複数業務システムのための クラウドコンピューティング導入時における 事業者の最適な選定方式の提案

土方広夢† 原田篤史†† 佐々木良一†

近年，クラウドコンピューティングが注目を浴びており，多くの企業組織が事業活動を行う上でクラウドコンピューティングの利用を検討している．それに伴い，様々な企業がクラウドサービスを展開するようになった．クラウドコンピューティングの導入を考える企業では，導入に際して多岐にわたる項目に着目した上で契約するクラウド事業者を選ばなくてはならない．しかし，複数の項目を考慮した上での事業者選定にはセキュリティリスクの分析や，クラウド事業者の調査が必要であるため，長期間にわたる検討や計画が必要であると考えられる．そのため，そのような選定を短期間で効率よく行うためのサポートツールなどが必要であるが，現在までそういったツールは，開発されてこなかった．そこで，自動車部品製造業の企業を想定したモデルケースを用い，その企業が行っている 4 つの業務にとってそれぞれ最適なクラウド事業者を複数の候補の中から効率的に選定する方式を提案する．

Proposal of Method for Selecting Optimal Combinations of Cloud Computing Providers for Multiple Business Systems

HIROMU HIJIKATA† ATSUSHI HARADA††
RYOICHI SASAKI†

Recently, cloud computing has been attracting much attention, and many companies are considering to use the cloud computing in the process of business activities. Accordingly, various providers expand the cloud computing services to match the movement. Companies introducing cloud computing must choice the provider considering the characteristics of the provider on a wide range of fields. However, the choice should be considered to be required long-term consideration and planning because security risk analysis and investigation about cloud providers are required. Therefore, the support tools for efficient selection within short term are necessary. However, such tools have never been developed until now. Therefore, assuming a model case for automobile parts manufacturing company, we propose a method to effectively select candidates from among several providers for the four businesses of the company.

†東京電機大学大学院未来科学研究科
††三菱電機株式会社 情報技術総合研究所

1. はじめに

近年，様々なメディアでクラウドコンピューティングという言葉が飛び交うようになった．そのような時代にあり，多くの企業組織が事業活動を行う上でクラウドコンピューティングの利用を検討している．それに伴い，様々な企業がクラウド事業を展開するようになった．しかし，業務システムのクラウド化は，コスト削減を可能とする反面，個人情報を保存するサーバセンターの所在地や，不正者の攻撃に対する耐性などセキュリティ面での強度が問題視されている．また，クラウドコンピューティングの導入を考える企業では，導入に際してセキュリティの問題以外にも，コストやユーザビリティ等多岐にわたる項目に着目した上で契約するクラウド事業者を選ばなくてはならない．さらに，複数の業務システムにクラウドコンピューティングを導入する場合については，それぞれの業務に合った，クラウド事業者をそれぞれ選ぶ必要がある．しかし，複数の項目を考慮した上での事業者選定にはセキュリティリスクの分析や，クラウド事業者の調査が必要であるため，長期間にわたる検討や計画が必要であると考えられる．

そのため，そのような選定を短期間で効率よく行うためのサポートツールなどが必要であるが，現在までそういったツールは，開発されてこなかった．そこで，自動車部品製造業の企業を想定したモデルケースを用い，その企業が行っている 4 つの業務にとってそれぞれ最適なクラウド事業者を複数の候補の中から効率的に選定する方式を提案する．

選定方式には東京電機大学の佐々木らによって開発された多重リスクコミュニケータ（MRC：Multiple Risk Communicator）の一部機能を利用する．

2. クラウドコンピューティングとは

クラウドコンピューティングとは，米国標準技術局（NIST：National Institute of Standards and Technology）によって定められた定義によると，“設計可能な計算機資源（ネットワーク，サーバ，ストレージ，アプリケーション，サービス）の共用備蓄所（プール）へ，簡単かつオンデマンドにネットワークアクセスすることを可能にするモデルである”とされている．本質的な性質としては，オンデマンドセルフサービス・幅広いネットワークアクセス・計算資源の備蓄所・迅速な伸縮性・測定されたサービスなどが挙げられる[1].

