Vol.2010-DPS-142 No.4
Vol.2010-CSEC-48 No.4
2010/3/4

クラウドと IT リスクに関する考察

佐々木良一[†]

概要：近年クラウドコンピューティング（Cloud Computing, 以下、単にクラウドともいう）に関する関心が高まっている。クラウドには「いろいろな長所がある半面、セキュリティなどに関しいろいろな問題がある」と指摘されながら十分な検討が行われてこなかった。本稿では、クラウドについてその概要、動向、それの影響について整理するとともに、クラウドと IT リスクの問題を（a）狭義のセキュリティ、（b）ディペンダビリティ、（c）トラストの 3 つに分類し課題と対策案を整理する。あわせて、それらを実現するための技術について提案を行う。

Consideration on Cloud Computing and IT Risk

Ryoichi Sasaki[†]

Abstract: Recently, the interest to cloud computing has increased. Although, the cloud computing has many advantages, it has also disadvantage concerning the security. However, enough analysis to the security has been not conducted. This paper deals with the outline, the movement and the effect of the cloud computing. Moreover, we describe IT risk problems and countermeasures from viewpoints of security in narrow mind, dependability and trust issue. Last of all, we propose the techniques to achieve the countermeasures.

1. はじめに

近年クラウドコンピューティング（Cloud Computing,）に関する関心が高まっている。クラウドコンピューティング（以下、単にクラウドともいう）というのは、米国グーグルの CEO エリック・シュミット（Eric Schmidt）が 2006 年に最初に利用したといわれることばであり、後述するようにいろいろな定義があるが、「ローカル・マシンやリモート・サーバ・ファームではなく、グローバルにアクセス可能な分散されたリソースの集合体を利用するコンピューティング」とする IBM の定義がわかりやすい。従来のコンピュータ利用は、ユーザー（企業、個人など）がコンピュータのハードウェア、ソフトウェア、データなどを、自分自身で保有・管理していたのに対し、クラウドコンピューティングでは「ユーザーはインターネットの向こう側からサービスを受け、サービス利用料金を払う」形になる。

クラウドは，利用者がいろいろなコンピューティングサービスを必要な時，必要な規模で安価（場合によっては無料）で使えるなどの長所がある半面，セキュリティに関する問題も多いと指摘されている。このセキュリティに関する問題の検討も始まっている[３]-[５]が，問題の本質を的確に指摘し，対策をわかりやすく明確に示したものになっているとはかならずしも思えない。

本稿では、２節でクラウドについてその概要、動向、それの影響について整理する。３節ではクラウドと IT リスクの問題を（a）狭義のセキュリティ、（b）ディペンダビリティ、（c）トラストの 3 つに分類して検討すべきであることを示すとともに、課題と対策案を整理する。４節では、それらを実現するための技術について提案を行う。

2．クラウドコンピューティングの概要

2.1 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については、先に述べた IBM のものを含めいろいろな定義がなされてきたが最近では米国の NIST（National Institute of Standards and Technology）の定義[１]がよく引用されるようになってきた。ここでは、「このクラウドモデルは可用性を推進するものであり、５つの重要な特徴、3 つのサービスモデルそして 4 つの実現モデルによって構成される。」としており、５つの重要な特徴は表 1 に、3 つのサービスモデルは図 1 に、そして 4 つの実現モデルは図 2 に示すとおりである。

† 東京電機大学未来科学部情報メディア学科

Vol.2010-DPS-142 No.4
Vol.2010-CSEC-48 No.4
2010/3/4

表1　5つの重要な特徴

重要な特徴(Essential Characteristics)	解　説
オンデマンド・セルフサービス On-demand self-service	ユーザーが、プロバイダーの提供するコンピューティング機能(サーバーの使用時間やネットワーク・ストレージなど)を人手を介することなく自動的に割り当てられ、提供されること。
広範なネットワークによる接続 Broad network access	ネットワーク上で利用される標準的なメカニズムを介して、異なるデバイス(携帯電話、ノートパソコン、PDA等)で利用できること。
システム資源のプール Resource pooling	プールされているプロバイダーの物理的なコンピューティング資源を仮想し、ユーザーの要求に応じて、ユーザーごとに独立したシステム単位(マルチテナント)として動的に割り当、再割り当てできること。コンピューティング資源がどこに存在しているかは、ユーザーからは、分らない。ここでいう資源とは、ストレージ、処理能力、メモリ容量、ネットワーク帯域幅、仮想マシンを言う。
迅速な順応性 Rapid elasticity	必要となる資源の増減が、システムによって迅速かつ弾力的に行われる機能を有していること。そして、この対応が自動的に行われること。
従量課金サービス Measured Service	各種サービス機能(例えば、ストレージ、計算処理、帯域幅など)をその使用量に応じて課金する仕組みを持つこと。

