

クラウドコンピューティング に関する考察



2010年4月13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”を超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。

2010年4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)】

久住 昭之	(0035712003C)
瀬戸 昭彦	(0065252006C)
滝沢 康	(0012552001C)
千枝 和行	(0029302004C)
古川 正紀	(0005462001C)
牧田 一雄	(0052712005C)
山上 幸一	(0049182005C)
山崎 直和	(0035252003C)

(注)本記載内容は、ITコーディネータ個人としての見解を述べたものであって、個人が所属する企業・団体としての見解を述べたもので無いことをお断りします。

また、本書において使用しているシステム名や製品名などで各メーカー等の登録商標を使用している部分があるが、文中においては TM、コピーライト表記はしていません。

目次

1. クラウドコンピューティングで提供されるサービスを利用する上での考慮点	久住 昭之	4
2. クラウドコンピューティングによるワークスタイル変革について	瀬戸 昭彦	8
3. クラウドコンピューティング利用のメリットと課題の研究	千枝 和行	13
4. ITC視点でのクラウドコンピューティング考察	古川 正紀	23
5. 「クラウドコンピューティング」へのアプローチ	牧田 一雄	36
6. 現実的なクラウド適用の考え方	山上 幸一	57
7. クラウド時代に求められるネットワークについて	山崎 直和	60
8. Google Apps を使用した安否確認システムの試行について	滝沢 康	65

クラウドコンピューティングで提供されるサービスを利用する上での考慮点 ～ ITC がクラウドサービス利用にあたって考慮すべき事項 ～

久住 昭之

1. はじめに

これまで、情報システム利用者が開発・構築・運用・保守してきた情報システムについて、クラウドサービス(以下、クラウドサービスとはパブリックなクラウドサービスを指すものとし、その他の場合には別に表記する)の利用を検討する企業が数多く出てきている。

しかしながら、クラウドサービスを利用するにあたっては、その特性を十分理解した上で利用していかないと、「こんなはずではなかった」というような状況に陥る危険性がある。

本資料では、クラウドサービスを提供する事業者側の立場に立って、クラウドサービスを利用するにあたって、自社保有の形態とクラウドサービスを利用する形態における、情報システム利用者側が理解しておくべき違いを中心として考察する。

なお、以下では基本的にシステムの運用開始後に問題が発生しないように、利用を開始する前に理解、あるいは了解しておくべき点を中心に考察している。(開発基盤としてのクラウドサービス利用は対象としていない)

2. 考察にあたっての前提

クラウドサービスを利用するということは、これまで情報システム利用者が自らの手に握っていた情報システムに対するコントロール権／主導権をクラウドサービス提供事業者に渡すということであり、そのトレードオフが提供スピード、あるいは利用コストの低減につながっているものと考えられる。

クラウドサービスはサービス提供事業者にとっては仮想化技術などを活用してのリソースシェアを基本としたサービスと考えることができるが、そのリソースマネジメント権(キャパシティ管理、増減設等)はサービス提供事業者の手中にある。つまり、情報システム利用者がこれまで自社保有の形態では自由に決めることが出来てきていたことが、クラウドサービス提供事業者のルールに自らの情報システムを従わせなければならないということである。

上記のことを前提とした場合における、クラウドサービス利用上の考慮点について以下に考察する。

3. クラウドサービス利用上の考慮点

以下では、クラウドサービスを利用した情報システムを安定的・快適に利用する上でキーとなる、品質面での特性毎に考慮すべきポイントを考察する。

3-1 可用性

情報システムを自社保有の設備等で構成する場合に比べ、クラウドサービスの可用性は、サービス提供事業者がクラウドサービスのためのネットワークや機器、電源等インフラ部分の冗長化構成をどのように設計するのか、故障発生時の回復目標時間をどの程度に設定するのか、などに依存することになる。つまり、可用性を高めるための対応はサービス提供事業者のポリシーに依存することになり、可用性レベルがクラウドサービスを利用する場合にどの程度になるのか、それがクラウドサービス利用者の求める水準を満たすのかどうか、をはっきりと評価しておかなければならない。

また、クラウドサービス提供事業者のサービス提供用設備の設置環境(立地条件や建物の耐震特性など)や災害対策等についても評価できることが望ましい。

3-2 信頼性・安全性

クラウドサービスでは、実際のデータ格納・保管場所がどこにあるのかがはっきりと分からない場合があり、国外であることもありうる。その場合には、DB 内のデータにはそれが存在する国内法が適用されることになるため、万が一の場合におけるカントリーリスクを考慮して DB のバックアップ等を手の届くところにおくことが必要となる。

また、データ消失時におけるリカバリについてどのようになっているのかなど、データの安全性の面での評価をしっかりと行っておくべきであり、リスクがある場合には、利用者が自らデータのバックアップ等を行っておくことが必要である。

セキュリティの観点からは、クラウドサービス利用時においては、サービス提供事業者のセキュリティポリシーに従ったセキュリティ管理がなされることになる。そのため、サービス提供事業者による情報の取扱方法等を十分把握評価しないと、サービス提供事業者からの情報漏えいや改ざん、目的外使用といったことが十分チェックできないだけでなく、サービス利用終了時におけるデータの回収や適切な消去等がされず残されたままとなる可能性もある。

3-3 機能性

クラウドサービスとして提供されるサービス機能はあくまでサービス提供事業者の仕様に基づくものであることから、個別の利用者ごとにカスタマイズして利用することは想定されていない。従って、クラウドサービスを利用して情報システムを実現していく場合においては、必要な機能が備わっているかどうかを十分確認し、場合によっては制約を受けることも許容することが必要である。

3-4 運用性・保守性

クラウドサービス提供事業者にとっては、個々の利用者の要求に応じてクラウド基盤の運用を行うことはできず、クラウドサービス全体を提供者として安定的に運用していくことが使命となる。従って、メンテナンスウインドウの設定などは利用者の業務特性を考慮したものではなく、事業者側の都合で設定されることになる。

このようなことから、クラウドサービスを利用した情報システムにおいては、そのシステム運用がクラウドサービスの運用条件に依存する部分が発生することを理解しておくことが必要である。

3-5 性能

クラウドサービスにおいては、複数の独立した利用者がクラウドサービス提供事業者の用意するリソースを共用することになる。この場合に懸念されることとして、他の利用者のアプリケーションの振る舞いによりリソース競合等の事象が発生し、自分の利用しているサービスの性能に影響がでることが考えられ、場合によっては、他の利用者のアプリケーションの影響によりサービス提供が停止したりすることも考えられないことではない。

また、DB 構造が提供者側で決定されることから、その内容を十分に理解した上でのアプリケーション処理としないと十分な性能が得られないといったことになる。情報システムを実装する上で DB の構造がわからないためにチューニング等がしにくく、その結果として望むだけの性能が発揮できないといったことが発生しうる。

更に、クラウドサービス提供事業者自身が十分なシステムリソースを用意しないことによる JOB 処理時間の遅延やスケジュールの変更などが発生することが考えられる。

3-6 継続性

自社保有の設備であれば、仮に機器やソフトウェア提供ベンダが倒産したり買収されたりしてもシステム利用者が所有するものを失うことはないが、クラウドサービスを利用する場合には、クラウドサービス提供事業者の倒産や買収により、あるいは災害の罹災によるサービス提供の停止といったことが可能性として考えられる。これらに対する防衛策は、サービスの利用者にとっては主体的に対応することは難しいと思われる。

4. 終わりに

本資料では、クラウドサービスを利用する上で運用上影響がでる可能性のあるポイントについて

簡単に考察した。

上述したとおり、クラウドサービスを活用して情報システムを実現していく場合においては、クラウドサービスのサービス仕様・提供条件・限界を十分理解した上で利用していかないと、思うようなことが実現できない。

例えば、クラウドサービスを利用し、十分に価値のあるアプリケーションとしては、個別のカスタマイズ等があまり必要とならないと思われるもの、例えば電子メールや、パッケージ型のグループウェアなどが考えられる。

一方で、やや自社保有形態に近くなるが、ミッションクリティカルなアプリケーションをある程度自分がコントロールできる要件を備えたプライベートクラウドで実現するという事は考えられないことはないが、ミッションクリティカルなアプリケーションについては、クラウドサービスを利用するよりは、従来どおり自らシステムリソースを準備し、自分がすべてコントロールできる範囲でのサービス実装をすることが情報システムの安定運用を確保する上ではより確実であると思われる。

いずれにせよ、自分の実現したい情報システムの要件や特性を十分勘案した上で、利用しようとしているクラウドサービスの仕様、特長等をきちんと把握し、コストとのトレードオフにおいてある程度の割り切りをしてその利用可否を選択することが重要であり、クラウドサービスの欠点・弱点をよく知った上で活用を考えるべきである。クラウドサービスをどのようなケースで利用し、どのようなケースでは利用しないかという、自分なりの基準を設け、それに沿ってのアプリケーション実装を進めていくことが必要であるとする。

以上

クラウドコンピューティングによるワークスタイル変革について

2010/02/09 瀬戸 昭彦

【テーマ】

クラウドコンピューティングや SaaS 等サービス提供型の情報システムが普及することで、ワークスタイルがどのように変わっていくのか検討する。

<< 概 要 >>

1. 情報システムの在り方

従来の情報システム(構築から運用まですべて自社で)

ブロードバンドの普及によるインターネットを前提とした情報活用

2. 働き方のニーズ

少子高齢化、団塊世代のリタイアによる労働人口減少、育児・介護を抱える人たちの働き方など、社会・企業・個人のニーズについて

3. IT を活用した働き方と期待する効果

モバイルワークなど、IT 活用による「時間」と「場所」を越えた働き方とその効果について、社会・企業・個人の観点からまとめる

4. 実現に向けた課題

情報セキュリティやルール作り労務管理、教育研修など実現にあたり、解決すべき課題

5. まとめ

1. 情報システムの在り方

従来は、大型コンピュータ、クライアント・サーバシステムによる情報システムを自社内で構築し・運用してきた。自社で情報システムを維持・運用することによるコストの問題や、情報システム部門が日常のシステム運用に忙殺されて IT 戦略の立案まで回らないなどの課題がある。(乱立する業務システム、過度の設備、運用工数・費用の増大)

情報通信技術の発達と通信インフラの整備により、インターネット活用がより高速に、安価になってきている。

情報システムのあり方として、

業務に必要なITリソースが迅速かつ低コストに配備でき、運用工数も減る

処理量が急増しても迅速に対応できる(スケーラブル)

一時的な要求に備えて大量のリソースを保持し続ける必要がない

以上のような点を解決していく必要がある。

2. 働き方のニーズ

IT 技術の進展は、世界中がネットワーク化され「誰でも」「いつでも」「どこでも」ブロードバンドの環境が使えるようになってきている。一方で、ビジネスがグローバルな環境での競争に対応すべくビジネス再構築も必要となってきた。

また、少子高齢化による労働人口減少に対する優秀な人材確保の面からも、従来のように「会社へ行く」「会社へ帰る」ことを前提とした仕事の仕方では、立ち行かなくなる可能性がある。

3. IT を活用した働き方と期待する効果

通信環境の整備やクラウドコンピューティングなどのサービスが充実することで、時間や場所にとらわれない働き方が現実的となってきた。

例えば、育児や介護のため離職せざるを得なかった、地方在住で都市部への通勤が難しい人々なども就業できる作業環境が提供される。また企業の従業員にとっても、在宅勤務や顧客先への直行直帰などオフィスを基点とした活動ではなく、モバイルワークによる通勤時間短縮による効率的な活動が実現できる。企業にとっても「固定的」「均一的」働き方から「柔軟性」「多様性」を許容する働き方を導入することで「CSR」の観点からも重要となってきた。

【社会にとっての効果】

- ・都市問題の緩和
- ・雇用、新規産業の創出
- ・環境負荷の軽減
- ・社会構造の変革
- ・地域活性化

【企業が期待する効果】

- ・組織変革、意識改革とスピード化
- ・優秀な人材確保と新しいナレッジの獲得
- ・オフィスコストの削減
- ・パンデミックや災害の際の対策

【就業者が期待する効果】

- ・通勤の肉体的精神的負担の軽減
- ・仕事の生産性、効率性の向上
- ・家庭内コミュニケーション向上
- ・趣味や自己啓発の時間確保

などが期待されている(テレワーク白書 2008 より)

4. 実現に向けた課題

4.1 社内でのルール作り

労働時間や業績評価等の扱いについて、みなし労働時間制の適用や、通常の勤務者との異なる賃金制度等を定める場合には就業規則を作成・変更し届け出るなど対応が必要となる。具体的には以下の項目について検討が必要である。

①労働時間

モバイルでの勤務が、就業規則に規定されていない勤務体系(例えばフレックスタイム制)を適用する場合や在宅勤務時のみなし労働時間制を適用する場合において、就業規則に事業場外みなし労働時間制の規定がないときは、その規定を追加する必要がある。

②給与・手当

人事評価制度を新設あるいは改定したり、通勤手当を変更する場合や在宅勤務手当を新設する時、又は、業務内容の変更による給与の変更を行う場合には就業規則(賃金規程)に追加する必要がある。

③安全衛生

在宅勤務の場合には、自宅の作業環境が安全衛生法上適した作業環境である事を義務づけるため、一定の基準等を定める場合には、就業規則にその内容を追加する必要がある。常時型在宅勤務の場合は健康管理について自己に委ねることが多くなることから、導入時や定期的に一般の健康診断とは別に健康診断を実施したり、産業医による健康相談を義務づけたりする場合には、就業規則にその内容を追加する必要がある。

VDT 作業にかかるガイドラインに示されているように「連続作業」等や腰痛防止の健康体操などを示す場合で新たに「VDT 作業管理規程」等を作成する場合には、就業規則にその内容を追加する必要がある。

④セキュリティ

料の持ち帰りルールや漏洩防止のための情報管理の方法について、情報管理について十分な対策をとる必要がある。

(「4.3 セキュリティ対策」を参照)

4.2 セキュリティ対策

分類	対策方法	内容
外部からの不正アクセス対策	ファイアーウォール導入	社内ネットワークと外部との境界を設定
	IPS / IDS ※	導入不正アクセスの進入検知もしくは排除
不正アクセス対策 データ盗聴、改ざんの防止	VPN 等導入	許可された者が外部から社内ネットワークにアクセスする際の認証および通信経路上でのデータの暗号化
端末管理 情報漏えい対策	ウィルス対策ソフトウェアの導入	コンピュータウイルスの感染防止、駆除、被害拡大の防御
	シンクライアントなどの端末の種類検討 端末操作制御ソフトウェアの導入	端末へのデータ保存や USB デバイスなどの外部記憶媒体への書き出しを制限
端末管理	検疫システムの導入	アクセスしてくる端末のセキュリティレベルの維持

※ IPS : Intrusion Prevention System(侵入防止システム)

IDS : Intrusion Detection System(侵入検知システム)

5. まとめ

IT を活用した「時間や場所にとらわれない働き方」には、企業にとって導入メリットが多いと思われるが、導入にあたっての課題として、セキュリティや導入するためのコストが重要と思われる。一方で、

情報セキュリティの確保は、テレワーク導入とは関係なく企業にとって必要な取組みであり、現在では技術的に高度なセキュリティを確保する廉価な機器も多数あり、導入が現実的となりつつある。

ワークスタイルの変革に向けた情報基盤として、クラウドコンピューティングは有効なツールとなると思われる。

以上

クラウドコンピューティング利用のメリットと課題の研究 ～ 利用者の視点から ～

I T ガバナンス研究会
千枝 和行

1. はじめに

クラウドコンピューティングが注目を集めている。

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。

初めは、Amazonなどが自社の余剰システム資源を他社に貸し出したのがきっかけであるが、意外に需要が多かったのが個別のビジネスとして立ち上げた結果、他社の参入を招き、ひとつのビジネス分野として拡大しつつある。

利用者は、利用するシステムの物理的な存在を意識することなく、ソフトウェアとシステム環境の双方の提供を受けることが可能なため、いわゆるシンクライアントで利用が可能であり、比較的低性能な「ネットブック」と呼ばれる小型の携帯用PCでも利用が可能である。しかも、インターネットに接続できれば、いつでもどこでも利用可能であり、いろいろなサービスを利用できることからユビキタスの実現のひとつの形とも受け取れる。

一方、システムを自己管理している企業や公共団体にとって、サーバー及びアプリケーション機能を所有から利用に変えることで管理コストや人件費の削減に貢献できることから、特に、公共団体でのサービス利用の普及に関して政府が中心となり、利用を進めてコスト削減をすることを方針に掲げている。

このような大規模サーバー群、仮想化による技術などをきめ細かいサービスとして提供していくことで、そのメリットを享受するとともに、利用に当たって見えてきた課題について、以下の文章で検討を進める。

2. クラウドサービスの利用例

現状のクラウドシステムでは、信頼性の観点で基幹システムに採用するには問題があり、またサービスメニューが少ないことから、主に情報系・管理系システムとして利用されている。(以下、この項は日経新聞より引用)