クラウドコンピューティングのサービスモデルには以下の 3 つが存在する．

1. Software as a Service （SaaS）
クラウド基盤上で稼働するアプリケーションを提供するサービスを指す．利用者は，Web ブラウザのようなクライアントインターフェースを通じ，様々な情報端末からアプリケーションにアクセスが可能である．
2. Platform as a Service （PaaS）
サービス提供者によりサポートされるプログラミング言語やツールを用いて作成または用意したアプリケーションを，利用者がクラウド基盤に配置可能なプラットフォームを提供するサービスを指す．
3. Infrastructure as a Service （IaaS）
OS やアプリケーションを含め，利用者が任意のソフトウェアを配置し実行可能にする処理能力やストレージ，ネットワーク，あるいは他の基礎的な計算機資源を提供するサービスを指す．

SaaS，PaaS，IaaS は図 1 のような階層構造を持つ．

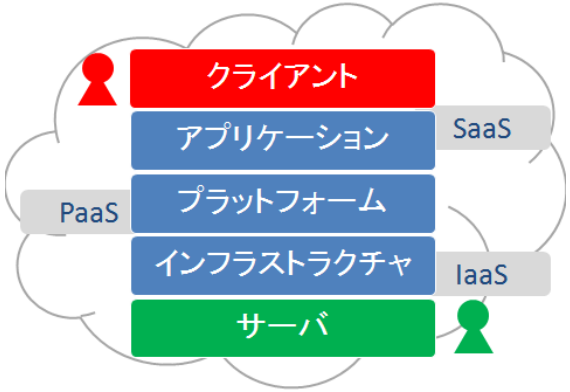

図 1　クラウドコンピューティングの階層
Figure 1　Stratum of cloud computing.

また，クラウドコンピューティングの配置モデルには以下の 4 つが存在する．

1. プライベートクラウド
単一の組織によって運用されるクラウド基盤を指す．
2. コミュニティクラウド
複数の組織により共用されるクラウド基盤を指す．
3. パブリッククラウド
一般利用者や大きな産業体が利用可能であり，クラウドサービス事業者により所有されるクラウド基盤を指す．
4. ハイブリッドクラウド
2 つ以上のクラウド（プライベート，コミュニティ，パブリック）から構成されるクラウド基盤を指す．

クラウドコンピューティングの構造は図 2 のようになっている．

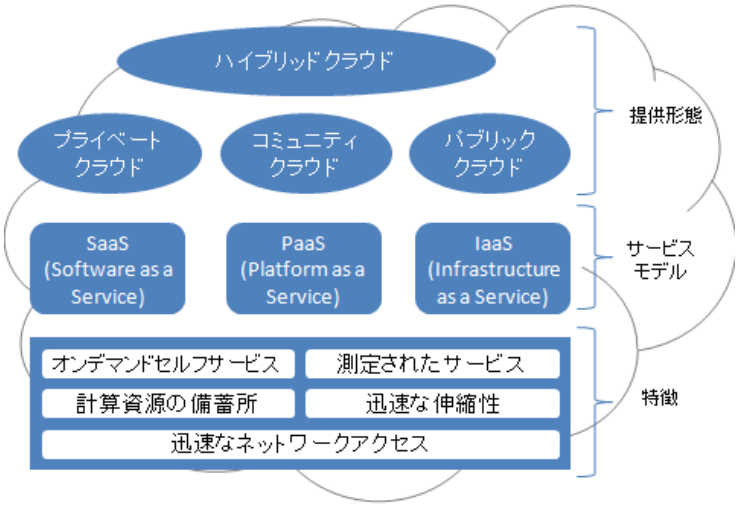

図 2　クラウドコンピューティングの構造
Figure 2　Structure of cloud computing.