http://japan.zdnet.com/blog/netcommerce/2009/10/30/entry_27035197/?ref=rss

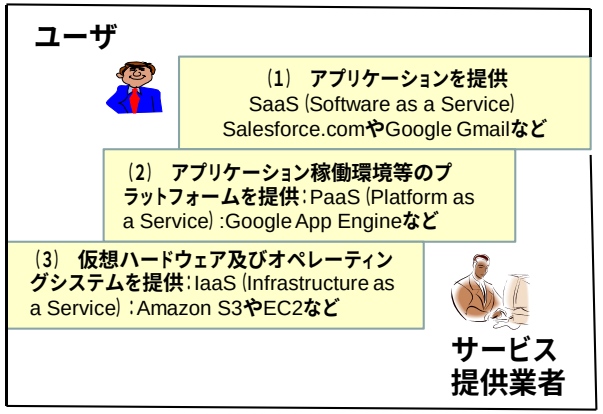

図1　クラウドの3つのサービスモデル

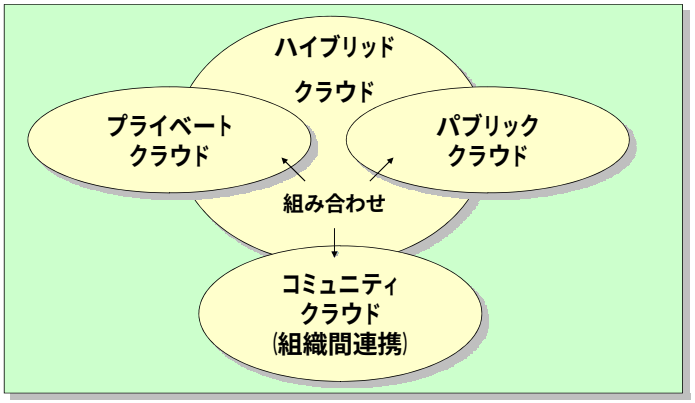

図2　クラウドの4つの実現モデル

2.2　クラウドコンピューティングがもたらすもの

クラウドが今後普及していくことは間違いないと考えられるが、その適用分野は、パブリッククラウドについては、最初は図３に示すように、「顧客獲得のために差別化を生み出す分野ではなく」、かつ「問題があると重大な影響がある分野ではない」領域を中心にして実現されると考えられる[２]。このため中小企業からの導入が中心になっていくだろう。大企業においては新しいサービスを始める分野から導入が進むのではないか。一方、プライベートクラウドは大企業が導入の対象となり、コミュニティクラウドは企業群や地方自治体群が参加の対象になるだろう。

いろいろなことが安価に実現できると期待するユーザの立場からのクラウドの面だけでなく、Google や Amazon.com、マイクロソフトなどによる国際的囲い込み戦略としてのクラウドの面もある。この面からみると、クラウドは第 4 のダウンサイジングの波であり、計算機、ネットワーク、ソフトウエアに次ぎ SI に関するダウンサイジングが進行

Vol.2010-DPS-142 No.4
Vol.2010-CSEC-48 No.4
2010/3/4

しつつあると見ることもできるだろう。これにより日本の IT 産業はいろいろな影響を受けると考えられるが、特に SI 産業はマーケットを失い残されたマーケットも低価格化の波を受けざるを得なくなると考えられる。プライベートクラウドやコミュニティクラウドでよい提案ができた企業だけがよいポジションをキープできることになるのだろう。

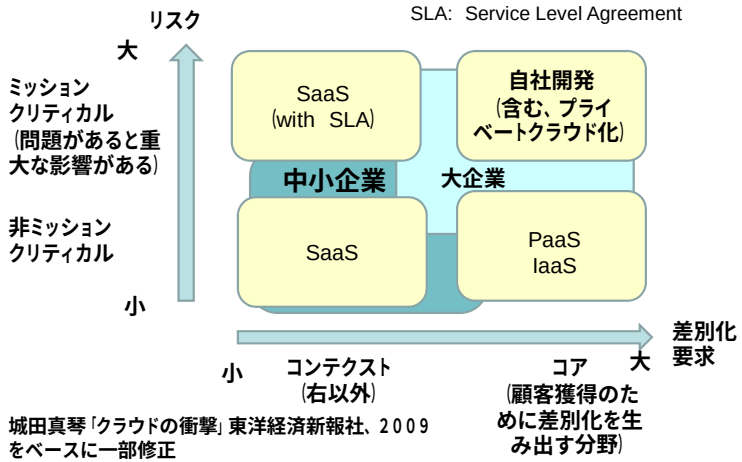

図3　クラウドの適用領域

3．クラウドコンピューティングと IT リスク

クラウドにおいては、セキュリティが大きな問題になるといろいろなところで言われているが[３][４][５]、それらの問題を的確に指摘し、対策をわかりやすく示したものになっているとは必ずしも言えない。セキュリティの問題といわれているものは、正確には安全・安心に関する問題あるいは IT リスク[６]に関する問題というべきものであり、次の３つに大別すべきであると考えられる。