伊藤忠商事は、米国のサクセスファクター社のサービスを利用し、全社の人事管理を行なう。同社では、人事システムが拠点によって異なるという問題があったが、クラウドサービスを利用することにより、どこからでも人事履歴・人事評価の入力・参照が出来るように改善する。これにより、システム導入費用は従来の5分の1程度で済むという。当面は管理職のみ約2,000名の管理でスタートし、徐々に展開する。

損害保険ジャパンは、セールスフォースドットコム社のサービスを利用し、顧客からの苦情の問い合わせや、事故処理などの履歴を管理するシステムとして利用する。このシステムを営業

担当者や代理店の事務職員合わせて37万5千人が利用する。これにより、システム導入・運用費用を7割削減できると言う。

日本政府も、セールスフォースドットコム社のサービスを利用し、エコポイントの管理システムとして利用する。プロジェクトの立ち上げから稼働まで1ヶ月あまりしかなく、短期間の立ち上げは、同社でないと上手く行かなかったために採用した。

以下、次のような例もある。

情報系システムとして :ユニ・チャーム、東急ハンズ、ローソン

営業支援システムとして :ユニクロ

顧客管理・苦情処理システムとして:郵便局会社、HOYA

購買システムとして :パイオニア

3. 個人としての利用

Googleなどが行っているクラウドサービスを利用する個人が増えている。

ファイルサーバー機能や検索機能に加え、これまで培ってきたメール機能、スケジュール管理などのPIM機能、グループウェア的な機能、更には最近流行のツイッター機能などを織り込んだ、既存機能の総集編的なサービスの集合体であり、利用者にとって待ちに待った機能と言っても過言ではない。

クラウドサービスを個人で利用する場合は、ソフトウェアを自前で用意する必要がないことから、ネットブックPCなどの低性能PCでも手軽に利用が可能である。その上、ファイルやメールを自分のPC上に記憶しておく必要が無いことから、インターネットに接続さえ出来れば、いつでも、どこからでも利用が可能である。

このことは、利用者に次のようなメリットをもたらす。

- ①いつでもどこからでも利用できるため、細切れ時間を利用してレポートを継続作成できるなど、細切れ時間の効率的利用や、時間管理を合理的に実施できる。
- ②ファイル・メールを持ち歩いて紛失する恐れが無く、セキュリティ上安全である。従って、PCも自前のものである必要が無い。
- ③メールの送受信でも、誰かにプレゼンテーションするときでも、Web接続さえ出来ればその場ですぐ実行できる。
- ④同一サービスで、複数の人の間でファイルを共有できる。

等々・・・。

作家、レポーター、営業担当者、出先で業務をしなければならない人などには大変重宝するものと思われ、ネットワーク環境さえ意識しておけば、いつでも安価に利用できるのも、個人利用や出張・外出が多い人には利用価値が高く、急速に普及していく可能性が大きい。

また、ソフトウェア開発の環境を個人単位でクラウド上に持つことが可能となり、新たなソフトウェアの個人ビジネス手段として利用でき、また、個人が情報発信するターミナルとしての手段としての可能性もある。

それによって、新たなサービスが生まれ、ビジネスチャンスにも繋がることが考えられる。大い

に期待したい。

4. 組織体としての利用

(1) 公共組織(政府、地方公共団体、公法人など)での利用

公共組織では予算削減が緊急課題であり、総務省が中心となってクラウドサービスを利用することが叫ばれ、その検討が始まっている。

これは、政府を初めとする公共組織の予算膨張を少しでも軽減するために、コア業務でないシステム管理を外出しにしてコスト軽減を図ることが差し迫った課題になっているからである。特に社会保障関連の予算の全体支出に占める割合が年々増加することが見込まれることから、相対的な費用抑制が必要となる。

従って、2009年8月から新政権に変わって後、「事業仕分けによる3兆円削減」の政府予算の見直しを行ったのは当然のことである。このような状況下であるので、少しでも無駄な費用は抑えるためにクラウドシステム活用によるコスト削減が必須なのである。

地方公共団体も同様の状況であり、今後システムを順次更新していくにあたり、コンピュータリソースをクラウドシステムに移行していく方針が打ち出されている。

昨年調査し、報告した自治体EAについても、クラウド化は避けられず、共通アプリケーションを提供するAPLICの動向が注目される。こちらの方も、新たな事実が出てきた場合、引き続き調査・研究を行う予定にしている。

(2) 私企業での利用

殆どの大手・中規模企業は、自社内にコンピュータシステムを持っており、情報管理と活用がなされている。

個別企業が自社でのシステム開発を行わずサービスを利用するのは、

- ・巨額な開発費がかかる銀行システム(中小の銀行の利用)
- ・企業間での共同利用が必要なExtraNetを利用するシステム
- ・中規模企業でASPや共同利用するシステム(自社内では維持できない)
- ・大企業の系列企業で共同利用がされているシステム

などであり、大いに普及しているとは言いがたい。

日本企業では業務の定型化を避け、独自のやり方を行なう傾向がみられるが、他社への差別化の仕組みを、コンピュータシステムの仕組みを通じて実現しようとする企業が多いことが原因のひとつと考えられる。

他社への差別化システムとしては、ユナイテッド航空が開発した航空券発行システム「SAVE R」やFEDEX(フェデラルエクスプレス)の荷物追跡システムが有名であるが、筆者の考えでは新たな製品を生み出す研究開発用のシステム及び顧客満足度を高めるシステム以外は、各社が個別に独自システムを持つ必要がないと感じている。

基幹システム(生産、物流、経理、決算など)は企業独自のやり方を行う必要は少なく、既存のERPパッケージシステムやASPなどの利用でコストを抑え、そこで浮いた費用をコアビジネ

スの分野に集中投資することが競争力を高める方策と考えられる。クラウドサービスの利用はコスト抑制に貢献することが期待できる。

また、大規模以外の企業においても、グループウェアの導入により経営の「見える化」や情報伝達・共有は既に行われて成果を上げており、そのシステム管理を外部サービスに置き換えてコストを抑えることが出来れば、これまた企業の体質強化に繋がると考えられる。

更に、システムリソースの使用量に波があり、日時処理、月次処理、年次処理などで大量のリソースを必要とするが、それ以外の時期においてはシステム利用量が下がる企業では、その都度システムの増設をおこなうより外部サービスの利用がコスト的に望ましい。コストの固定費化を避け、費用として処理できるからである。

ただ、現在公表されているサービスからは、利用者がクラウド化に積極的に取り組まなければならないサービスの提供が少ないことも事実である。

(3)クラウドシステム利用の形態

クラウドシステムの個人の利用形態、メリットについては述べた。

では、組織体が利用する形態は、どのようなものであろうか。

サービスを提供する側からは、いくつかのサービス形態が提案されている。

①コンピュータリソースのみを提供する(Haas)

- ・一般文書の保管・検索用に利用する。特に画像・イメージ文書は大容量を必要とし、現状でも文書量が増え続けて、ハードウェアをいくら追加しても追いつかないような運用をしている場合は好都合である。
- ・企業の過去資産のバックアップストレージとして利用する。

②開発環境を利用する(PaaS)

- ・Webシステムなど、早期にシステムを立ち上げたい場合に、開発環境ごと利用する。
- ・本番環境以外に、開発環境を自社内に持ちたいがリソース的・コスト的に難しい場合に利用する。
- ・開発サービスを行っている場合で、顧客ごとに別の開発ツールが必要な場合、その開発ツール毎に利用する。

③アプリケーションプログラムごと利用する(SaaS)

- ・ビジネスの基本機能(メール、メモ管理、スケジュール管理、掲示板、表計算など)のみを利用する。
- ・セキュリティ管理が要求されないe-Learningシステム、会議室予約システムなどを利用する。
- ・自社のシステムと連携するハイブリッドシステムとして利用する。高い機密性を要求されるシステムのみを自社内で管理し、残りのシステムをクラウドシステムとして利用する。
- ・ERPなど基幹業務の業務パッケージごと利用する。

•ExtraNetのようにジョイントビジネスや共同利用の共有システム環境として利用する。ビジネスが発生した時に契約し、終了した場合に解約すれば余計なシステム資産を持たなくて済む。

④アプリケーションプログラムごと利用する(Saas+α)

•ビジネスツールをコンサルティングサービス付きで利用する。特にベンチャー企業がビジネスを立ち上げて間もない時期、若しくは自社内にそのようなリソースを持つことが出来ない企業が、サービスとしてアシスタント機能付きで利用する。

⑤サーバーを統合して企業内集中運用する

•従来ある分散型サーバーを集約し、マルチOSと仮想技術を利用することで複数の業務アプリケーションを企業内クラウドシステムに集約し、集中型運用として利用する。

(4)クラウドシステム利用のメリット

クラウドシステムの利用には、以下のようなメリットが考えられる。

- ①シンクライアント志向なので、PC上にビジネスソフトが無くても利用できる。
 - ②システム資源をスケーラブルに利用できる。特にシステムリソースに時間的・季節的な要因で凹凸がある場合、利用料に応じてシステムリソースを選択利用でき、自社保有のようにその都度システム資源の買い増しを行わずに済む。
 - ③コンピュータシミュレーションなど、一時的に大量のCPU資源が必要とされる場合に、サービスで利用できる。
 - ④システムリソースを自社内にまったく持たない運用も可能になる。
 - ⑤新たな開発環境をシステム資源の購入無しで利用できる。
 - ⑥プロジェクトごとにシステムリソースを確保できる。プロジェクト終了時に契約終了だけで済む。
 - ⑦災害対策などのバックアップシステムを自社内に持つ必要が無い。
- 等々・・・。

システムリソース丸ごとの利用でもいいし、システムを細かく区分し、その区分ごとの利用でもいいという具合で、とにかくスケーラブルに従量制で利用できて、コストとして管理できるメリットが大きい。

(5)組織体(企業・公共団体など)が利用できる環境

現在喧伝されている組織体向けクラウドサービスは(3)に示した通りである。

サービスメニューを見ると、どちらかというとシステム会社やシステム関係者向けのサービスが主体であって、基幹業務や利用者が十分に使いこなせるようなサービスメニューは少ないと感じられる。

基幹システムなどをクラウド化するには、システム管理が「法的な堅牢性」を持っていないといけないが、現状ではサービス提供メーカーが売り上げ停滞を解決するための営業上のデモンストレーション的な売込みが多く、利用者がすぐに飛びつく様な環境が多く提供されている

とは理解しがたい。

そもそもクラウドコンピューティングの定義も、また到達点の青写真も曖昧で、サービス提供会社主導で進められているので、組織体の多くは暫くの間は様子見という選択を取らざるを得ないと考えられる。

また、日本の公共団体が利用するには、やはり行政法などに対する「法的な堅牢性」が担保されている必要があり、海外の会社が提供しているサービスでは難しく、官公庁の指導で国内クラウド提供メーカーが独自の対応を迫られる可能性が考えられる。

5. クラウドシステムの導入

クラウドシステムを導入・利用するためには、組織体として準備しておくことがある。

クラウドシステムを利用するには、どのシステムをクラウド化するのがいいかの判断が必要となる。そのためには自社のシステム環境の洗い出し、重要度・優先度などに基づくマッピング情報が必要となる。

そして、それらはシステムの再整理を伴うのでITのコンサルタントと協働で進めなければならない性質のものである。単に、既存システムを外だし、若しくはサーバー集約を行なえばいいというものではない。

現状のシステムのハードウェア構成、データベース構成、ソフトウェア構成、マスターデータ配信構成、ネットワーク構成などを洗い出し、マッピングとランク付けを行う必要がある。

6. クラウドコンピューティングのIT統制

(1)リテラシー(有効性、効率性)面

クラウドサービスを利用すると、メール機能、PIM機能、グループウェア機能、全文検索機能などが選択的若しくは統合的に利用可能となる。

事務処理としてみれば、統合的なサービス提供利用で効率的な利用が期待できる。

企業内にある文書を全文検索機能で検索(勿論セキュリティは付ける)出来るようになれば、文書の所在や内容の「見える化」が進み、一種のナレッジマネジメント的な利用に進むと考えられる。当然ノイズ(不要ファイル)のヒットも多くなるが、文書整理しながら進めれば、ナレッジの質の向上が図られることが期待できる。

基幹システムやデータベース内のデータは、全文検索で検索しても有効な情報が得られる可能性は低い。これらの情報は、生データから必要な情報を一次加工して他の情報とレベル合わせを行った上で全文検索をおこなうと、より有効な活用が推進される。

これら企業内の情報・データは、統合的に検索され、活用されることによってPDCA的なサイクルが生まれ、企業における情報を扱うリテラシー全体が向上していく。

情報の統制をおこなう場合、アクセス権の設定によっておこなうのがひとつの方法であり、複合的なACLの設定を行なうことによって、情報統制が可能となる。もうひとつは実際のアクセス状況をモニタリングし、分析と評価を行なうことで、異常アクセスなどを早期に発見でき、対策を

取ることが可能となり、コントロール性が増す。

(2) マネジメント(安全性、信頼性、機密性)面

クラウドコンピューティングを社内のみでまかなう場合のIT統制は、従来のIT統制と変わりはない。

クラウドコンピューティングを社外サービスで利用する場合は、その統制水準・統制内容はサービスの提供会社に依存してしまう。その多くはSLAとして確認される内容となる。内部統制に対しては「公認会計士協会 18号監査報告書」や「AICPA SAS70報告書」の提出に対応していなければならない。それらの報告書を入手できない場合は、自らが監査を行なって報告書を作成しなければならない。

管理の水準に関しては、ITIL (ISO20000) など公的基準を採用している場合は一定の統制が担保される。

公的基準で運用がなされていない場合はその水準の証明が難しく、SLAなどで確認していくことになる。必要がある場合は、システム監査なども実施しなければならない。

実際の運用は、コンピュータの稼動に関してはクラウドサービスが持っているログ機能とモニタリング機能を活用し、操作面に関しては、記録を点検して分析・評価することで、コントロールすることが可能となる。

7. クラウドコンピューティングが内包する課題

(1) ハードウェア・ソフトウェア・アプリケーション面

利用の自由度が高いクラウドコンピューティングではあるが、いい面ばかりではないので、その問題点・課題を把握しながら利用する必要がある。

以下に問題点を列挙する。

- ①システムを自社でコントロールできない(業務の安定性確保が出来ない)
- ②パフォーマンス、信頼性がベンダー依存になってしまう。(同上)
- ③マルチベンダー化ができないかもしれないので品揃えに制限がでる。
- ④業務全体の情報整合性をとれなくなる可能性がでてくる。
- ⑤処理が定型化するので、EUCで補足する必要がある。
- ⑥ベンダー監査が必要になる。(説明責任裏づけが必要になる)
- ⑦法規制に係るシステムには利用できないケースがでてくる。
- ⑧外出しするには各システムのポジショニング評価が必要になる。(余分なコスト)等々・・・。

停止することが許されない重要システムでは、①や②の問題があり、現状のサービス稼働率(99.9%程度)では採用に二の足を踏む企業が多い。

システムの信頼性・安全性・機密性などを証明しなければならないシステムに関しては、①や⑥や⑧の問題があり、内部統制に対しては「公認会計士協会 18号監査報告書」や「AICPA SAS70報告書」の提出に対応できなければ採用することができず、法規制で情報が格納され

ている場所を物理的に隔離しなければならないクラウドシステムでは、その独立性を証明する必要がある。

それほど神経質にならなくてもいい場合であっても、③や④や⑧のように自社に残すシステムとのシームレスな連携を新たに検討しなくてはならない。特にマスターデータのデイリーの配信は重要で、事前によく考えておかなければリスクが大きい。

企業によっては独自処理をフロントエンドシステムで行っている場合があり、それらのシステムの扱いも検討せねばならず、後処理をEUCで行っている場合は、それらの連携も考慮しなければならない。

TCO (Total cost of ownership) とすればコストダウンにはなるが、安くなるのはシステムの開発費・運用管理費やクライアント費だけであって、その周辺のコストは下がらないと考えないと予想外のコスト増加に見舞われる場合が起こり得る。

いずれにしても、企業や公共団体が安全に利用するためには、監査報告書の提示が必要で、それが出来ない場合は定期的なベンダー監査を行うことが望ましい。場合によっては、利用者が共同でチームを編成して行っても、実施しておくほうが望ましいと考える。

(2) ネットワーク環境

外部を利用するクラウドシステムは、明らかにネットワークがボトルネックになる。

インターネットを介すにしろ、基幹システムを外出しにした場合、ダウン対策やネットワークの冗長性の確保などが企業側の努力として必要になる。

場合によっては、システム提供会社と直接ネットワーク接続を行う必要が出てくる場合もありうる。

しかも、ネットワーク経由の大量バッチ処理やクライアント/サーバーのリアルタイム処理などには不向きで、制限事項を考慮すると、外部クラウドを利用できる範囲は限定される場合も有りうる。