クラウド事業者は，Google，SalesForce，日本では NEC，Nifty など数多く存在する．そのため，企業のシステムに適したクラウド事業者を選ぶことが難しい状況になっている．

また，クラウドコンピューティングの利点として，日々変化するビジネスシーンに合わせた迅速なシステムの構築が可能であることや，システム構築に必要な費用が削減できるといった事柄が挙げられる．一方で，クラウドコンピューティング固有のリスクも存在する．

2.1 クラウドコンピューティングのリスク

前章にて解説をしたクラウドコンピューティングにはセキュリティや他の様々なリスクがあると言われている．欧州ネットワーク情報セキュリティ庁（ENISA：

European Network and Information Security Agency）によって報告されたクラウドコンピューティングのリスクを以下に挙げる[2].

クラウドコンピューティングにおけるリスクには，大別して，組織的なリスク，技術的なリスク，法的なリスク，共通事項と分類することができる．その分類と具体的なリスク内容を表 1 に示す．リスク内容の括弧内はリスクの評価となっており，それぞれ H は高い（頻繁に発生する），M は中程度（稀に発生する），L は低い（ほとんど発生しない）となっている．

表 1　クラウドコンピューティングのリスク
Table 1　Risk of cloud computing.

分類	リスク（評価）
組織的なリスク	ロックイン（H），ガバナンスの喪失（H），サービスの停止・障害（H），クラウドプロバイダの買収（M），サプライチェーンのトラブル（L）
技術的なリスク	内部者の悪意（H），管理者の特権乱用（H），リソースの問題，管理者機能の悪用（M），データ妨害・漏洩（M），DDos（M）
法的なリスク	法令による命令や証拠保全（H），裁判管轄の違い（H）
共通事項	ネットワーク管理ミス（H），ネットワークのダウン（M），ネットワークトラフィックの経路変更（M），権限奪取（L），自然災害（L）

組織的なリスクは，ロックインやガバナンスの喪失など，クラウド事業者の在りようが問題となるリスクである．技術的なリスクは，システムがもつ

3.　MRC（Multiple Risk Communicator）とは

セキュリティ対策の選定等の問題を考えた際に，複数の関与者間での意見の対立が起こることがある．例えば，個人情報漏洩問題の対策を講じる際に，シンクライアント PC を導入するためには莫大なコストが必要なため，経営者には難色を示されてしまったり，メール送信に上長の許可を必要とする制度を取り入れれば従業員の作業効率が下がってしまうため，反対にあってしまったりといったことが考えられる．

そのような対立を解決するためには，関与者の間でリスクコミュニケーションを行う必要がある．MRC は，対策案の最適な組み合わせを求めるとともに，そのようなリスクコミュニケーションを支援するための佐々木らが開発したツールである[3].

MRC は，それを用いて個人情報漏洩に関する最適な対策の選定方法の研究などが行われてきた[4].

MRC では，図 3 に示すような手順で組み合わせ最適化問題として定式化を行い，対策案の最適な組み合わせ（最適解）を求め，関与者間のリスクコミュニケーションを繰り返すことにより合意形成を支援する． また，関与者の他にファシリテータと呼ばれる者がいる．ファシリテータは，意思決定関与者間の議論の仲立ちを行う立場の者である．専門家は，MRC へのデータ入力や，リスク分析などを行う者のことである．

リスク分析にはフォルトツリー解析を用いる[5]．フォルトツリー解析とは，発生してはいけない事象（頂上事象）の発生する確率が不明である場合に用いる解析手法である．フォルトツリーでは，頂上事象に対してその原因となる事象を AND ゲートや OR ゲートを用いて，ツリー上に展開する．そして，発生確率が特定できる事象までの展開が完了した段階で，最下層の事象（末端事象）の発生確率を定め，頂上事象の値を求める．

