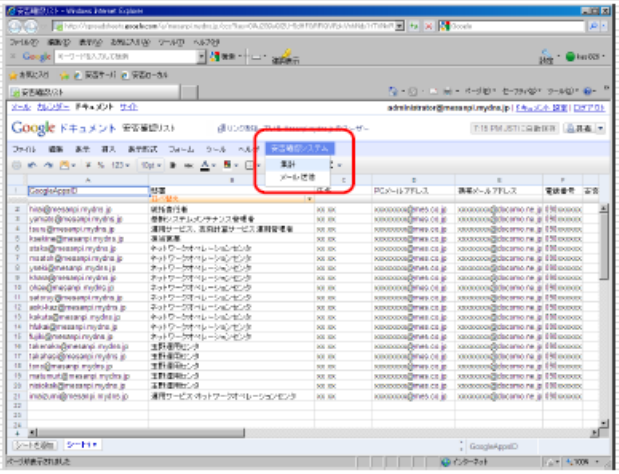
登録フォームはGoogleドキュメントの自動生成を行う機能により作成

登録したデータはスプレッドシートの保管される仕組み

10

システム利用イメージ4

□ 安否情報の集計・参照



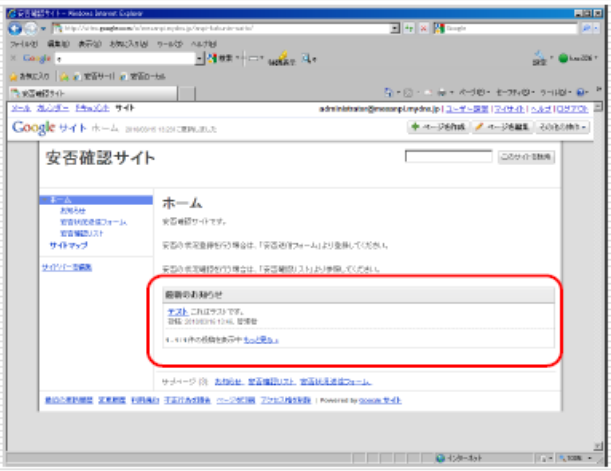
登録フォームから入力されたデータを手動で集計する

メール送信と同様にスクリプト機能を使用し、個人ごとの最新の入力内容をスプレッドシートに反映する

11

システム利用イメージ5

□ お知らせ掲示板機能



掲示板機能はGoogleサイトの標準機能で作成可能

12

今後の課題

- システム要件の見直し
  - 部門を限定し、試験運用を実施
  - 実施結果から課題を抽出、システム要件の再検討を行う
- システムの見直し
  - 見直したシステム要件を元に、システム仕様を見直す
  - Google Appsの機能のみでは難しい要件(データのチェック・部署や勤務地などによる安否確認対象者の絞込み・権限制御・帳票出力)も想定されるため、Google App Engine上での構築も検討する

13

(参考)Google Appsとは

- Gmail、Googleドキュメント、Googleサイト等のアプリケーションをWebベースで提供するクラウド型のサービス。
- 独自ドメインによる運用も可能
- Standard Editionは無償で利用可能(50ユーザまで)
- Premier Editionは年間6,000円/1ユーザ

14

(参考)Google App Engineとは

- WebアプリケーションをGoogleのインフラ上で実行することができるクラウドサービス
- 使用CPU時間、転送データ量などにより従量課金が行われる。ある程度までの使用量であれば課金されない
- 課金を行うことにより、どこまでもスケールアウトしていくことが可能

15

終わり

16

中小“輝”業のクラウド活用は従来型IT思考の脱皮から

ITCイースト東京主催セミナー「龍馬とクラウド」より抜粋

2011年6月30日

日本ユニシス株式会社
坂本　徳明

注意：本資料は執筆者個人の見解です。

中小企業のおかれた経営環境

- 戦後多くの創業者が使命感･志に燃えて起業し、会社を発展させてきたが、ある程度ビジネスが軌道に乗る一方で、各業界における技術･流通システムなどのライフサイクルが峠を越え、陳腐化が始まり、日本の経済構造全体が変革期に入っている。
- 低付加価値品の量的拡大モデルではもう限界に来ており、大企業製造業を頂点とする従来型の「下請けピラミッド構造」は否応なく変化を迫られている。

画一的な下請け中小企業から多様性の中で自立する中小輝業へ

- 中小企業の特徴は、その多様性にある。少子高齢化・人口減少など社会の成熟化が進む中、趨勢として、量的な意味での「物質的豊かさ」から、「質的な豊かさ」を求める傾向が強まっている。
  その意味で、人生観、生活スタイル、精神的豊かさ、自然環境との共存などを含めた「変化する国民の価値観」を受け止める主体となり得るのは中小企業である。

- 今までのように、規格化・効率化・コストダウン、大量生産・大量流通という土俵で勝負し続けるのではなく、多様性のなかに付加価値の源泉を見つけ、新たなビジネスモデルで勝負する。そのようなことができる環境が整いつつある。
  そのひとつがクラウドである。

本資料は執筆者個人の見解です。

3

中小輝業にとってこそ、クラウドはその真価を発揮する

- 従来のITは、大量生産・大量流通、効率化、コモディティといった、戦後の経済成長モデルの中で進化してきた。

- 戦後の経済成長モデルとは異なるビジネスモデルに活路を見出そうとする中小輝業にとって、従来型の画一的かつ効率中心のITでは、新たな価値を創出することはできないのではないか。

- クラウドの背景は戦後の経済成長モデルとは異なる。その意味から、中小輝企業とクラウドの親和性は高いのではないか。

- しかし、中小輝業がクラウドを活かすためには、乗り越えなければならない課題がある。

本資料は執筆者個人の見解です。

4

クラウドは従来型ITのアンチテーゼ

- 今までのIT当たり前。実は・・・
  - 使わないものにまでお金を支払わされている
    - 未使用ソフトの割合が高い
    - IT資源は余剰
  - ITの進化をリスクとして受け入れない人材
    - おごり　慢心　成功体験　外を見ない
    - 網羅的であるが平均的　とがった強みがない
    - 保守的で受身の姿勢
    - 過度な完ぺき主義　変化への警戒心
- ITの進歩によって初めて可能となる新しい仕組みを是とし、人間がそれに適応していくという発想。
  この発想があって初めてクラウドがその真価を発揮する。

本資料は執筆者個人の見解です。

クラウドの活用は発想の転換から

- 少なくとも中小輝業のクラウド活用においては、従来型のIT発想でクラウドについてあれこれ議論するのはナンセンス！
  - 是として受入れ、それに適応するスタンス
- 必要なのはクラウドのもつ機能の改善・拡充ではなく、IT関係者が従来型の思考方法から脱皮（メタモルフォーゼ）することなのでは
  - 視座を変える勇気

本資料は執筆者個人の見解です。

あなたはITCとして中小輝業のクラウド活用を支援できますか？

- 自ら未来をつくることにはリスクが伴う。しかしながら、自ら未来をつくろうとしない方がリスクは大きい。
  - “ゆで蛙状態”からの脱皮
- リスクテイクしようとする中小輝業経営者の相談相手であるITCも、同じようにリスクテイクしなければならないのでは。
  - “従来型”からの脱皮
- 中小輝業の経営戦略やIT戦略の立案において、現在の思考スタイルで大丈夫ですか。
  - 脱皮は自己否定から始まる

本資料は執筆者個人の見解です。

7