セキュリティ面では盗聴やウイルス感染対策が必要となる。新しい防御技術が生まれても、それを破る技術も生まれ、イタチゴッコが避けられない。

これも利用者側のリスク負担要素となる。

8. ITCとして考慮すべきこと

コスト削減に貢献が期待されるクラウドシステムであり、経営者の関心も高くなると思われる。特に官公庁がクラウドシステムの検討を叫んでいるので、余計その傾向が高まると予想される。

ITCが顧客の持つシステムのあり方の再検討を、クラウドシステムを含めた見直しとして聞かれた場合、以下の事に注意して検討する必要がある。

- ①その企業の業界におけるポジショニングはどうなっているのか？ (競合ポイント)
- ②その企業のシステム利用の成熟度はどの程度か？ (利用者レベル)
- ③コンピュータシステムを利用した他社への差別化は行われているか？ (戦略性)
- ④業務推進上で法律上の規制はあるか？ (制約)

⑤システムの機能別の区分けは行われているか？、特にマスターデータの連携の設計図は確立されているか？ (鳥瞰図)

⑥企業情報の区分とライフサイクルは確定しているか？ (情報のライフサイクル)

⑦システム運用のコスト(固定資産、運用経費、社外人件費、社内人件費、利用者の人件費など)が把握されているか？、特にTCOとして定期的に把握されているか？ (コスト構造)

⑧資産(ハードウェア、ソフトウェア、アプリケーションなど)のライフサイクル管理は行われているか？ (管理レベル)

コンピュータシステムの見直しは、利用の成熟度とシステムのライフサイクルとして捉えるべきである。そして、クラウドシステムのような新しいサービスをどのように取り入れていくかは、その前に対象企業の管理がどのようになっているか、コスト構造がどのようになっているかを定期的に把握しておき、その比較として検討される必要がある。

その上で、

①システムの重要性 (止まっても大丈夫か)

②情報のシームレス度 (連携できるか)

③他社への差別の度合い (戦略性はあるか)

④コスト構造の変化の度合い (ほんとうにコストダウンか)

⑤運用上のメリット・デメリット(他に阻害要因は無いか)

などを総合的に評価し、判断した上で導入検討を進めていく必要がある。

ポイントは、企業の体質強化に繋がるかどうかの見極めであり、そういうインパクトが無い場合、見送ることが賢明と考えられる。

9. おわりに

クラウドコンピューティングは、個人的にはユビキタスを実現し、企業組織的にはサーバーやシステムの再編成とシステム資源のフレキシブルな運用、コスト低減をもたらすものとして期待されている。また、統制面に於いても、ログ機能やモニタリング機能を活用することによって向上することが期待される。

もともとはAmazonなどの会社が、自社のIT余剰資源を貸し出したことから始まっているが、現在公表されている内容を見ると技術的には既存のものを多く利用しており、従来の技術の延長若しくは再編成によって、主として規模の経済を狙った新しいビジネスとして展開が進んでいる。

誤解を恐れずに表現すれば、お金の保全に関し、従来は自宅にタンス預金していたものを、新しく銀行ができたので、その分厚い壁に囲まれた金庫に保管してもらう様なものである。それぞれ一長一短があり、決めるのは利用者側ということになる。

現状の利用サービスメニューは多くなく、自前システムを移設することからはじめなければならぬかもしれないので、既存システムを持つ企業組織体の多くは、競合他社や市場動向を見ながら、可能な部分から利用拡大を図っていくことになる。

一方、システムをまったく持たないベンチャー企業などにとっては、ゼロから短期間でしかも低コストでシステムを立ち上げるのが可能なので、利用メリットは大きい。

システム提供会社にとってもビジネスチャンスと捕らえ、製品の品揃えに経営資源を向けているが、コンシューマー向けサービスを考えた場合、日本国内のビジネス展開では土地の面積・価格や回線事情などから、米国の様な大規模サーバーを設置できる環境を確保することが困難で、むしろ中国のような土地や人件費が安い国や税制優遇国家に進出してグローバルビジネスを考えたほうが良いようにも思える。現にIBM社では、中国を初めブラジル、インド、韓国、ベトナムにクラウドセンターを構築している。

ソフトウェア面や法規制対応では日本は米国に大きく遅れをとっているが、情報システムの統合連携サービスの方向に進んでいくことを前提に、いろいろなサービスが生まれてきて需要拡大の機会が訪れたと感ぜられる。

いずれにしても、中小の企業においてもIT資源を安価に利用できるチャンスが訪れてきているので、IT資源を利用するのは当たり前になり、利用面において他社に差別化できる様な使い方を生み出せるかどうか企業が躍進の鍵になるとと思われる。

以上

ITC視点でのクラウドコンピューティング考察

2010.04.29

古川正紀

1. 考察のきっかけ

インターネット経由で各種サービスを提供するクラウドコンピューティングは、その形態自体は特に目新しいものとは言えない。SaaSのようにインターネット経由で業務用アプリケーションを提供するASPは従来から存在するし、そもそも、ネットワークコンピューティングは既に様々なかたちでビジネスに浸透している。

SaaSに関しては、経済産業省が推進する中小企業向けSaaS事業として「J-SaaS」がある。主に従業員数20人以下の小規模企業を対象として、財務会計などバックオフィス業務から電子申告までを一貫して行える、便利なワンストップサービス(SaaS活用型サービス)を官民連携して構築・普及を目指している。これは、中小企業の会計力・経営力向上と電子申請の活用を同時に促進したものと見えよう。

ただ、クラウドコンピューティングにはSaaSばかりではなく、アプリケーションを実行するための“プラットフォーム”自体を第三者に提供するPaaS、更にはOSなども自由にインストール可能な仮想マシンやストレージといった“インフラストラクチャ”を提供するIaaSも含まれる。また、仮想化技術などを活用した大規模データセンターの構築に長けた企業が提供するクラウドに加え、企業内でのクラウド型システム構築(いわゆるプライベートクラウド)を行うサービスも出てきている。

今年度のITガバナンス研究会課題「クラウドコンピューティング」について、ここでは現在の日本における全体的な位置付けから推し量り、近い将来ITコーディネータとしてこの道具(手段)をどのように使いこなすのが相応しいかを考察してみたい。

2. リクルート社が実施したアンケート結果

リクルート社キーマンズネットが2009年6月に、500人弱の会員を対象にアンケートを実施した結果がある。母数を構成している人たちの多くが、ITベンダーの人たちや企業のITセクションの人たちと思われるので、幾分先進的な結果傾向が出るのは止むを得ない。

その結果から見ると、クラウドコンピューティングの中で最も利用したいと考える提供サービスについては、「SaaS(アプリケーション自体の利用)」が約7割を占め、「PaaS(プラットフォームとしての利用)」は約12%、「HaaS/IaaS(ハードウェアもしくはインフラとしての利用)」は約15%となっている。クラウドコンピューティングがよりいっそう浸透すれば、比率はもう少し変化する可能性はあるが、現状では妥当な結果と言えるかもしれない。しかし、「PaaS」利用が多いのではないかと予想していた筆者の思惑は、大きく外れた結果となって出ている。

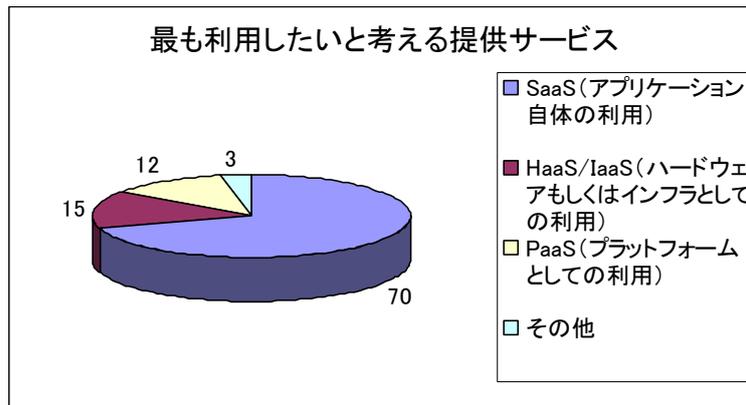


表-1 最も利用したいと考える提供サービス

また、若干視点を変えたものとして、クラウドコンピューティングを活用する場合、どのような利用形態が最適と考えるかという質問もあったが、この場合には「サービスを利用」が約 47%、「自社にクラウドインフラを導入」が約 15%で、「混在利用(ハイブリッド型)」という回答者も約 37%に及んだ。これは例えば、導入する分野に応じて利用形態を使い分けたいということであろうと思われる。

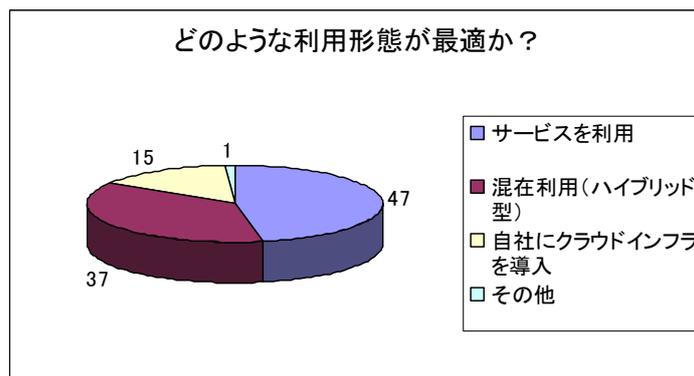


表-2 どのような利用形態が最適か?

クラウドコンピューティングによるサービスは、既に従来型の製品やサービスと比較検討を行う段階に入っているかという問いに対しては、やはり「いいえ」が最も多く、半数強に達している。ただ、逆に考えれば、「比較検討の対象としている」「近いうちに比較検討を行う予定」を合わせれば約半数となるわけで、話題先行の段階よりも、やや具体的な検討段階に入ったと言えるのかもしれない。これは前述の「J-SaaS」が本格稼動された2009年4月以降に実施されたアンケート結果であることも影響しているのかも知れない。

3. クラウドコンピューティングを適用したい利用分野

クラウドコンピューティングを適用したい利用分野については、「本番環境を含む情報系システ

ム」(約 48%)、「PC クライアント環境のクラウド化」(約 40%)が若干多い程度で、あまり目立った差はないように思える。しかし、クラウドコンピューティングを適用できないと考える利用分野では、「基幹業務システム」(約 52%)のみが突出する結果となった。

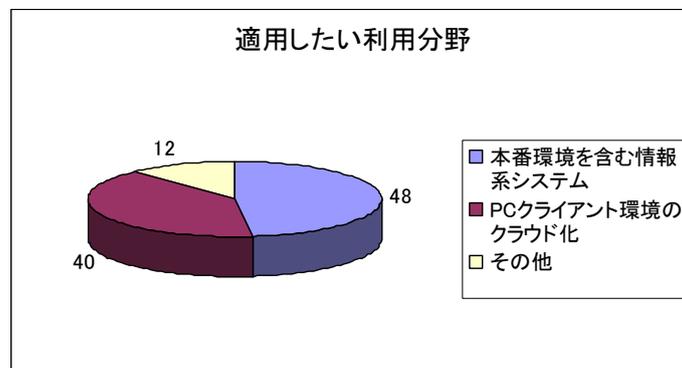


表-3 適用したい利用分野

これは企業活動における重要度が高く、システムの信頼性も要求されるという理由だろうが、前述のプライベート・クラウドも含めて考えているか否かによっても、状況は変わってくるのかもしれない。適用したい/適用できない分野に関する線引きに関しては不変かという質問を見ても、「まったく不変」という回答は約 6%にとどまっており、「自社インフラへの導入か否かなど、利用形態によって異なる」(約 25%)、「今後の技術向上によって変わるかもしれない」(約 48%)という人が多いのが、未確立の状況をよく見てとっていると思われる。

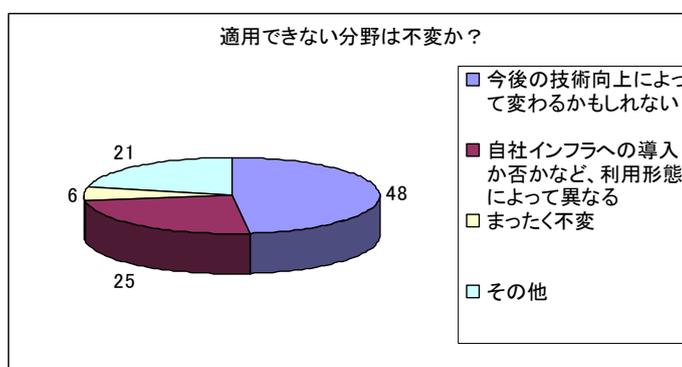


表-4 適用できない分野は不変か?

料金体系については、多くの回答者が「固定の初期コストと運用コスト」(約 46%)が最適と考えているようである。「使用容量やデータ転送量による従量課金」(約 20%)を選んだ回答者はコスト低減を期待する一方、固定を選択した方はほとんどが“コストが変動すると予算化しにくい”という理由を挙げている。また、初期コストに関しては要・不要それぞれに様々な捉え方があるが、“クラウドコンピューティングとはいえども導入に際して一定のコストはかかるはずであり、それが運用コストに乗せられるよりは、初期コストとして明瞭に計上されるほうが望ましい”という考えが大勢だ。この点は「J-SaaS」の売りの部分(初期費用ゼロ)と、見方として大きく異なっており、注

目に値する。

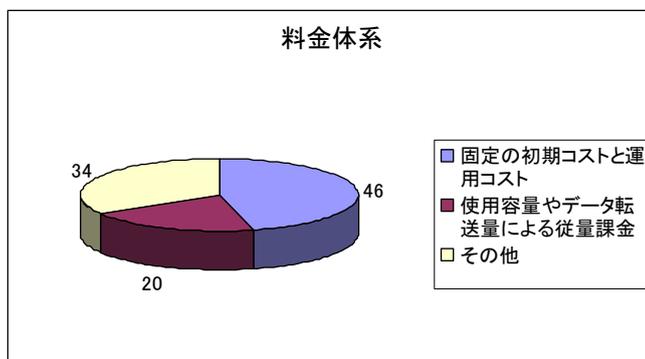


表-5 料金体系

次に、サービスレベルに関しては、「速度・品質など、契約時に定めたサービス水準を保証（SLAに基づくコミット型）」が望ましいという回答が約68%に及び、「価格が少しでも低くなるのなら、サービス水準に対する保証はなくてよい（ベストエフォート型）」（約29%）を大きく上回った。重視する項目については複合グラフで示しているが、大まかに言えば、「業務継続性（信頼性）」「性能（レスポンス）」「データ保護（バックアップ）」の順となっている。

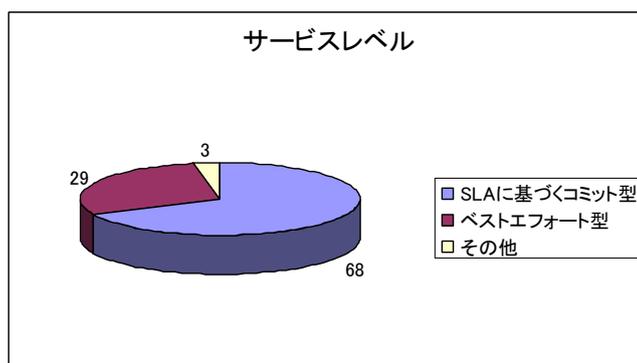


表-6 サービスレベル

4. クラウドコンピューティングの不安要素

クラウドコンピューティングにおける不安要素については、1番目に「導入実績・事例の少なさ」を挙げている人が多く、以下、「仮想化等の技術の未成熟による不安」「ベンダごとの対応・定義の違い」と続く。「サービスレベルの低さ」と回答した人は意外に少なかったようだ。

また、「サービス提供元が国内事業者か海外事業者かにこだわるか」「データの保管が国内か海外かにこだわるか」という点のいずれも「なるべく国内」が約7割、「こだわらない」が約3割という結果となっている。事業者に関しては、サポート体制、日本独自のビジネス様式や業務プロセスへの理解といった理由で、「なるべく国内」と回答した人が多いと思われる。また、データ保管については、セキュリティがしっかりしていればどちらでもかまわないが、なんとなく国内のほうが

安心できるという意識にすぎないように思われる。

正直なところ、クラウドコンピューティングと一口に言っても、その意味するところは幅広く、しかも曖昧である。Google や Amazon といった巨大サービス企業が、自社のシステム構築で培った技術や潤沢なリソースをパブリッククラウドとしてビジネス化した意図や利用メリットは容易に認識できるものの、現在では多岐にわたる分野で“クラウド”という言葉や概念が用いられており、それぞれのサービスが具体的にどのような内容のものなのか、どういったメリットがあるのかは見えにくいケースも多い。

ただ、逆に言えば、既にクラウドは一般的な概念となっており、アプリケーションにせよ、プラットフォームやインフラストラクチャにせよ、「所有から利用へ」という特色をうまく活用すれば、企業システムの一部、もしくは全体のトータルコストや運用・管理負荷を低減できる可能性があることも多くの人が認識済みだ。もちろん、そのためにはシステム間の連携など、解決すべき問題もまだまだ残されている。現時点では何をクラウド化するのか、そして、何をクラウド化しないのか。利用企業もサービス提供側も、まずはそのあたりを見極めていく段階と言えるだろう。