MRC では，末端事象の発生原因を防ぐ対策案を定め，そのパラメータとして対策案効果を決定する．対策案効果の値に応じて末端事象の発生確率を低減することで最適解の算出に利用する．対策案効果については，4.3 節にて詳しく述べる．

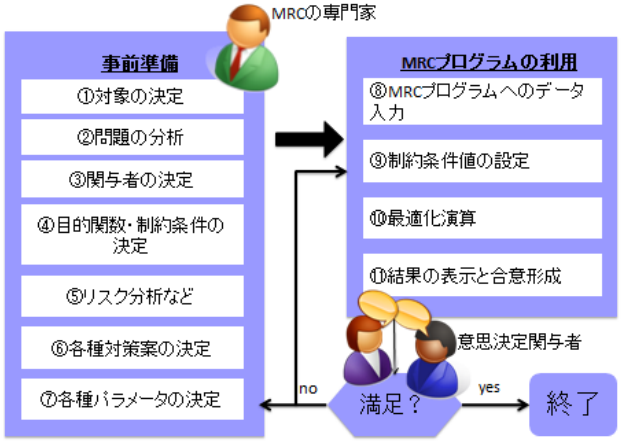

図 3　MRC の概要
Figure 3　Outline of MRC.

4. MRC を用いた適用

本方式では，MRC における最適化問題の解を算出するための演算部と，演算に必要な目的関数と制約条件の入力部，リスク分析のためのフォルトツリー解析支援部を利用する．それらを利用した上で，自動車部品製造業の企業を想定し，その企業が行っている業務にとってそれぞれ最適なクラウド事業者を複数の候補の中から効率的に選定するモデルケースを用い，MRC による適用を行う．

4.1 想定する組織

想定する組織は，前述の通り自動車部品製造業を営む企業 X 社で，詳細は表 2 の通りである．

表 2　想定する企業の情報
Table 2　Information of assumed company.

詳細の項目	内容
業種	製造業/自動車部品の製造
従業員数	1,000〔名〕
年間の売上	150〔億円〕
クラウド化する業務	発注・製造・受注・在庫管理
取引先企業数	納入元50社/納入先2社
保持する機密情報	発注情報・受注情報・取引額
情報件数	52件

機密情報は四つの業務でそれぞれ 52 件ずつ保持しているものとする．また，保持する機密情報の価値は一件あたり 2,000 万円とする．

また，X 社は業務システムのうち，発注，製造，受注，在庫管理のシステムをクラウド化することを検討しており，それぞれの業務システムに対し最適なクラウド事業者の選定を行う．そこで，経営者や従業員，クラウドコンピューティングの知識を有する社員の間で最適なクラウド化に向けたリスクコミュニケーションを行う際に，本方式を用いるものとする．

4.2 フォルトツリー解析を用いたリスク分析

頂上事象には，前述の ENISA のリスクにおける技術的なリスクの項目を用いる．その中でも発生頻度の高い，内部者の悪意，管理者の特権乱用が原因である機密情報の漏洩を頂上事象とするフォルトツリーを展開する．

この適用では上記フォルトツリーを八つ作成する．その内訳を以下に示す（表 3）．

表 3　全フォルトツリー
Table 3　All fault trees.

変数	頂上事象の内容
f1	発注における内部者の悪意が原因となる情報漏洩
f2	発注における管理者の特権乱用が原因となる情報漏洩
f3	製造における内部者の悪意が原因となる情報漏洩
f4	製造における管理者の特権乱用が原因となる情報漏洩
f5	受注における内部者の悪意が原因となる情報漏洩
f6	受注における管理者の特権乱用が原因となる情報漏洩
f7	在庫管理における内部者の悪意が原因となる情報漏洩
f8	在庫管理における管理者の特権乱用が原因となる情報漏洩