（１）狭義のセキュリティに関する問題：外部や内部の人間による故意の不正によって生じる問題。

（２）ディペンダビリティに関する問題：ソフトのバグやハードの故障やヒューマンエラーによって生じる問題。

（３）トラストに関する問題：サービス提供者への信用と信用すべき状態の間にアンバランスが生じる問題。

以下それぞれについて問題の概要と対応策を述べる。

3．1　狭義のセキュリティの問題と対策

狭義のセキュリティに関する問題は、図４に示すように①外部の不正者によるクラウドサービス提供業者への攻撃、②外部の不正者によるサービス利用者への攻撃、③内部の不正者によるクラウドサービス提供業者への攻撃、④内部の不正者によるサービス利用者への攻撃に大別される。

このうち、①③のクラウドサービス提供者に関する対策は次のようなものが考えられる。

（ａ）入退出管理、監視カメラなどの物理的対策

（ｂ）アクセス制御、暗号化、セキュリティ監視などの情報処理的対策

（ｃ）セキュリティ管理、監査などの管理的対策　他

これらは、一般企業などにおける対策と基本的に同じであるが、説明責任を果たすためやどちらに責任があるかを明確にするためのログの収集などの対策は一般により強く要求されると考えられる。

一方、クラウド（特に SaaS）のサービス利用者に関する対策は、セキュリティ監視やセキュリティ教育が中心になると考えられる。これらの企業にもクライアントＰＣなどは残るが、それに対するセキュリティ対応能力はどんどん落ちると考えられ、ここへの攻撃が問題になりうる。そのため、検疫ネットやセキュリティ監視、セキュリティ応急

Vol.2010-DPS-142 No.4
Vol.2010-CSEC-48 No.4
2010/3/4

対応と組み合わせた End-End セキュリティサービスのクラウド化は大きなビジネスチャンスになりうると考えられる。これらに対する技術開発は今後の課題であろう。

なお、PaaS や IaaS の場合は、サービスの提供者と利用者の間で、セキュリティ対策の種々の分担を適切に行う必要がある。

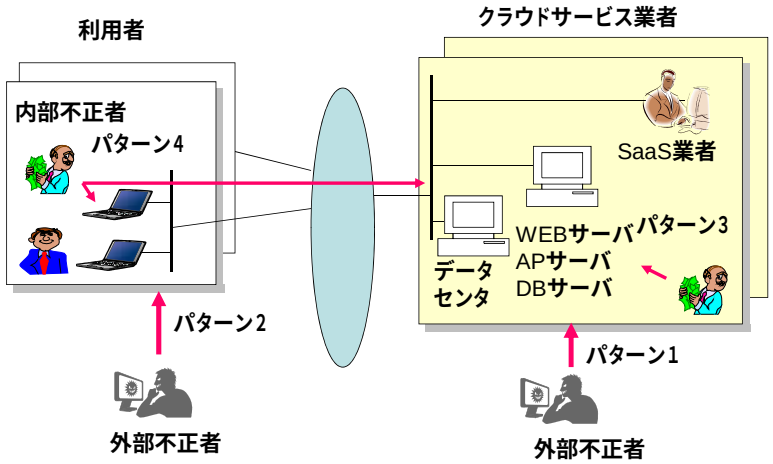

図4　セキュリティに対する攻撃パターン

3.2　ディペンダビリティの問題と対策

ここで扱うのは、ソフトのバグやハードの故障、ヒューマンエラーさらには天災などによって生じる問題である。これらの問題に対する対策は以下のように整理することができる。