5. パブリック・クラウドとプライベート・クラウド

クラウドサービスが汎用的な IT インフラとして普及していく過程では、多様な利用目的に適合するための、サービス自体の多様化が進んでいくことになる。この流れのなかで、「パブリック・クラウドサービス」「プライベート・クラウドサービス」の区別がなされることがある。この分類も、クラウドという言葉そのものと同様、意味が大きく揺れている。

「プライベート・クラウド」は、「企業の社内における、サーバ仮想化技術を生かしたクラウド的な環境の構築および運用」の意味で用いられてきた。この延長線上で、「プライベート・クラウドサービス」という言葉を「特定のユーザー組織だけのために外部の主体が運用するクラウドサービス」という意味で用いている人々がいる。その一方で、企業の社内システム運用をターゲットとした自社のクラウドサービスを、プライベート・クラウドサービスと呼ぶ事業者が増えてきた。従ってここでも、言葉の正確な定義を議論することには、まったくメリットがない。

ただし、社内システム運用向けのニーズに応えるための試みが活発になってきているのは重要な動きであり、これを無視することはできない。ここでは、便宜上、概念としての社内システム運用向けクラウドサービスを広く「プライベート・クラウドサービス」と呼ぶことにする。

プライベート・クラウドサービスでは、レスポンス、可用性、セキュリティ といった、企業 IT インフラの構築と運用において重視されてきた要件を、どうクリアするかが 1 つの課題となる。一方、企業の社内システム用途では、Web サービス事業者に重宝されるような、リクエストの増減に応じた IT リソースの機動的な伸縮といった要素の優先度は低下する。

プライベート・クラウドサービスと呼べる1つの典型例を、大規模SI業者やシステムベンダが提供するクラウドサービスに見ることができる。

これらの企業が提供するクラウドサービスは、従来のITアウトソーシングサービスの「切り売り」、あるいはITアウトソーシングサービスのエントリ商品とも形容できる性格を持っている。基幹システムや、ITインフラ全体の運用代行を行ってきたITベンダーが、サーバ1台など従来よりも小規模な単位で、より低価格なバージョンとして提供するものと表現できる。

これらのサービスでは、料金体系はあまり明確ではない。すぐに利用開始できるような機動性もない。それよりも、個別対応が特徴といえ、データセンターへの接続も、専用線やVPNなど、ユーザー企業の要望次第で対応するというのが基本的なスタイルだ。一般的にはサーバ仮想化技術を使っているが、物理サーバを専用に割り当てるのかも顧客次第だろう。要するにすべては顧客次第で、企業が社内で構築するようなITインフラ環境を、事業者のデータセンターに移動して運用するということが基本だ。こうしたサービスなら、上記のレスポンス、可用性、セキュリティといった要件は容易にカバーできる。クラウドといっても、実体はカスタムメイドの環境を運用するだけだからだ。当然、効率性やコスト削減効果についても大きな期待がしにくい。

今後は現在のパブリック・クラウドサービスと、ITアウトソーシングの切り売りのプライベート・クラウドサービスのバランスをとったサービスが増えてくるはずである。一方で、パブリック・クラウドサービスを、レスポンス、可用性、セキュリティといった点で補うサービスも登場してくるだろう。

6. ITコーディネータとしてのクラウドコンピューティングへのアプローチ

ここまでリクルート社が実施したアンケート結果を基に現在のクラウドコンピューティングの状況を分析してみた。ここで利点・欠点を纏めてみよう。

【利点】

- ・ 立ち上げスピード … すぐに使い始められるし、やめるのも容易である。
少ない予算でも迅速にシステムを立ち上げることができる。そして、立ち上げたその瞬間から、もう世界と繋がっているということは大変優位である。
- ・ スケーラビリティ … 使用量に基く価格設定が可能である。
通常、業務の繁忙期と閑散期の浮き沈みが激しい場合、繁忙期に合わせてITリソースを準備しなければならないので、繁忙期の部分をアウトソースすることが可能となると、明らかにコストを抑えられる。
- ・ 変化への柔軟な対応 … 処理量の急激な増加に迅速且つ柔軟に対応できる。
長期契約の必要もなく、ITリソースを必要なときに必要なだけ手に入れることができるの

で、ごくわずかなコストで、あらゆる面でアジリティを高めることが可能である。

【欠点】

- ネットワーク環境 … 膨大な量のデータのやり取りが発生する場合、潤沢なネットワーク帯域が必要。
膨大な量のデータを社外のクラウドとやり取りすると、非常に大きなネットワーク帯域が必要になる。ネットワーク・コストを考えると、自社でストレージをそろえた方が安上がりなケースも発生しうる。
- アプリケーション・パフォーマンス … 現在利用しているアプリケーションが、そのままクラウド環境でも、問題なく使えるのか…？
アプリケーションのアーキテクチャによっては、利用できるクラウド・サービスが制限されるケースもありうるし、従来とまったく変わらないパフォーマンスが確保できる保証はない。
- 取り扱いデータ … セキュリティー規約などで制限を受けるデータの取り扱いはどうするか…。
競合他社を利するような機密情報や顧客の個人情報などのデータを扱うアプリケーションをパブリック・クラウドに置くことに関しては、賛否両論があろう。一般的には避けられるケースが多いと思われる。
- メリット享受の限界 … 規模が大きくなるに連れ、メリットは薄くなる。
一般的に規模が大きいほど、ITリソースのプールも大きい。そしてITリソースのプールが大きいほど、パブリック・クラウドにアウトソースする場合の金銭的メリットは少なくなると考えられている。この場合は、プライベート・クラウドを構築した方が経済的だと考えられる。

ITコーディネータとしてクラウドコンピューティングへアプローチするには、この利点・欠点を良くわきまえ、利用者がより多くの利潤を得るように企画提案しなければならないだろう。

7. クラウドコンピューティングのまとめ、結論

システムの歴史は「集中」と「分散」を繰り返してきたが、今は「それが同時に起きている」状況と言えよう。

「クラウドコンピューティング」という言葉を言い出したのはグーグルの人であり、「Computer」ではなく「Computing」であることがミソである。

(注: Computer「そのもの」ではなく、「使い方」(又は利用する「スタイル」)を指している。)

クラウドコンピューティングとは一言で言ってしまうと(自分で所有するのではなく)「借りる」ことである。つまり、「(すぐ)使えれば誰が所有していいやうが関係ない」という発想であり、例えば車で言えば「レンタカー」のようなものである。

コンピュータなるものは、相当簡便になった今日と言えども、実際に使えるようになるまで時間

と手間が掛かるものである。構成を選んで、発注して、製造して…枚挙に暇が無い。

これを借り物で済ませ、その代わり簡便な使い方の環境を手に入れる…、クラウドコンピューティングとは「割り切り」である。(車を、家を、PCを所有しなくても)「走れば良い」「寝られれば良い」「計算できれば良い」と言うもので、「割り切り」である以上、制約が在るのは当然と認識すべきである。

よく「クラウドってあの『コスト削減』のやつでしょ?」と言われるが決してそうではない。今までがあまりにも無駄が多すぎただけである。これがクラウドコンピューティング選択の決め手ではないことに注目すべきである。

クラウドコンピューティングの特徴として、「ネットワークを通じた利用」(=手元にある必要がない。どこにあらうが関係ない。),「必要に応じた利用」(=大量のリソースのオンデマンド利用=不要になったら停止すればよい。),スケールアウト型システム(=1人で作業して100日よりも、100人で作業して1日、という考え方)が挙げられる。

一人に集中すると、1人(個人)の処理能力への依存度が高くなってしまふのと同じで、自社で所有する、1台のコンピュータリソースに集中すると、その処理能力への依存度が高くなってしまふ、リスクも高まるわけである。

これを回避すると言う観点でも、クラウドコンピューティングを採用する意義は存在する。

ただし、コンピュータのアルゴリズム的には、クラウドコンピューティングは「集中」「順列処理」が基本である。

「分散」させて「並列処理」を行うメリットとしては、「機械損失の回避」が挙げられる。たとえば、たくさんのお客さんを待たせないようにする、等であるが、クラウドコンピューティングには、複雑なJOB制御は向いていない。

クラウドコンピューティングの実例としては、「Amazon EC2」がDBを高速に動かせるしくみとして、インフラ利用(PaaS、IaaSの領域)として有効であることが認められ、よく知られている。

G-mail、hotmailをクラウドコンピューティングという人もいるが、これは定義範囲の広げすぎと思われる。

SaaSではマッシュアップ技術の活用がユニークである。たとえばグーグルマップであるが、地図のみで完結しないで、お店情報の一部として組み込んだりすることも可能である。これは注目すべき領域と言えよう。

パブリック・クラウドは、不特定多数にクラウドサービスを提供するので、セキュリティ確保には充分留意しなければならない。(銀行カード・クレジットカードで決済など…)。

プライベート・クラウドは、社内や関係者に閉じたクラウドサービスを提供するので、データ保護にメリットがある。

クラウドコンピューティングの主戦場はPaaSと言われている。中でも代表格のForce.comは有力である。

CRMシステムをSaaSとして提供しているので、ユーザーを多く抱えている。(SaaS発のPaaSと言われている)

IT コーディネータとして、「自分で SaaS インフラを作りたい！」と言う場合は、Apache Hadoop プロジェクト(HDFS や Hadoop Mapreduce)や Eucalyptus (Amazon EC2、Xen)が活用出来よう。

仮想化技術はクラウドコンピューティングにはもはや必須技術である。サーバ仮想化の例では、10 台分が1台に統合可能と言われている。保有コスト(スペースや消費電力)が削減されることは言うまでもない！

分散型ストレージの例としてまたもやグーグルが代表格として挙げられる。壊れたディスクは使い捨てだそうで、生きているディスクのどれかにアクセスできればOKという発想。(自前文化では発想できないところまで進んでいる…。)

key-value 型の特徴として、リレーショナルDBのような結合の仕組みはないフラットなDBとのこと。リレーショナル…はクラウドに向かないとのこと。

「スケールアウト」は発展途上の考え方のようなものである。良書が出ているので(発展プロセス込みで)読んで学習することをお勧めする。

クラウドとのハイブリッドは、「今後当たり前になる」。

クラウドはデータが混在するのを嫌う傾向があるといわれている…。等々…。

如何だろうか…？ 纏めになっていないかも知れないが、この様に言えるのではないだろうか…？

「今すぐクラウドを活用する必要はないが、要素技術として、使えるものは直ぐに使った方がよい。」

以上

「クラウドコンピューティング」へのアプローチ

牧田一雄

1. はじめに

IT ガバナンス研究会の 2009 年度の研究テーマは「クラウドコンピューティング」であった。この数年「クラウドコンピューティング」という言葉を、インターネットや雑誌、会話の中で聴かない日は無い状況である。

現状の「クラウドコンピューティング」は、HW ベンダーや SW ベンダー、SIer、サービスプロバイダーが、自社の製品やサービス、能力に自分の都合の良いように「クラウドコンピューティング」という言葉を使い、ユーザーに対して優位な「イメージ」を作り上げ、IT 市場の大きなうねりに埋没しまいとしている。また、IT コーディネータを含めた IT コンサルタントは、「クラウドコンピューティング」の採用が、企業に差別化と競争優位をもたらす解決案であるかのようにクライアントに提言している。

「クラウドコンピューティング」を含めたこのような IT 状況の中で、IT コーディネータとしてクライアントをミスリードしないために、適切な ITC プロセスの運用が重要になると考えている。

本レポートでは、次の項目について検討を試みる。

- 「クラウドコンピューティング」という形容にについて、クライアント視点の定義
- 「クラウドコンピューティング」という形容に求められている IT ケーパビリティや要求事項。
- 「クラウドコンピューティング」という形容の EA への反映

本レポートは 1 年間の結果というよりは、「クラウドコンピューティング」の捉え方の今後の課題として整理として、IT コーディネータとして ITC プロセスの中で「クラウドコンピューティング」を適切に取り扱う筋道がたてられればと思う。

2. 「クラウドコンピューティング」の定義

クライアントが作成した「クラウドコンピューティング」についての一貫した定義は、「クラウドコンピューティング」計画を 2009 年に発表した米国連邦政府が、「クラウドコンピューティング」をサービスとして購入するための準備を米国連邦政府の一連の文書に記述されている。それらは IT コーディネータがクライアントの視点に立った「クラウドコンピューティング」を検討するために有効である。

「クラウドコンピューティング」の基本となる定義は、米国国立標準技術研究所 (National Institute of Standards and Technology, NIST) が作成した「The NIST Definition of Cloud Computing」という、MS ワードで 2 ページの短い文書である。NIST の使命は、「To promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.」である。

この文書の中で、「クラウドコンピューティング」は、

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of **five essential characteristics, three service models, and four deployment models.**

と定義されている。

定義の中の 5 つの重要な特性 (Five Essential Characteristics) は、

- **On-demand self-service.** A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service's provider.
- **Broad network access.** Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs).
- **Resource pooling.** The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.
- **Rapid elasticity.** Capabilities can be rapidly and elastically provisioned, in

some cases automatically, to quickly scale out and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.

- ***Measured Service.*** Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported providing transparency for both the provider and consumer of the utilized service.
- ***(Pay per use.)*** Capabilities are charged using a metered, fee-for-service, or advertising based billing model to promote optimization of resource use. Examples are measuring the storage, bandwidth, and computing resources consumed and charging for the number of active user accounts per month. Clouds within an organization accrue cost between business units and may or may not use actual currency.

である。

3つのサービスモデル (Three Service Models) は、

- ***Cloud Software as a Service (SaaS).*** The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.
- ***Cloud Platform as a Service (PaaS).*** The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.
- ***Cloud Infrastructure as a Service (IaaS).*** The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer

does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

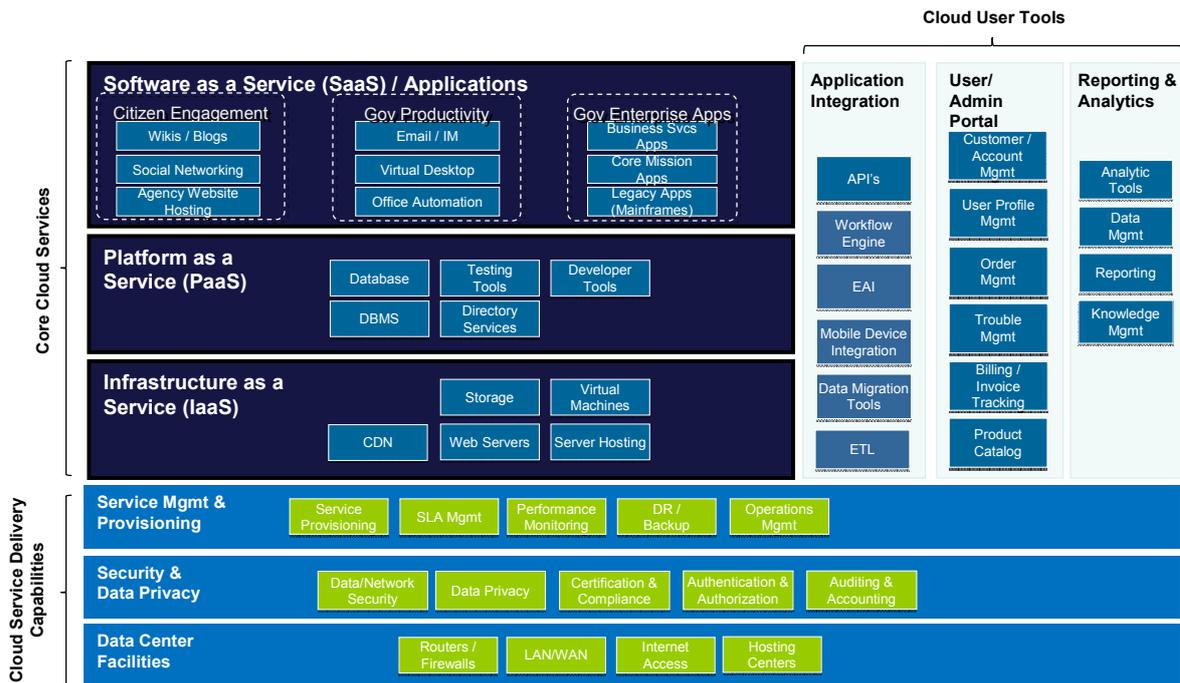
である。

4つのデプロイメントモデル (Four Deployment Models) は、

- **Private cloud.** The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.
- **Community cloud.** The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.
- **Public cloud.** The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.
- **Hybrid cloud.** The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds).