各フォルトツリーを図 4 と図 5 のように簡易的に展開した．展開したツリーの末端事象における発生確率は，頻繁に発生する場合には 0.8，稀に発生する場合には 0.4，ほとんど発生しない場合には 0.2 とした．これは例えば，0.2 の場合には 5 年間に 1 回発生するということを表している．

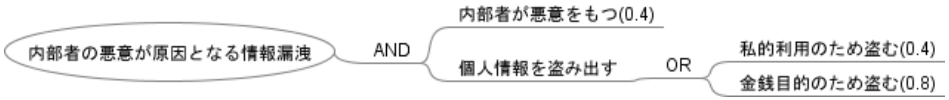

図 4　内部者の悪意が原因となる情報漏洩
Figure 4　Information leakage caused by venomous insider.

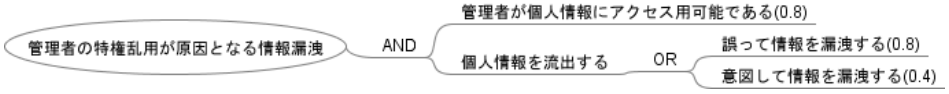

図 5　管理者の特権乱用が原因となる情報漏洩
Figure 5　Information leakage caused by abusing of administrative privileges.

.

4.3 目的関数と制約条件の設定

目的関数とは，MRC による最適化演算の際に最小となるように構成された関数のことである．本モデルでは，頂上事象の発生確率と発生した際の損害額の積と，クラウド化にかかる総費用の和を目的関数として用いる．目的関数は次の式で表すことがで

きる．

$$目的関数 = \mathrm{Min}(20000000 * 52 * \sum_{x=1}^{8} f_x + \sum_{y=1}^{4} \cos t_y)$$

制約条件とは，MRC により最適解を算出する際に考慮される制約のことである．制約は値で表わされ，制約条件 A<=a（A は条件名，a は有理数）のような形で用いる．

制約条件には，ENISA のリスクにある組織的なリスクと法的なリスクを用いる．その中でも，リスク評価が H となっているロックイン，ガバナンスの喪失，サービスの停止・障害，法令による命令や証拠保全，裁判管轄の違いを制約条件とする．また，その変数をそれぞれ，c_1，c_2，c_3，c_4，c_5 とする．

次節で紹介するクラウド事業者毎に制約条件の各項目に対する耐性を数値（耐性値）として与える．耐性と値の関係を表 4 にまとめる．

表 4　耐性値の目安
Table 4　Indication of tolerance value.

耐性の度合い	値
強い耐性がある	1.0
やや強い耐性がある	0.8
中程度の耐性がある	0.6
耐性が弱い	0.4
耐性がない	0.2

耐性値が 1.0 のとき，対応するリスクを無視できるものとし，それ以下のときは割合で耐性が減っていくものとする．また，値が 0.0 のときにはリスクを一切低減することができない場合とする．

選ばれた全ての事業者の耐性値の総和が，制約条件で指定した値（制約条件値）を超えない（あるいは，下回らない）ようにすることで条件として用いる．

4.4　クラウド事業者

四つの業務システムをクラウド化するためのクラウド事業者の候補としては，海外のパブリッククラウド提供者 A 社，国内のパブリッククラウド提供者 B 社，プライベートクラウドを提供する国内の大手自動車メーカーC 社を想定する．また，システムをクラウド化せずに自社システムをもちいるという選択肢も用意することとする．ただし，C 社によるシステム構築は受注業務のみとする．以下に候補となる事業者とその特徴をまとめる．

表 5　候補となる事業者と詳細
Table 5　Prospective providers and those details.