① 通常時対策

（1）機能更新時の変更管理

（2）分散環境におけるデータの同一性保持

（3）負荷変動への対応機能（分散処理技術、サーバ仮想化技術）

② 障害回避対策（フォルトアボイダンス）

（4）バグの少ないソフトの導入など

③ 障害時対策（フォルトトレランス）

（6）計算機やネットワーク機能の多重化（フォルトトレランス）

（7）データのバックアップ（消去対応、アーカイビング）

（8）地震などに備えたバックアップセンターの設置（ディザスタリカバリー）

（9）BCP（business continuity plan）・BCM（business continuity management）の推進

これらは、いずれも重要な技術であるが、クラウドコンピューティングにおいては、図 5 に示すように仮想化やディペンダブルコンピューティングは基本技術としていろいろ研究されてきており、セキュリティ技術者が新しく参入して実施すべき研究項目は少ないと考えられる。ただ，複数の組織が入り組んだ中での事業継続計画の研究はこの分野においてもこれからであり，面白い研究テーマになりうると考えられる。

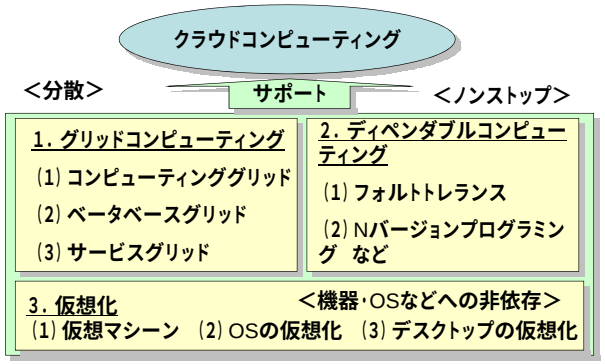

図5　クラウド実現のための基本技術

Vol.2010-DPS-142 No.4
Vol.2010-CSEC-48 No.4
2010/3/4

3.3　サービス提供者へのトラストの問題と対策

クラウドサービスには，以下のような不安がありうる（図 6 参照)。

（a）将来にわたりサービスしてもらえるか

（b）データの目的外使用や不正処理をしていないか

（c）希望する安全レベルが確保されているか

（d）政府などによる検閲のある国で処理してないか

（e）障害や不正があったとき調査などに協力してもらえるか

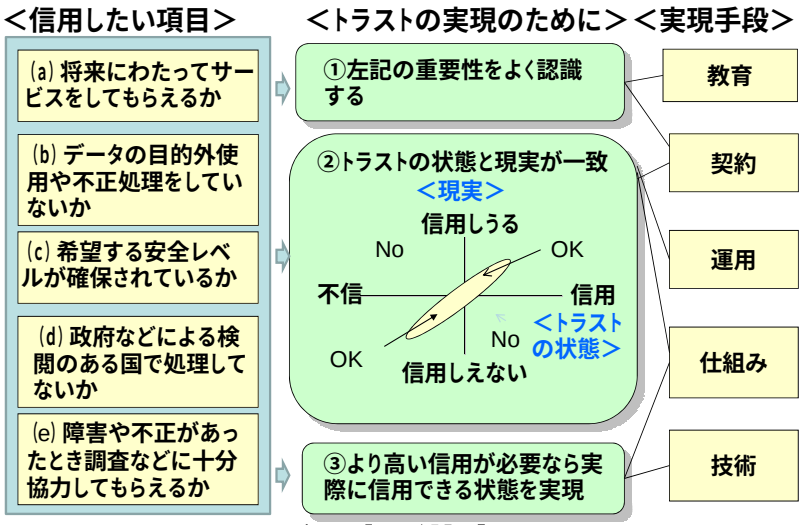

図6　サービス提供者へのトラスト

このような問題を解決するためには次のような対応が必要である。

（1）クラウド利用者は上記のような問題があることをまず知る必要がある。

（2）次に，これらの問題が解決されているのかどうかの正しい認識をクラウド利用者が持つとともに，

（3）価格やサービスの質との関係においてクラウドを利用すべきかどうかを適切に判断できるようにする必要がある。

このためには①クラウド提供者が信用を勝ち取れるようにするための技術や運用だけでなく，②認識どおりの状態であることを確保するための SLA（Service Level Agreement）などの契約やコンプライアンスなど法的な対応も大切となる。もっとも重要なことはどのように契約するかであり、適切な契約を行えるようにするためのガイドが総務省から出ている[7]。

技術としては、クラウドサービス提供業者のようなサーバなどを管理する者であっても不正を行えばすぐにわかる高度な技術が必要となると考えられる。

4．必要となる技術

以上まとめると、次のような技術が大切になると考えられる。

（1）狭義のセキュリティに関連して

クラウドユーザ（特に SaaS ユーザ）のための検疫ネットやセキュリティ監視、セキュリティ応急対応と組み合わせた End-End セキュリティサービス技術

（2）ディペンダビリティに関連して

複数の組織が入り組んだ中での BCP（business continuity plan)・BCM（business continuity management）技術