である。

この NIST の「クラウドコンピューティング」の基本的な定義に基づいて、連邦政府一般調達局 (General Services Administration, GSA) は、「Federal Cloud Computing Initiative Overview」の中で、次のように米国連邦政府が想定する「クラウドコンピューティング」全体のフレームワーク全体も表している。



また、「Federal Cloud Computing Initiative Overview」の中で、解決が期待される課題や期待される利益が記述されている。

解決が期待される課題（Cloud Computing Initiative）として、

- Continue the migration towards a services-based environment that is technology and vendor-agnostic
- Enable rapid deployment of technology solutions for the Federal government without developing stove-pipes
- Enable scalability for existing and new capabilities
- Increase savings through virtualization
- Potentially reduce cost of infrastructure, buildings, power, and staffing
- Improve the government's ability to create a transparent, open and participatory government

が挙げられている。また、利益（Benefits）として、

- Rapid provisioning and deployment of services
- On-demand scalability and elasticity for new services and capabilities
- Creation of a services-based environment that is interoperable and standards-based
- Opportunity for Cost Savings
 - ✓ Leverages economies of scale
 - ✓ Promotes innovation and service sharing

- ✓ Allows for “Measured” Payment (Pay per Use)
- Enables agencies to reinvest in, and concentrate on, core mission objective
が挙げられている。

3. 「クラウドコンピューティング」の RFI と RFQ

連邦政府一般調達局(General Services Administration, GSA)は、米国政府の各省庁が利用する Infrastructure as a Service(IaaS)を調達するための Request for Information (RFI) と Request for Quote(RFQ)を発行し、IaaS を提供しようとしているベンダーから回答を求めている。

RFI では、IaaS を提供するベンダーに対して、次の 5 つの大項目について質問をしている。

- **Please address the following Business Model, Pricing Model and Service Level Agreement (SLA) questions:**
 - ✓ What is the scope and nature of your IaaS offerings, including computing as-a-service, file storage as-a-service, and associated administration capabilities? Please identify and explain. Note that for the purposes of this RFI we are not focused on platform-as-a-service or application sandboxing for test purposes, though you may suggest synergy between your IaaS offerings and other offerings.
 - ✓ Describe in general terms your IaaS pricing model as it relates to CPU, memory, storage, bandwidth, data transfer capacity, and other relevant pricing.
 - ✓ Describe your capability to offer hosting services, including any capabilities for server provisioning, preconfigured system images and applications stacks, management, operating system patching, security software, and other managed services.
 - ✓ Describe the standard SLAs, if any, that are included in your cloud computing service offerings. Please detail SLAs on the overall service as well as SLAs for the specific customer instances in use, such as a given virtual server, storage volume, or other service unit.
 - ✓ Do you offer the flexibility of negotiated customer-specific SLAs or only fixed offerings?
 - ✓ Please provide past performance information, to include recent and relevant contracts for the same or similar items and other references (including contract numbers, points of contact with telephone numbers and other relevant information).
- **Please address the following Business Model, Pricing Model and Service Level Agreement (SLA) questions:**
 - ✓ What is the scope and nature of your IaaS offerings, including computing as-a-service, file storage as-a-service, and associated administration

capabilities? Please identify and explain. Note that for the purposes of this RFI we are not focused on platform-as-a-service or application sandboxing for test purposes, though you may suggest synergy between your IaaS offerings and other offerings.

- ✓ Describe in general terms your IaaS pricing model as it relates to CPU, memory, storage, bandwidth, data transfer capacity, and other relevant pricing.
- ✓ Describe your capability to offer hosting services, including any capabilities for server provisioning, preconfigured system images and applications stacks, management, operating system patching, security software, and other managed services.
- ✓ Describe the standard SLAs, if any, that are included in your cloud computing service offerings. Please detail SLAs on the overall service as well as SLAs for the specific customer instances in use, such as a given virtual server, storage volume, or other service unit.
- ✓ Do you offer the flexibility of negotiated customer-specific SLAs or only fixed offerings?
- ✓ Please provide past performance information, to include recent and relevant contracts for the same or similar items and other references (including contract numbers, points of contact with telephone numbers and other relevant information).
- **Please address the following Operational Support questions:**
 - ✓ Describe the core components of ensuring availability from your perspective (e.g. # of locations, # of locations at Internet Exchange Points (IXP)?
 - ✓ Are you Border Gateway Protocol (BGP) Peered?
 - ✓ Is your network dual homed? If so, with whom?
 - ✓ How are you able to prioritize our traffic if need be?
 - ✓ Do you maintain any industry certification standards such as ITIL, ISO 20,000, and/or CMMI?
 - ✓ How do you maintain effective levels of patch management on the Operating Systems, VMs and/or hypervisors in an open virtualization environment?
 - ✓ Describe your handling of potential availability issues such as significant cloud computing outage, high network load or insufficient bandwidth access. What is your mitigation strategy in case of potential network

outages, bandwidth shortages, or spikes in service demand?

- ✓ What types and combinations of CPU processors, virtualization formats, and operating systems are supported by your service? In addition, what capabilities are there for testing various combinations of these?
- ✓ What kind of trouble ticketing system do you have, and is it visible from our site?
- ✓ What level of automatic alerting can you provide to our support staff in the event of failure, degraded service, or exceeded planned utilization?
- ✓ Please describe your system for IP address assignment and persistence in a virtual environment.
- ✓ Please identify which ports are allowed or accessible through your infrastructure (i.e. 25, 80, 139, and 443) and which we might assume would be blocked. Are any unique ports or API calls required?
- ✓ Describe your IP Management in a virtual environment. Can you provide renewal capabilities, including level of support for static IP addressing?
- ✓ Describe how you manage domain controllers in a Demilitarized Zone (DMZ).
- ✓ Describe how you manage remote administration for provisioning and Virtual Machine (VM) access.
- **Please address the following Data Management questions:**
 - ✓ Describe your handling of data isolation, data recovery and handling/security of data at rest and in transit.
 - ✓ Can you guarantee that data will remain within the continental United States, both in transit and at rest? If so, how?
 - ✓ Describe your roles and responsibilities regarding data ownership, e.g. logging data.
 - ✓ Describe your method for getting customer's data back in-house either on demand or in case of contract termination for any reason.
 - ✓ How would you handle data remnants throughout their service lifecycle?
 - ✓ Who owns the Intellectual Property for artifacts developed in or hosted in your cloud?
- **Please address the following Security questions:**
 - ✓ Describe your security architecture around the cloud services that you provide, including Open Systems Interoperability layers 1-4. Please provide an overview of your methods to limit data dispersal to unauthorized entities.

- ✓ Please explain how you provide physical security in a shared tenant environment.
- ✓ Describe your approach to addressing IT security challenges in cloud computing, in particular - dealing with hacker attacks, the potential for unauthorized access, and inappropriate use of proprietary data and IT applications. What are your processes and solutions for preventing these challenges from occurring?
- ✓ Describe the cloud computing authentication models that you think would be most effective for Government administrative use. Describe how your service offering could enable eDiscovery, forensic analysis, auditability, and other similar governance requirements.
- ✓ Detail your support for Security Assertion Markup Language (SAML) services.
- ✓ What approaches for encryption key management do you support? Describe how you manage them.
- ✓ List and describe any NIST 800-53 rev 3 (FISMA) controls that may be challenging to achieve within your IaaS services provided in a cloud environment. What other certifications and compliance standards do you support, have third party certification for, or comply with, such as HIPAA, PCI, and SAS 70?
- ✓ To what extent have you implemented [DNSSEC](#)?
<http://csrc.nist.gov/publications/nistpubs/800-81/SP800-81.pdf>
- ✓ What is your level of support for full IPv6 capabilities, especially in the network, in Domain Name System (DNS), storage, and any operating systems that you provide? Please detail any capabilities that are not fully IPv6 compliant.
- ✓ What kind of intrusion detection and intrusion prevention systems do you use, and are your customers provided access to these?
- ✓ Identify what parts of your infrastructure are FIPS 140-2 compliant.
- ✓ What controls are in place for administrative access, both internal to your company and for administrative access from government clients? Please include discussion of administrator controls over provisioning.
- ✓ Describe how [penetration testing](#) and [source code analysis](#) is performed in a cloud environment.
- **Please address the following Interoperability and Portability questions:**
 - ✓ Describe your recommendations regarding “cloud-to-cloud” communication

and ensuring interoperability of cloud solutions.

- ✓ Describe your experience in weaving together multiple different cloud computing services offered by you, if any, or by other vendors.
- ✓ As part of your service offering, describe the tools you support for integrating with other vendors in terms of monitoring and managing multiple cloud computing services.
- ✓ Please explain application portability; i.e. exit strategy for applications running in your cloud, should it be necessary to vacate.
- ✓ Describe how you prevent vendor lock in.

RFQ の Attachment C: Statement of Work で次の要求事項 (Requirements) を提示している。

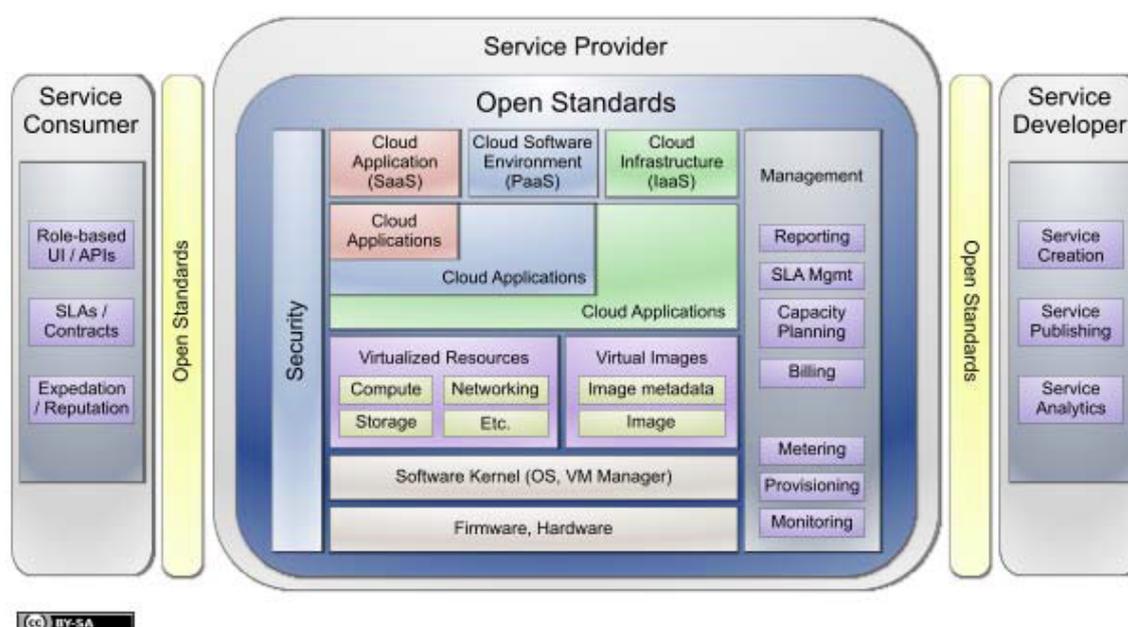
- General Cloud Computing Requirements
 - ✓ On-demand self-service
 - ✓ Ubiquitous network access
 - ✓ Location independent resource pooling
 - ✓ Rapid elasticity
 - ✓ Measured Service
- IaaS Common Technical Requirements
 - ✓ Service Management and Provisioning Requirements
 - Service Provisioning
 - Service Level Agreement Management
 - Operational Management
 - Disaster Recovery and Continuity of Operations
 - Data management
 - ✓ User/Admin Portal Requirements
 - Order Management
 - Billing/Invoice Tracking
 - Utilization Monitoring
 - Trouble Management
 - User Profile Management
 - ✓ Integration Requirements
 - Application Programming Interfaces
 - ✓ Data Center Facilities Requirements
 - Internet Access
 - LAN/WAN
 - Data Center Facilities

- Lot Specific Technical Requirements and Past Performance
 - ✓ LOT 1: CLOUD STORAGE SERVICES
 - Cloud Storage Service Requirements
 - Storage and Bandwidth Tiers
 - ✓ LOT 2: VIRTUAL MACHINE
 - Virtual Machine Requirements
 - Bundling of Virtual Machine Service Attributes
 - Virtual Machine Technical Requirements
 - ✓ LOT 3: CLOUD WEB HOSTING
 - Cloud Web hosting requirements
 - Bundling of Cloud Web Hosting Service Attributes
- Compliance Requirements
 - ✓ Section 508
 - ✓ Information Technology Systems Security Requirements
 - ✓ Security Clearance Requirements
 - ✓ Privacy Requirements

4. 「クラウドコンピューティング」と利用シナリオ

Cloud Computing Use Case Discussion Group は、「Cloud Computing Use Cases White Paper」を作成して、クラウド利用者とクラウドベンダーに対して共通の利用ケース・シナリオを提供している。「Cloud Computing Use Cases White Paper」も先に紹介した NIST のクラウドコンピューティングの定義を基本としている。また、Cloud Computing Use Case Discussion Group の活動は、「Open Cloud Manifesto」の Open Cloud の6つの基本方針に基づいている。

「Cloud Computing Use Cases White Paper」の中で、次のようなクラウドコンピューティングのフレームワークを提示している。



「Cloud Computing Use Cases White Paper」は、このフレームワークに基づいて、必要な標準規格や APIs が何かを説明している。標準規格の種類は、

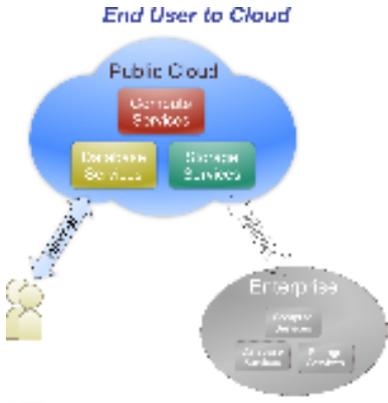
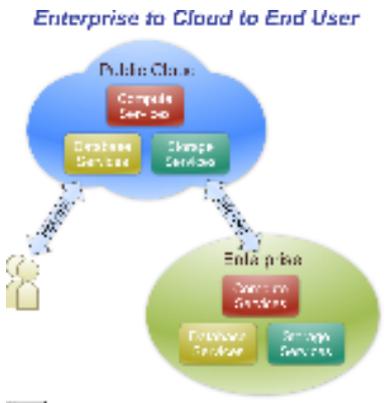
- Standards Across Cloud Service Types
- Standards Within Cloud service Types
- Standards Between the Cloud and the Enterprise
- Standards Within an Enterprise

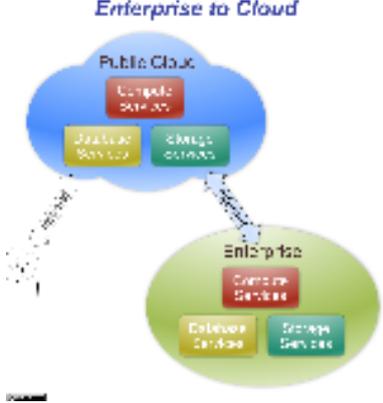
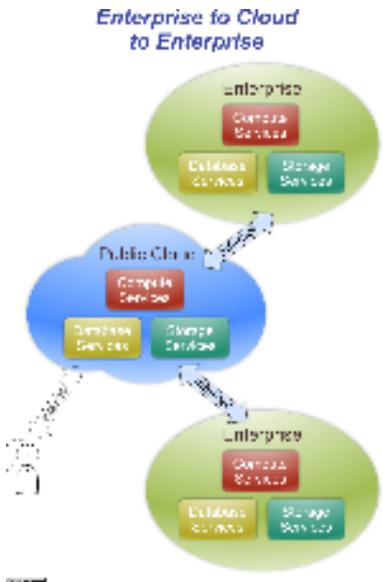
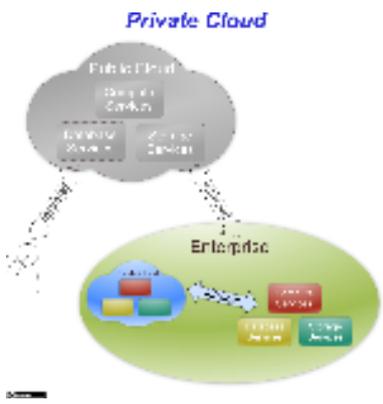
であり、APIs は、

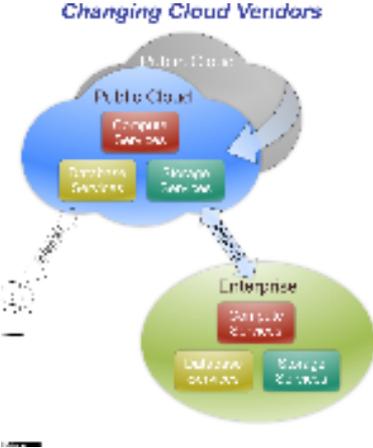
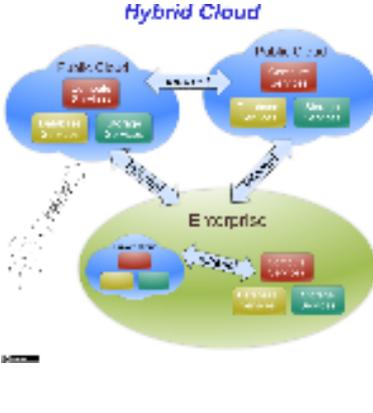
- Levels of APIs The Wire/Language-Specific Toolkits/Service-specific Toolkits/service-Neutral Toolkits
- Categories of APIs Ordinary Programming/Deployment/Cloud Services/Image and Infrastructure Management/Internal Interfaces