社名	詳細	特徴
A社	海外の事業者（パブリック）	安価・ロックインの危険性
B社	国内の事業者（パブリック）	高価
C社	国内の大手自動車メーカー（プライベート）	受注業務のみ対応
X社	自社システム	手間がかかる

クラウド事業者毎の各事業システムをクラウド化する費用（コスト）とフォルトツリー f_1 から f_8 までの各末端事象に対する耐性，制約条件毎の耐性を表 6 と表 7，表 8 にまとめる

表 6　各事業者の耐性値
Table 6　Tolerance value of each providers

	f1	f2	f3	f4	f5	f6	f7	f8
A社	0.4	0.4	0.4	0.4	0.4	0.4	0.4	0.4
B社	0.6	0.6	0.6	0.6	0.6	0.6	0.6	0.6
C社	-	-	-	-	1.0	1.0	-	-
X社	0.8	0.8	0.8	0.8	0.8	0.8	0.8	0.8

表 7　各システムの費用
Table 7　Cost of each systems.

	発注システムのコスト	製造システムのコスト	受注システムのコスト	在庫管理システムのコスト
A社	300[万円]	200[万円]	200[万円]	200[万円]
B社	400[万円]	300[万円]	300[万円]	300[万円]
C社	-	-	400[万円]	-
X社	600[万円]	500[万円]	500[万円]	500[万円]

表 8　各事業者の制約条件値
Table 8　Constraints values of each providers.

	c1	c2	c3	c4	c5
A社	1.0	0.8	0.4	0.4	1.0
B社	0.4	0.6	0.2	0.0	0.0
C社	0.6	0.6	0.2	0.0	0.0
X社	0.0	0.0	0.2	0.2	0.0

4.5 MRC による演算結果

上記モデルを MRC に入力し，演算を行った結果を次のような解が得られた．この演算では，制約条件に条件を設定しない状態で行った．

- 発注システムにおける最適なシステムは X 社による自社システム
- 製造システムにおける最適なシステムは X 社による自社システム
- 受注システムにおける最適なシステムは C 社によるプライベートクラウド
- 在庫管理システムにおける最適なシステムは X 社による自社システム

この結果は，機密情報の価値がシステム導入コストに比べて非常に大きかったために，コストを度外視した上でリスクの低減を行ったためであると考えられる．しかし，実際の適用では関与者に経営者が存在するため，コストの削減や，クラウド化による迅速なシステム構築などの観点から，A 社や B 社のようなクラウド事業者を選定する必要を訴える可能性がある．その際に，制約条件値を設定することで，コストやリスクに関する関与者の意見を MRC による最適解に反映することが可能となる，

5. おわりに

本稿では，企業が業務システムにクラウドコンピューティングを導入する際の最適な事業者選定法に関して，自動車部品製造業の企業を例に述べた．この度の適用では，関与者間におけるリスクコミュニケーションや制約条件を設定した際の求解を行なわなかった．そのため今後は，実際に利用した際の評価を行うとともに，異なる業種の異なる企業が利用する場合であってもより柔軟に対応することが可能なシステムとすることが課題であると考えられる．

また，本方式では，配置モデルごとの最適化を行ったが，今後はサービスモデル毎の最適化を想定していく必要がある．

参考文献

1) Peter Mell,Tim Grance,（訳: 金岡晃）「NIST によるクラウドコンピューティングの定義」，http://kanaweb.cs.tsukuba.ac.jp/doc/nist_cloud_def_japanese.pdf

2) ENISA「Cloud Computing: Benefits, risks and recommendations for information security」，http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport

3) 佐々木良一，日高悠，守谷隆史，谷山充洋，矢島敬士，八重樫清美，川島泰正，吉浦裕：多重リスクコミュニケータの開発と適用，情報処理学会論文誌, Vol.49, No.9, pp. 3180-3190 (2008)

4) Hiromu Hijikata, Ryoichi Sasaki: Application of Multiple Risk Communicator for Consensus on Personal Information Leakage Measures Considering Digital Forensics, ICIMT 2010 2nd International Conference on Information and Multimedia Technology, pp. 223-227 (2010)

5) N.J. McCormick: Reliability and Risk Analysis, Academic Press Inc. (1981)