（3）トラストに関連して

クラウドサービス提供業者のようなサーバなどの管理者であっても不正を行えばすぐにわかる技術。サーバの管理者であれば記録の消去などいろいろな処理を行い得るのでその実現は簡単ではないが重要な技術である。

Vol.2010-DPS-142 No.4
Vol.2010-CSEC-48 No.4
2010/3/4

（３）に関しては、すでに研究を開始している。ここでは、クラウドサービス業者のとるログが改ざんされていないことを証明できるようにするためＨｉＧＡＴＥ（High Grade Anti-Tamper Equipment）というＰＣベースのハードソフトシステムを開発している[８]。改ざんの検知は通常ならＩＣカードなどを利用したデジタル署名を利用することによって実現可能である。しかし、ＰＣやサーバなど情報処理装置の持ち主ならＩＣカードに与えるハッシュ値を PC などの中で変更することは容易である。これを防止するためにはＰＣそのものをＩＣカードのようにトラスティドサードパーティ化する必要がある。このため、図７に示すようなホワイトリストや不正プログラムの立ち上げ制御技術を用いることにより、この機能を実現している。詳細については文献[８]を参照願いたい。

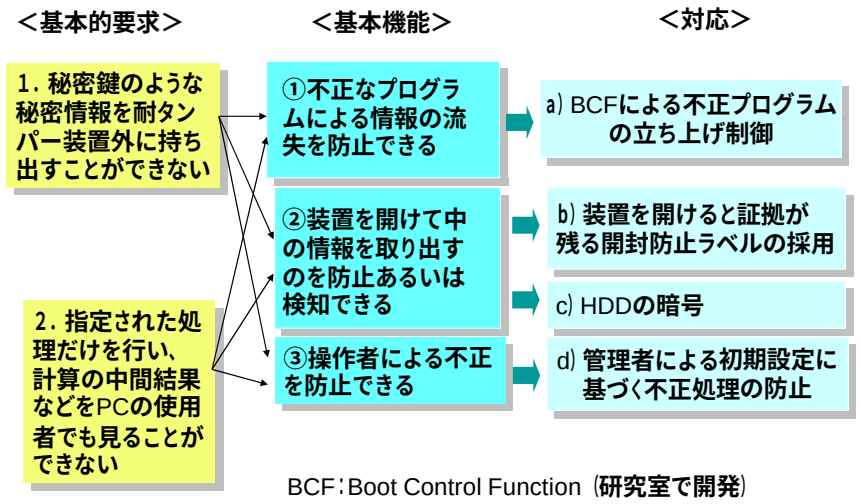

図7　HiGATEの機能要件と対策

これにより、クラウド業者がログなどの改ざんをすれば容易に検知できるので、不正の抑止が可能となる。HiGATE は、これ以外に情報処理装置の持ち主でも中間結果を見てはならないような計算（例えば、疫学調査のような複数の組織の情報を利用する統計処理）などにも広く適用できると考えている。

５．おわりに

以上，クラウドについてその概要、動向、それの影響について整理するとともに、クラウドと IT リスクの問題を（ａ）狭義のセキュリティ、（ｂ）ディペンダビリティ、（ｃ）トラストの 3 つに分類し課題と対策案を整理し、あわせて、それらを実現するための技術について提案を行った。

今後、引き続きクラウドコンピューティング化動向の監視を行うとともに、マーケットに受け入れられる IT リスク低減化対策の検討とその実用化展開を実施していきたいと考えている。

参考文献

１）http://csrc.nist.gov/groups/SNS/cloud-computing/index.html
２）城田真琴「クラウドの衝撃」東洋経済新報社、２００９
３）” Security Guidance for Critical Areas of Focus in Cloud Computing V2.1”, http://www.cloudsecurityalliance.org/csaguide.pdf
４）Tim Mather, Subra Kumaraswamy, Shahed Latif, ”Cloud Security and Privacy”, Oreilly & Associates Inc, 2009
５）浦本直彦「クラウドコンピューティングにおけるセキュリティとコンプライアンス」情報処理、vol.50、No.11、pp1099-1105、Nov.2009
６）佐々木良一，「IT リスクの考え方」岩波新書，2008
７）総務省「ＡＳＰ・ＳａａＳの情報セキュリティ対策に関する研究会報告書（平成 19 年度）」平成 20 年
８）桜井裕唯、芦野佑樹、上原哲太郎、吉浦裕、佐々木良一「大容量耐タンパ装置 HiGATE の試作と e-Discovery への適用」ＣＳＳ２００９