である。これらを踏まえて、想定される利用ケース・シナリオを挙げて、さらに要求事項

との関係を洗い出している。

<p>End User to Cloud</p>	<p>In this scenario, an end user is accessing data or applications in the cloud. Common applications of this type include email hosting and social networking sites. A user of Gmail, Facebook or LinkedIn accesses the application and their data through any browser on any device. The user doesn't want to keep up with anything more than a password; their data is stored and managed in the cloud.</p>	 <p>The diagram illustrates the 'End User to Cloud' scenario. On the left, a user icon is connected to a blue cloud labeled 'Public Cloud'. Inside the cloud are three boxes: 'Compute Services' (red), 'Database Services' (yellow), and 'Storage Services' (green). On the right, a grey oval labeled 'Enterprise' contains three boxes: 'Compute Services' (red), 'Database Services' (yellow), and 'Storage Services' (green). Dotted lines connect the user to the cloud and the cloud to the enterprise.</p>
<p>Enterprise to Cloud to End User</p>	<p>In this scenario, an enterprise is using the cloud to deliver data and services to the end user. When the end user interacts with the enterprise, the enterprise accesses the cloud to retrieve data and / or manipulate it, sending the results to the end user. The end user can be someone within the enterprise or an external customer.</p>	 <p>The diagram illustrates the 'Enterprise to Cloud to End User' scenario. On the left, a user icon is connected to a blue cloud labeled 'Public Cloud'. Inside the cloud are three boxes: 'Compute Services' (red), 'Database Services' (yellow), and 'Storage Services' (green). On the right, a green oval labeled 'Enterprise' contains three boxes: 'Compute Services' (red), 'Database Services' (yellow), and 'Storage Services' (green). Dotted lines connect the user to the cloud and the cloud to the enterprise.</p>

<p>Enterprise to Cloud</p>	<p>This use case involves an enterprise using cloud services for its internal processes. This might be the most common use case in the early stages of cloud computing because it gives the enterprise the most control.</p>	 <p>The diagram, titled "Enterprise to Cloud", illustrates an enterprise (green oval) with Compute, Database, and Storage services connected to a Public Cloud (blue cloud) that also provides Compute, Database, and Storage services. Dotted lines indicate the flow of data and services between the enterprise and the cloud.</p>
<p>Enterprise to Cloud to Enterprise</p>	<p>This use case involves two enterprises using the same cloud. The focus here is hosting resources in the cloud so that applications from the enterprises can interoperate. A supply chain is the most obvious example for this use case.</p>	 <p>The diagram, titled "Enterprise to Cloud to Enterprise", shows two separate enterprises (green ovals) at the top and bottom, each with Compute, Database, and Storage services. Both are connected to a central Public Cloud (blue cloud) that also provides Compute, Database, and Storage services. Dotted lines show the interaction between the enterprises and the cloud.</p>
<p>Private Cloud</p>	<p>The Private Cloud use case is different from the others in that the cloud is contained within the enterprise. This is useful for larger enterprises.</p>	 <p>The diagram, titled "Private Cloud", depicts a Public/Private Cloud (grey cloud) with Compute, Database, and Storage services. This cloud is connected to an Enterprise (green oval) that also has Compute, Database, and Storage services. Dotted lines indicate the connection between the cloud and the enterprise.</p>

Changing Cloud Vendors	This use case involves multiple clouds working together, including both public and private clouds. A hybrid cloud can be delivered by a federated cloud provider that combines its own resources with those of other providers.	
Hybrid Cloud	This use case involves multiple clouds working together, including both public and private clouds. A hybrid cloud can be delivered by a federated cloud provider that combines its own resources with those of other providers.	

Requirement	End User to Cloud	Enterprise to Cloud to	Enterprise to Cloud	Enterprise to Cloud to	Private Cloud	Changing Cloud	Hybrid Cloud
Identity	✓	✓		✓			✓
Open Client	✓	✓	✓	✓	✓	✓	✓
Federated Identity		✓	✓	✓			✓
Location Awareness		✓	✓	✓		✓	✓
Metering and Monitoring		✓	✓	✓	✓		✓
Management and Governance		✓	✓	✓	✓		✓
Security	✓	✓	✓	✓	✓	✓	✓

Deployment			✓		✓		✓
Transactions and Concurrency				✓			
Interoperability				✓			✓
Industry-Specific Standards			✓	✓			✓
VM Image Format		✓	✓	✓	✓	✓	✓
Cloud Storage API		✓	✓	✓		✓	✓
Cloud Database API		✓	✓	✓		✓	✓
Cloud Middleware API		✓	✓	✓		✓	✓
Data and Application Federation		✓	✓	✓			✓
SLAs	✓	✓	✓	✓	✓	✓	✓
Lifecycle Management		✓	✓	✓			✓

5. 「クラウドコンピューティング」と脅威

Cloud Security Alliance (CSA) はクラウドコンピューティングに内在する脅威に着目して、「Top Threats to Cloud Computing」と「Security Guidance for Critical Areas of Focus Cloud Computing」というガイドラインを作成している。

「Top Threats to Cloud Computing」は、「Security Guidance for Critical Areas of Focus Cloud Computing」の手引きのような位置づけで、想定される脅威について、説明、例、対処、参照、影響、および、サービスモデルが記述されている。さらに「Security Guidance for Critical Areas of Focus Cloud Computing」で解説している各領域が参照できるようにポイントされている。「Top Threats to Cloud Computing」の中で挙げられているのは、次の7つの脅威である。

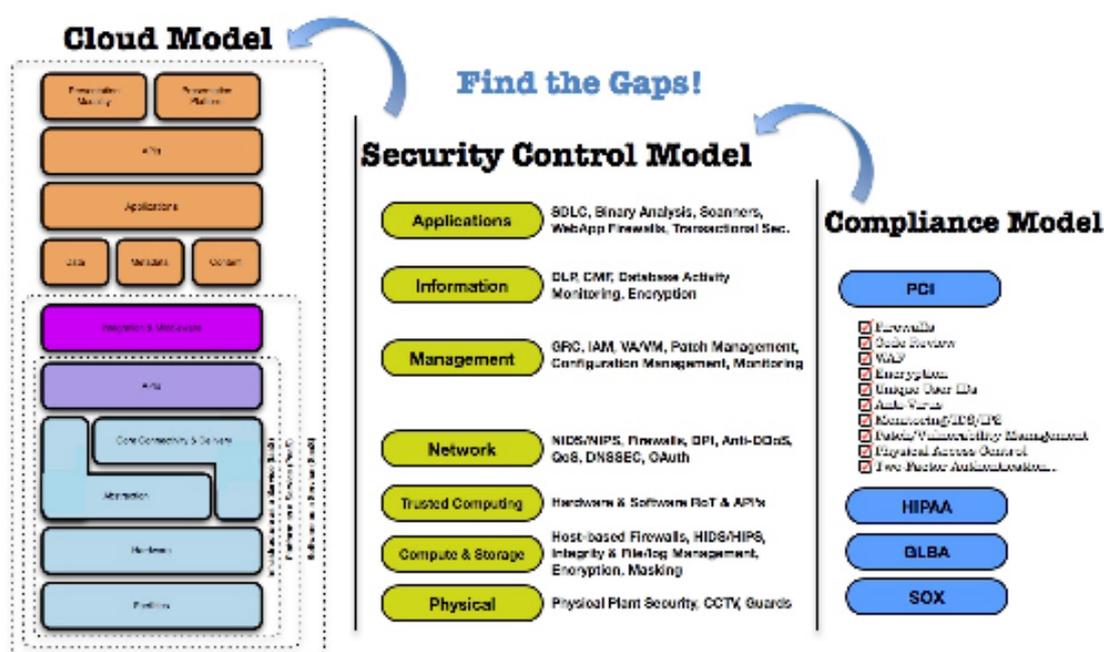
- Threat 1 : Abuse and Nefarious Use of Cloud Computing
- Threat 2 : Insecure Application Programming Interfaces
- Threat 3 : Malicious Insiders
- Threat 4 : Shared Technology Vulnerabilities
- Threat 5 : Data Loss/Leakage
- Threat 6 : Account, Service & Traffic Hijacking
- Threat 7 : Unknown Risk Profile

「Security Guidance for Critical Areas of Focus Cloud Computing」の中で解説されている領域は、次の13の領域(Domain)である。

- Section I. Cloud Architecture
 - ✓ Domain 1: Cloud Computing Architectural Framework
- Section II. Governing in the Cloud
 - ✓ Domain 2: Governance and Enterprise Risk Management
 - ✓ Domain 3: Legal and Electronic Discovery
 - ✓ Domain 4: Compliance and Audit
 - ✓ Domain 5: Information Lifecycle Management
 - ✓ Domain 6: Portability and Interoperability
- Section III. Operating in the Cloud
 - ✓ Domain 7: Traditional Security, Business Continuity, and Disaster Recovery
 - ✓ Domain 8: Data Center Operations
 - ✓ Domain 9: Incident Response, Notification, and Remediation
 - ✓ Domain 10: Application Security
 - ✓ Domain 11: Encryption and Key Management
 - ✓ Domain 12: Identity and Access Management
 - ✓ Domain 13: Virtualization

「Domain 1: Cloud Computing Architectural Framework」で「Security Guidance for Critical Areas of Focus Cloud Computing」におけるクラウドコンピューティングの基本概念を説明しているが、前に紹介した NIST の「クラウドコンピューティング」の定義に整合性がとられている。

「Security Guidance for Critical Areas of Focus Cloud Computing」のフレームワークの特徴は、クラウドモデルをコンプライアンスモデルおよびセキュリティ統制モデルと対応させている点が特徴的である。



Domain2 以降の領域の内容は次のとおりである。

Domain 2: Governance and Enterprise Risk Management: The ability of an organization to govern and measure enterprise risk introduced by Cloud Computing. Items such as legal precedence for agreement breaches, ability of user organizations to adequately assess risk of a cloud provider, responsibility to protect sensitive data when both user and provider may be at fault, and how international boundaries may affect these issues, are some of the items discussed.

Domain 3: Legal and Electronic Discovery: Potential legal issues when using Cloud Computing. Issues touched on in this section include protection requirements for information and computer systems, security breach disclosure laws, regulatory

requirements, privacy requirements, international laws, etc.

Domain 4: Compliance and Audit: Maintaining and proving compliance when using Cloud Computing. Issues dealing with evaluating how Cloud Computing affects compliance with internal security policies, as well as various compliance requirements (regulatory, legislative, and otherwise) are discussed here. This domain includes some direction on proving compliance during an audit.

Domain 5: Information Lifecycle Management: Managing data that is placed in the cloud. Items surrounding the identification and control of data in the cloud, as well as compensating controls which can be used to deal with the loss of physical control when moving data to the cloud, are discussed here. Other items, such as who is responsible for data confidentiality, integrity, and availability are mentioned.

Domain 6: Portability and Interoperability: The ability to move data/services from one provider to another, or bring it entirely back in-house. Issues surrounding interoperability between providers are also discussed.

Domain 7: Traditional Security, Business Continuity, and Disaster Recovery: How Cloud Computing affects the operational processes and procedures currently use to implement security, business continuity, and disaster recovery. The focus is to discuss and examine possible risks of Cloud Computing, in hopes of increasing dialogue and debate on the overwhelming demand for better enterprise risk management models. Further, the section touches on helping people to identify where Cloud Computing may assist in diminishing certain security risks, or entails increases in other areas.

Domain 8: Data Center Operations: How to evaluate a provider's data center architecture and operations. This is primarily focused on helping users identify common data center characteristics that could be detrimental to on-going services, as well as characteristics

Domain 9: Incident Response, Notification, and Remediation: Proper and adequate incident detection, response, notification, and remediation. This attempts to address items that should be in place at both provider and user levels to enable proper incident handling and forensics. This domain will help you understand the complexities the cloud brings to your current incident handling program.

Domain 10: Application Security: Securing application software that is running on or being developed in the cloud. This includes items such as whether it's appropriate to migrate or design an application to run in the cloud, and if so, what type of cloud platform is most appropriate (SaaS, PaaS, or IaaS). Some

specific security issues related to the cloud are also discussed.

Domain 11: Encryption and Key Management: Identifying proper encryption usage and scalable key management. This section is not prescriptive, but is more informational in discussing why they are needed and identifying issues that arise in use, both for protecting access to resources as well as for protecting data.

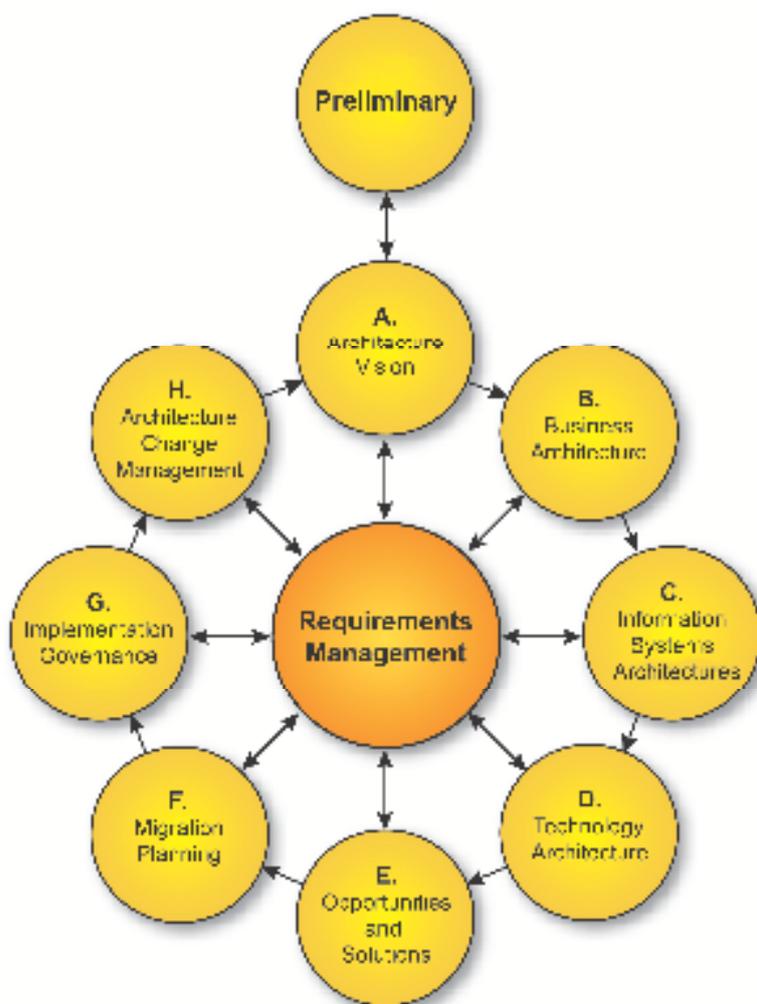
Domain 12: Identity and Access Management: Managing identities and leveraging directory services to provide access control. The focus is on issues encountered when extending an organization's identity into the cloud. This section provides insight into assessing an organization's readiness to conduct cloud-based Identity and Access Management (IAM).

Domain 13: Virtualization: The use of virtualization technology in Cloud Computing. The domain addresses items such as risks associated with multi-tenancy, VM isolation, VM co-residence, hypervisor vulnerabilities, etc. This domain focuses on the security issues surrounding system/hardware virtualization, rather than a more general survey of all forms of virtualization.

6. クラウドコンピューティングと EA

IT ガバナンスを企業全体に有効に働かす方法としてエンタープライズ・アーキテクチャ (Enterprise Architecture, EA) が有効である。EA は、企業のビジネス戦略とそれを支援する IT 戦略の整合性を、企業全体の観点から維持し、それに基づき IT 計画の立案し、IT 構築して、「As Is」から「To Be Model」への移行を実現するため仕組みである。

EA はビジネス層 (Business Architecture, BA)、情報システム層 (Information Systems Architecture, IA) (データ層 (Data Architecture, DA) とアプリケーション層 (Application Architecture, AA) が含まれる) およびテクノロジー層 (Technology Architecture, TA) の階層のトップダウン・アプローチと、それを維持するプロセス、および導入計画の策定から構成される。次の図は、オープングループの EA フレームワーク (The Open Group Architecture Framework, TOGAF) のサイクルである。



EA の各階層は、全体最適を図るためビジネスの観点から俯瞰される。従って、ビジネス戦略上の要求は BA にマッピングされ、DA、AA、TA の各階層に展開され反映される。こ

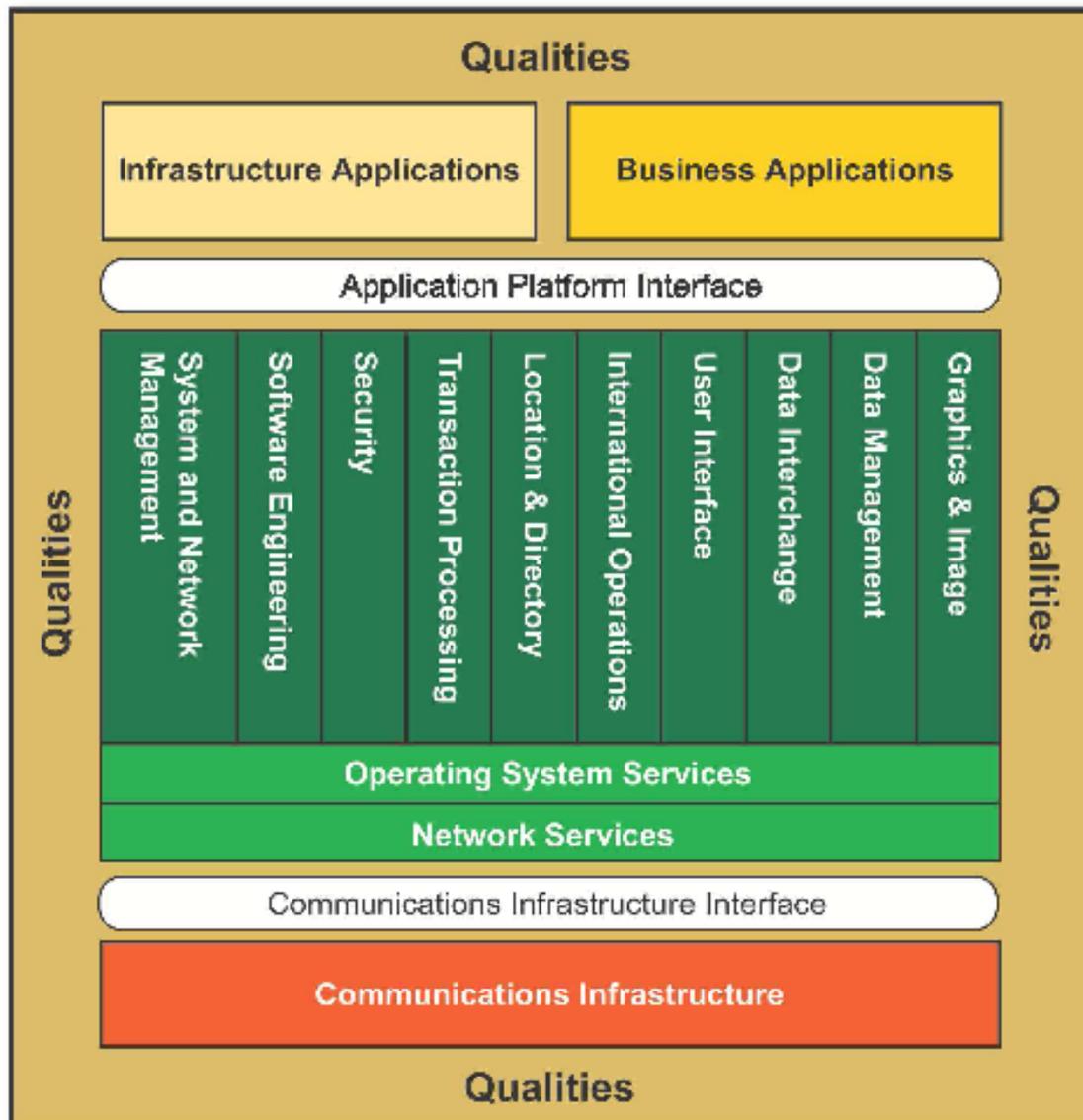
のようにトップダウンのプロセスの中で、切り出された個別の IT 構築プロジェクトは、全体との整合性を維持することが可能になる。市場投入までの時間や投資対効果が優先事項となるため、部分最適になる可能性が高い状況において、EA は部分最適に陥るリスクを最小化し、ソリューションとして「クラウドコンピューティング」の全体最適を担保するために重要であることがわかる。

そのためには、2 つの整備が重要だと考える。「クラウドコンピューティング」を想定にいた「非機能要件とサービスレベル」と「技術参照モデル」である。

「非機能要件とサービスレベル」は、BA から TA への要求の展開の中で非機能要件とサービスレベルなどについて、「クラウドコンピューティング」の選択肢も念頭においてものでなければならない。どのような非機能要件やサービスレベルが「クラウドコンピューティング」を含めて適正な指標になる可能性あるかは、前に紹介した「Cloud Computing Use Cases White Paper」や「Security Guidance for Critical Areas of Focus Cloud Computing」などのようなガイドが参考に、今後検討が必要である。

「技術参照モデル(Technical Reference Model, TRM)」は、技術革新も激しい環境において、自社の情報システムの構築や運用において、拡張容易性および可搬性、相互運用性を維持するために、EA の効果を上げるボトムアップのアプローチと重要になる。

TOGAF で定義されている TRM のカテゴリーは次の図のとおりである。



TRM 本体として入手しやすいものは、経済産業省で作成している「情報システム調達のための技術参照モデル(TRM)」である。自社の TRM は、TOGAF や経済産業省を参考に、現在導入済みのシステムの技術を基に作成を始め、必要となる可能性が高い技術を追加し、最終的に網羅性を高めて完成させると良いだろう。TRM の詳細度としても、技術標準および標準規格のレベルにとどめ、必要な場合については標準製品および推奨製品まで規定するとよいだろう。情報システムが対応できず陳腐化することを回避できる内容が必要であり、「オープンアーキテクチャ」および「仮想化」、「オートノミック」、「グリッド」などの基本技術の観点からのテクノロジースキャンを行い、他の TRM を参照しながら、自社の TRM の維持が重要である。

7. おわりに

氾濫する「クラウドコンピューティング」に惑わされないで、経営戦略を的確に支援する IT システムを ITC プロセスから乖離することなく、ITC として提言するためのアプローチを検討した。

今回の検討は ITC プロセスの「IT 戦略策定フェーズ」および「IT 資源調達フェーズ」のそれぞれの一部分に過ぎない。「クラウドコンピューティング」はパラダイムシフトといわれているが、ITC が経営戦略を的確に支援する IT システムを提言することは、IT システムにこのような改革を要求するビジネス環境についての議論なく進めることはできない。

現実的なクラウド適用の考え方

日立ビジネス 山上

ITガバナンス研究会として2009年度のテーマを「クラウド」に設定し、全般的な調査・検討から得られた各種の知見をまとめ・発信していく。発信により企業・団体の経営に「クラウド」をいかに取り入れていくべきか、そのアドバイスをしていくべきITCへの幾らかの示唆を提供することが本資料の目的である。

1. クラウドの定義（ASP、SaaS、PaaS、HaaS、IaaS、XaaS・・・）

20世紀末のASPに端を発し、現在のクラウドと称される各種のXaaSにより情報システム・情報機器のサービスとしての活用形態が確立されるという一連の流れをクラウドとして捉えたい。その活用形態がそれぞれ業務システム（SaaS）、プラットフォーム（PaaS）、ハードウェア（HaaS）、インフラ（IaaS）・・・と区分されているが、いずれにしても従来の所有による情報システムの利活用から、サービス利用による情報システムの利活用という新たな選択肢が豊富に準備されてきていることは良いことだと考える。

2. 選択の基準は戦略次第

それでは各企業・団体はどのサービス形態を「活用していくか」、「活用していくべきか」は企業・団体の経営方針・経営戦略に大きく依存するものと考えられる。経営戦略に基づく事業戦略、営業・販売戦略、財務・会計戦略、人材採用・育成戦略およびそれらを支えるIT戦略をどう定義・推進していくかによる。

3. クラウド適用によるIT利活用

従来のように大規模な初期投資をできる企業・団体のみが情報システムの恩恵を享受できる環境から、格安に月々の費用で情報システムが利用でき、初期投資体力がない企業・団体においても情報システムの恩恵を享受できる環境が整ってきている。

一方でサービスの提供・利用という名前のおり既定・既製のものを適切に利用し、サービスを自社・自団体の業務にあわせるのではなく、自社・自団体の業務を改善・改革し提供されているサービスに寄せていくという導入推進がなされているのだと推察する。

この手法は所謂「ERP」導入による業務改革・ベストプラクティスという過去の経験と限りなく類似しているものである。この経験に則り、FIT&GAP分析に基づくアプローチに長けている企業・団体がクラウド導入を成功させることができるであろう。この

手法では「ERP」が提供しているコア部分にどれだけ自社・自団体の業務を寄せ、コア部分で賄いきれない部分を外付けによる機能追加または「ERP」のコア部分に手を入れるということになる。この手法でGAPを解決した場合には製品のバージョンアップ時に互換性・移行性をいかにして確保するかということで大いに悩んできているが、現行のクラウドでは改善がなされているようである。外付けインターフェースおよびその互換性・移行性されており、また、その開発手法・開発言語等が予め準備・設定されている。さすがに内部のコア部分に手を入れていくということは過去の反省に基づき、なされないようになってきているようである。

4. 重視すべきは自社・自団体の強み

企業・団体の経営において独自の強み・特徴はその業務プロセスに織り込まれ、従事する人そのものに織り込まれていることが多い。従って、それをどこまでクラウドによって解決できるかが課題である。

一方、クラウドで強みが解決・維持できるということは、既定・既製のサービスに独自の強みが準備されていることと同義であり、他社・他団体がもしもその気になればまったく同様な強みを情報システムでしかも既定・既製のものとして利活用できることにいうことを意味する。

5. 強みを意識するほどにクラウドから離れていく

一般的な物言いになるが汎用的で自社・自団体の独自の強みに依存しない部分はASP、SaaSを導入し、強みに依存する部分が多くなればなるほどにSaaSに付帯するPaaSに外付け部分を作り込んでいくこととなる。さらに強みの部分の独自色が濃いほどに作り込みの部分が多くなっていくと想定する。さらに独自の作り込みが強化されるとPaaSで提供するミドルウェアで吸収できないケースが発生し、HaaS/IaaSにより提供されるハードウェア/インフラのうえにミドルウェアを含むアプリケーションを独自に準備することが想定できる。

これらのことから考えると強みを意識するほどにクラウドの既定・既設サービスで実現できることが離れていくと結論付けられる。

6. クラウド提供ベンダ選定の考え方

これらのことから考えてクラウドベンダはよりハードウェアに近い下層部分のうえに業務系をのせていくことが可能な総合ベンダまたは各層を個別に提供するベンダの連合軍的に束ねる企業群を選定することが利用者側の長期的な視野に立て有効といえる。

前述の通り、利用する企業・団体は独自の強みを中心に考えてクラウドベンダを選定していくことが重要といえるので、企業・団体は独自色の薄い部分から始めて段階的に独自色が濃い部分のクラウド適用を検討していくべきである。当然であるが独自色が濃い部分でかつ同業者の追随を許さないものは作りこみ強化により維持していく必要がある。「所有から利用」、「持たざる経営」と宣伝文句は大きいですが全てを持たないということには成り得ないことを十分に理解しておく必要がある。

究極的には従来型の自社・自前の部分を捨て去ることはありえず、プライベートクラウドまたはオンプレミスの形で生き残ることになるであろうし、それを捨て去ることができない企業・団体はそもそも存在意義が非常に弱いものになると言えるのではないだろうか？

7. 現実的なクラウド適用

現在は猫も杓子もクラウド！という狂乱の時代であり、既存ITベンダ（パッケージベンダ、S Iベンダ）のクラウド準備・進出が盛んに行われている。また、経産省推進のJ-SaaSも伸張中であり、今後もアプリケーション部分は百花繚乱の状況がしばらく続き、沈静化するのはいずれ先になるであろう。そのような状況の中で各企業・団体はどのようにクラウド導入を進めれば良いだろうか？

繰り返しになるが、独自の強みを中心にクラウドベンダを選定すれば良いのである。しかし、強みにあわせたものが特定ベンダで集中的に適用できることは少なく、どうしても個別の作り込みは抑えられない。各ベンダが提供しているクラウドのいいところ取りをしていくのが現実的なクラウド適用といえるのではないか？

いいところ取りを進める為にはアプリケーション間、ベンダ間、自社・自団体をつなぐデータの橋渡しが課題である。データ渡しをバッチ型のファイル転送式にするのか？ オンライントランザクショナルに1件渡しのメッセージ式にするのか？ Webサービス型にするのか等・・・議論はあると思う。

いずれにしてもクラウドベンダによるフルラインナップまでに期間がかかる現実、および特定のクラウドベンダによる囲い込み阻止の観点から考えてデータ連携の問題・課題は避けて通れないと考える。現段階では業種・業界横断的なデータ渡し的手段・手法は確立・普及しておらず（業界標準制定の機運・実績はあるものの、その統一運用が図られていない現実）、その実現には時間がかかる（永遠に実現しない？）と想定される。

各社・各団体ではデータ渡しの実現手法を十分に検討しつつ、クラウドベンダのいいところ取りを模索する期間が当分続きそうである。

—以上—

クラウド時代に求められるネットワークについて

山崎 直和

1. はじめに

仮想化や分散処理等を中核としたクラウド技術が注目を集めている。総務省や経済産業省をはじめとする政府においてもクラウド技術に関する調査や研究が活発に推進されており、まさにクラウド時代の到来と言える。

このような状況を踏まえ、このレポートにおいては「クラウド時代に求められるネットワークについて」と題して、主に今新たに求められるネットワークとはどのようなものか等に焦点を絞って考察することとしたい。

2. クラウド全体概況

まずは、クラウドの全体概況について再確認の意味を含めて考察する。

(1) クラウド技術を使う目的

技術の有効活用により、柔軟かつ迅速なシステム構築、システム運用コストの削減、環境負荷の低減等が見込まれる。

(2) 課題

主な課題としては以下のとおり。これらの課題を解決するためには、雲の上（サービス）だけで考えてもダメで、雲の中（プラットフォームやネットワーク）まで含めて考える必要がある。

- システムの信頼性・稼働率
- 安全性（情報セキュリティ・情報の所在）
- 既存システムとの連携 →マイグレーションが鍵！
- 既存ネットワーク環境の活用 →マイグレーションが鍵！
- トータルでの品質確保

3. クラウドの進化

クラウドは単一のクラウド（シングルクラウド）の時代から、プライベートクラウドとパブリッククラウドの連携（ハイブリッドクラウド）の時代、グローバルなクラウド間相互接続（インタークラウド）の時代へ進化しつつある。

- ・ 2010年～ シングルクラウド時代
- ・ 2012年～ ハイブリッドクラウド時代
- ・ 2014年以降？ インタークラウド時代

4. クラウドとネットワークの融合

このような状況の中、クラウドとネットワークの融合がさらに今後進んでいくと予想される。特に、ネットワークについては、現在キャリア各社が積極的に推進している NGN をさらに高機能化したネットワーク（新世代ネットワーク（NWGN）？）が登場するのでは、との噂も耳にする。この場合の想定される機能は次のとおり。

- ・ ダイナミックネットワーク機能
→アプリケーションに連動し、動的にトラフィックや経路を制御する機能
- ・ 仮想化機能
→アプリケーションからの要求事項に対して、帯域、遅延等を自動的に設計し、最適な仮想ネットワークを設計する機能

5. ネットワークに求められるもの

クラウド時代に求められるネットワーク要件としては、一般的に以下の3つに大別して考えることができると言われている。

① ネットワークの高速化

→大幅なトラフィック増が見込められるため、ネットワークの更なる高速化は必須である。

② セキュリティの確保

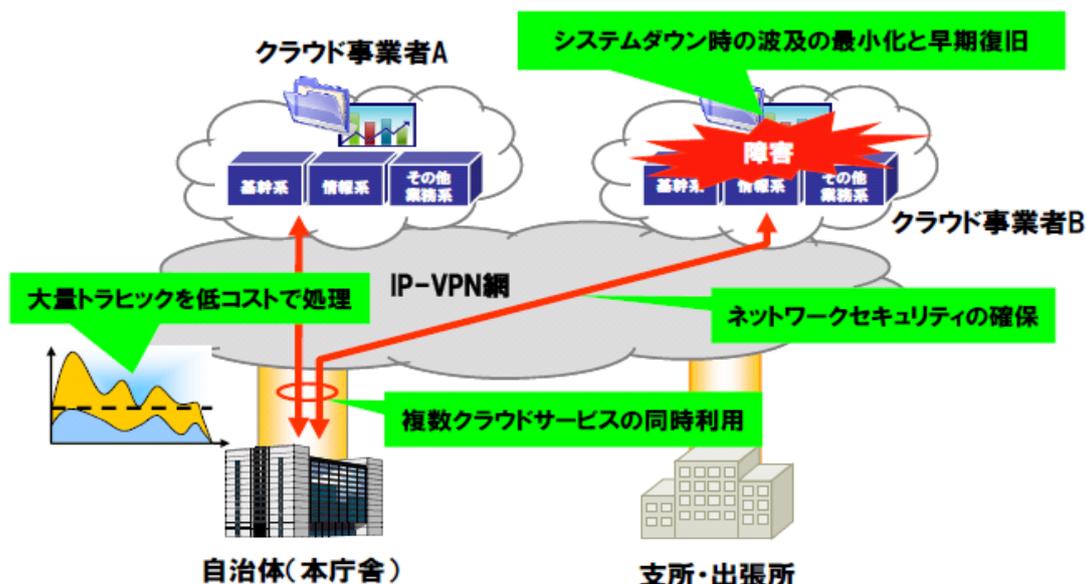
→ネットワークを流れる情報が今まで以上に多様化することが予想される。そのためシステム全体としてのセキュリティの確保は必須である。

③ 信頼性の確保

→今まで以上にネットワーク障害等が発生した場合の業務に与える影響が大きくなると予想される。そのためシステム全体としての信頼性の確保は必須である。

以上のように、クラウドに対応するためには当然のことながら今まで以上の要件がネットワークに求められるが、クラウドを推進する上での大きな目的の一つである「コスト圧縮」とは矛盾する話でもある。そこで、いかにコストを抑え、上記の要件を満たすかが今後求められるネットワーク要件となる。

つまり、今後求められる方向性は、『さらに「速く」「安く」「止まらない」「いつでもどこでも」「安全・便利」なネットワーク』であるといえる。



(出典) 光ブロードバンドの活用方策検討チーム (第5回) 配布資料

図 クラウド時代に求められるネットワーク要件の一例

6. 政府における検討状況

このような状況を踏まえ、ここでは政府における検討状況を考察してみる。現時点で公になっているクラウド関係の主な研究会等は次のとおり。

- ① スマート・クラウド研究会（総務省等）
- ② 光ブロードバンドの活用方策検討チーム（総務省等）
【http://www.soumu.go.jp/main_sosiki/kenkyu/broadband/index.html】
- ③ クラウドコンピューティング時代のデータセンター活性化策に関する検討会（総務省等）
- ④ グローバルクラウド基盤連携技術フォーラム（民間＋総務省等）
- ⑤ ASP・SaaS データセンター促進協議会（総務省、ASPIC）
- ⑥ 日本データセンター協会（経済産業省等）
- ⑦ クラウド・コンピューティングと日本の競争力に関する研究会（経済産業省等）
- ⑧ 政府情報システムの整備の在り方に関する研究会（総務省）
【http://www.soumu.go.jp/main_sosiki/kenkyu/system_seibi/index.html】
- ⑨ 自治体クラウド部会（LASDEC） ※共同アウトソーシング協議会の下部会
【<http://www.lasdec.nippon-net.ne.jp/cms/9,0,21,207.html>】
★参考：総務省の自治体クラウドポータル
【http://www.soumu.go.jp/main_sosiki/jichi_gyousei/c-gyousei/lg-cloud/index.html】

この中で注目すべきは②⑧⑨である。

②においては、第1回が2009/11/10に開催され、今までに5回（直近は2010/3/24）開催されている。まさにクラウド時代に求められるネットワーク要件について有識者を交えて議論されており、2010/2/28に実施された第4回会合においては、ブロードバンドとクラウドの活用事例が紹介され、次年度以降の実証実験に向けた提言が出されている。

⑧については、第1回が2009/6/3に開催され、今までに6回（直近は2010/1/26）開催されている。まさに霞ヶ関クラウドのあり方等について議論されており、今後さらに霞ヶ関クラウドの実現に向けて具体的な検討が進むものと予想される。なお、本研究会の内容に関連して、2010/2/5には「政府共通プラットフォームに係る業務・システム最適化計画策定及び仕様書（要件定義書）作成等支援作業の請負」業務の意見招請（RFC）が総務省より出されている。

⑨については、第1回が2009/11/24に開催され、今までに2回（直近は2010/3/15）開催されている。本部会においては、自治体クラウドを実現するために不可欠である標準仕様のあり方について議論されている。また、自治体クラウドにおいては自治体間を結ぶ既存のネットワークであるLGWANを利用することが想定されており、今後LGWANに求められる要件についても検討されるものと思われる。

7. 新たなネットワーク技術の一例

上述のように、現在、政府や関連ベンダー（キャリア）等において、クラウド時代に求められるネットワーク要件について積極的な検討が進んでいる。新たなネットワーク技術の一例としては、バーストイーサアクセスのようなものが挙げられる。

バーストイーサアクセスとは、一部の帯域（例えば10%）を確保しつつ、ある短時間において、10Mbpsもしくは100Mbpsの物理インタフェース速度までバースト可能なイーサアクセス回線のことである。ギャランティ型ネットワークの場合、契約帯域が最大速度であり、品質・運用面でビジネスニーズに適さない。また、増速する場合には高価な高速回線の準備が必要となる。それに比べてバーストイーサアクセスの場合、一部の帯域確保部分で基幹データを確実に通信することができ、クラウドからの大量データはバースト利用する、といった柔軟な使い方が可能になる。この場合、リーズナブルな料金で、ギャランティ型同様に高い運用品質が望めることになる。

8. ITコーディネーターの立場として（参考コメント）

日々劇的に変化するIT業界において、最適のソリューションやネットワークを選択することは、一般利用者にとっては非常に難しい。特に、クラウドサービスのようなどちらかと言うと実態が分かりにくいサービス形態の場合、どれだけの帯域／品質のネットワークを準備すればよいかはネットワーク技術者の立場からも判断しにくくなっているというのが実情である。

このような状況下において、ITコーディネーターのような人材は非常に重要な位置づけになると言える。一般利用者（企業）が何かをしたいのか、どのようなサービスを受けたいのか、利便性とセキュリティのどちらを重視するのか、可用性に対する要求事項はどの程度か、等のユーザ要件をきちんと把握し、一方で上述のような政府や関連ベンダー（キャリア）の取組みを踏まえつつ、最適なソリューションやネットワークを選択して示すことが今のITコーディネーターのような人材に強く求められているのではないだろうか。

以上

Google Apps を使用した 安否確認システムの試行について(第1報)

企業内 ITC IT ガバナンス研究会 滝沢 康

社内向けに行ったクラウドサービス (GoogleApps) を使用した安否確認サイトのプロトタイプ構築及び試行についての概要について述べる。

1. 目的

企業の「事業継続計画 ; BCP (Business Continuity Plan)」に取り組む場合に、重要な対策のひとつに安否確認の迅速化がある。

特にネットワークオペレーションセンタ (NOC) および運用部隊は情報インフラのベースであることから

- ・ 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、業務再開への初動体制構築を支援すること

を目的とした安否確認のシステム構築が不可欠となって来ている。

今回は、第1ステップとして安否確認サイトを GoogleApps 上に構築し、NOC 等の一部組織を対象にテスト運用を行う準備を整えるまでを行った。

今後は、NOC など運用部隊へ導入し運用を行い、運用検証を行うとともに検証結果をフィードバックし業務・システム双方の改善を行う。そして最終的には他組織への展開を図っていくものである。



3. 今回作成したドキュメント一覧は以下の通り

- 1) 安否確認サイト 基本設計書 (Rev1.0)
- 2) 安否確認サイト 設定定義書 (Rev1.0)
- 3) 安否確認サイト サイト構築手順書 (Rev1.0)

上記の文書は今回の報告書には添付していないがシステムの概要について次ページ取

り纏めたので参照されたい。

Google Apps を使用した 安否確認システムの試行について(第1報)

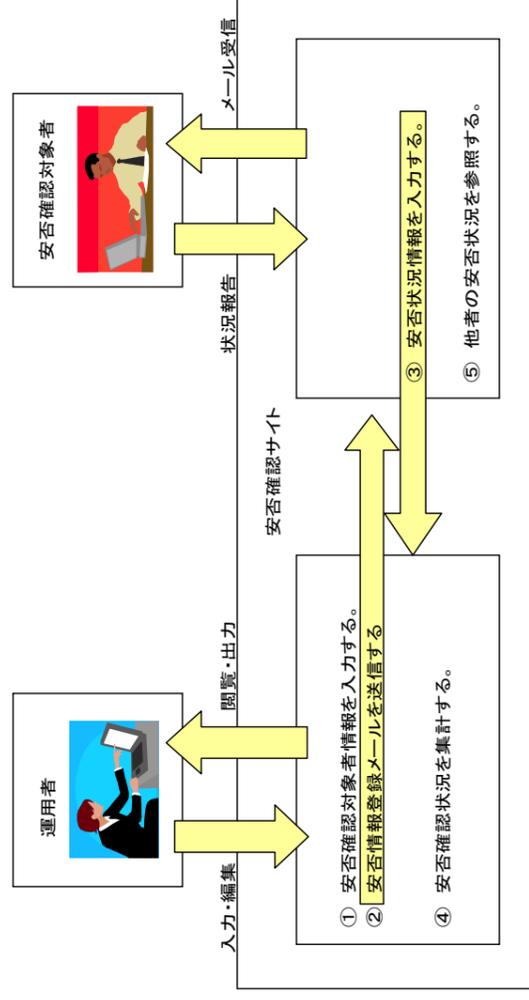
1. 試行(システム化)の目的

以下の実現を本システムの目的とする。

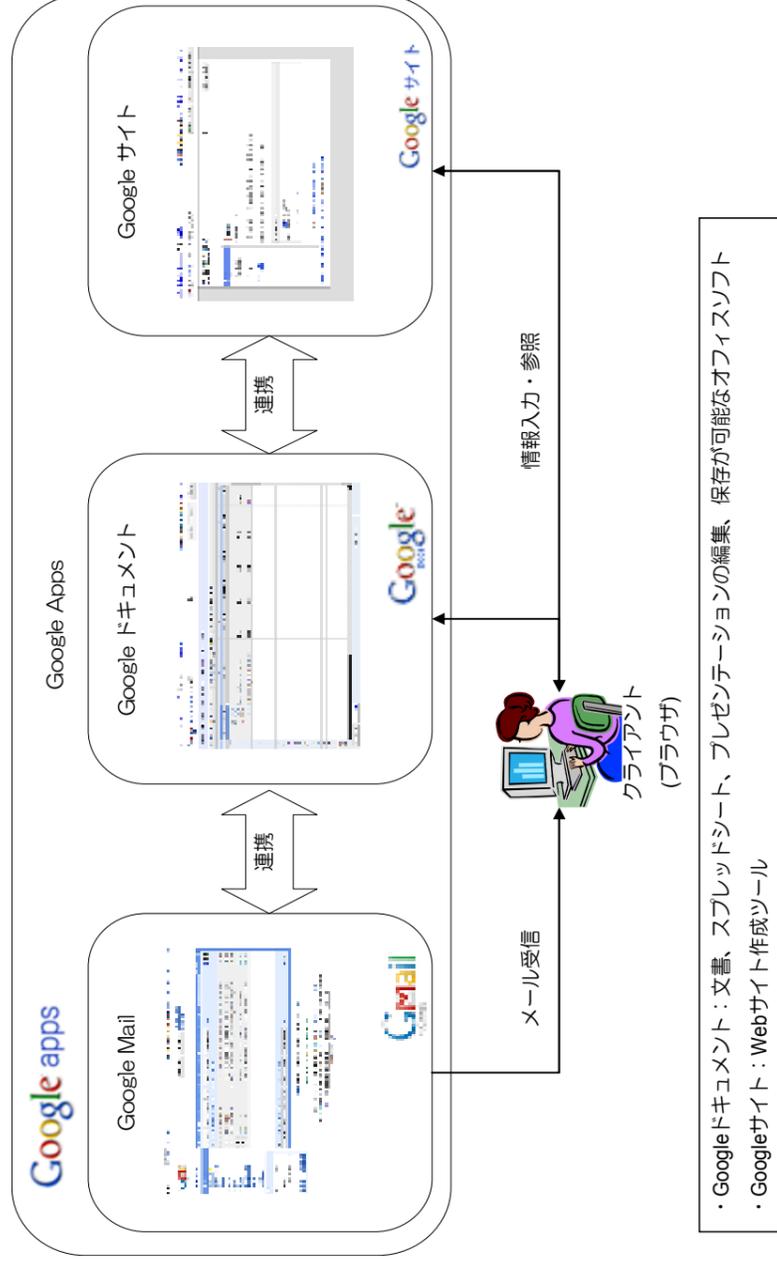
- (1) 災害発生時に社員の安否確認を迅速に把握することを可能にすること
- (2) 安否確認を迅速に行い、業務再開への初動体制構築を支援すること

- 機能1: 安否確認対象者のデータ管理機能
- 2: 安否確認対象者へのメール送信機能
- 3: 安否状況登録機能
- 4: 安否状況集計機能
- 5: 掲示板機能

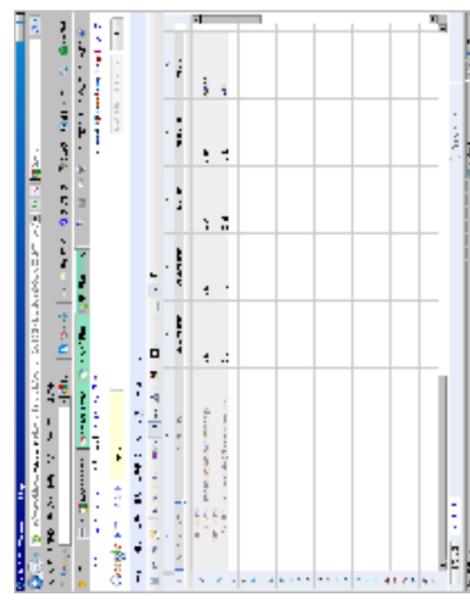
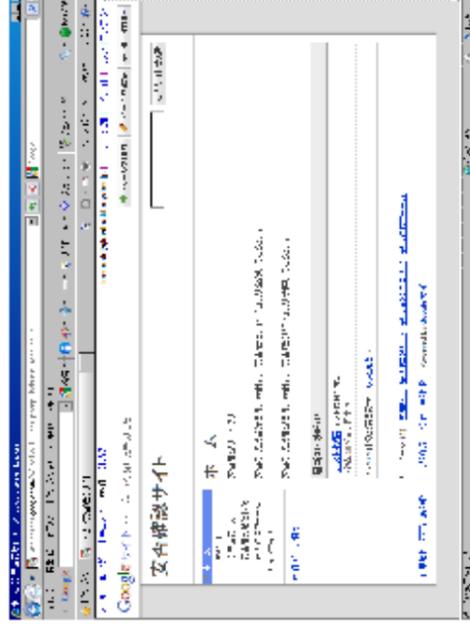
2. システム概念図



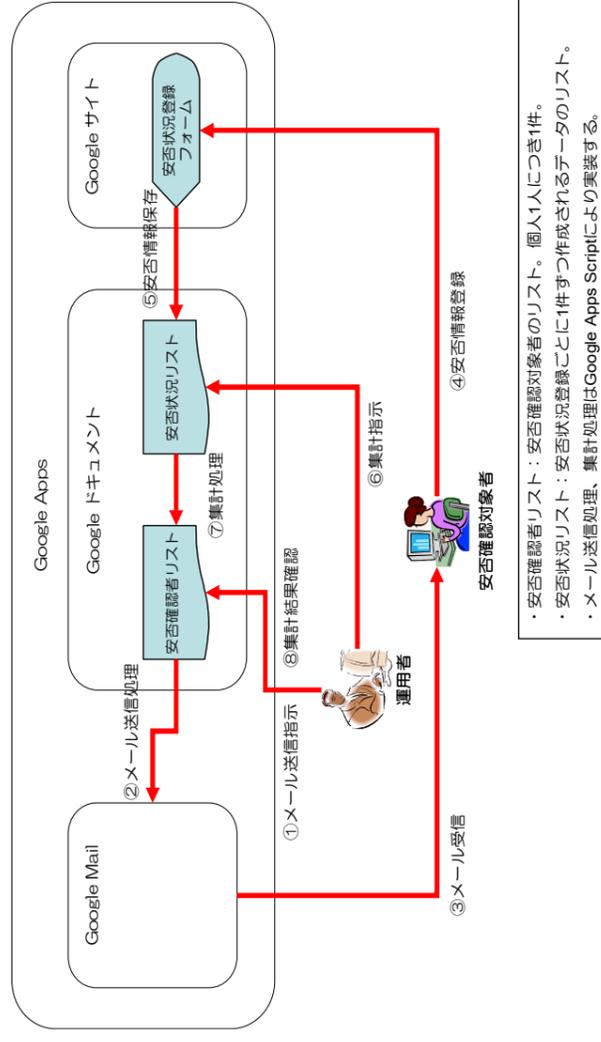
3. ソフトウェア構成



4. 画面イメージ 安否確認サイトトップページ



3. 安否確認の流れ



5. 今後の課題等

- 現時点(2010年4月13日)では(とてりあえず使用可能な)システム環境を構築したのみの状況。
- ① 基幹システム運用・保守メンテの部隊で実際に使って(試行)みてその結果をシステムにフィードバックする。
 - ② 携帯電話等(非スマートフォン)からメールのみでの安否確認可能な様に改造を検討。
安否サイトに確認対象者がアクセスしなくても安否確認が出来る様に検討(Webを使用しない)
 - ③ ①、②の結果をふまえて構築開(社内展開)する。