

教育機関における クラウドコンピューティングの活用

株式会社 アーツ情報システム 山内 雄司

経営学部 教授 小松原 実

1. クラウドコンピューティングの概要

クラウドコンピューティングとは、インターネット上に用意されたネットワークインフラ、サーバー、記憶領域、アプリケーション、その他のサービスなどの共有されたコンピュータリソースを、ユーザーの管理運用コスト負担およびプロバイダーの介在を最小限にしつつ、ネットワークを通じて必要なときに利用することができるというサービス形態を表す言葉である。近年のハードウェア技術の進歩により、物理的な実体であるコンピュータハードウェア上に複数のプラットフォームを仮想的に設けてそれらを別々に利用していくというハードウェア仮想化技術が普及しつつある。こうした仮想化によるコンピュータ資源の利用技術がクラウドコンピューティングを急速に発展・普及させつつある。

クラウドコンピューティングでは、通常はインターネット上に存在しているサーバーにアプリケーションソフトウェアを置き、必要な処理を行なわせる。すなわちユーザーは目の前にあるパーソナルコンピュータ(PC)やあるいは組織内のサーバーを用いて作業を行なうのではなく、インターネット上のサーバーを使って処理を行なうことになる。処理可能な作業の内容は多岐にわたり、顧客管理といった業務アプリケーション、メール・サービス、ファイルを保存するストレージ・サービス、文書作成(ワープロ)や表計算といったものなど、クラウドコンピューティングサービスはさまざまなものがすでに提供されている。特に文書作成や表計算は従来はパーソナルコンピュータで行なうことが当たり前であったのだが、こういったものまでも置き換えようという勢いである。

インターネットを図で表現する場合、雲(cloud)の図を使用する場合がよくある。インターネット上で通信によりデータをやりとりする際には、多くのネットワーク機器の間を経由していくが、どのような経路をとっているかを意識することは通常はなく、中は見えず全体がぼんやりと把握できる“雲”で表現する。クラウドコンピューティングという名称は、実行すべき処理を、このインターネットの中のどこかに存在するサーバーに任せることのイメージから付けられたものである(図1)。

クラウドコンピューティングにおいては、一般的には専用のクライアントソフトは使わず、Webブラウザ上から操作を行う。したがってユーザー側で必要なのはインターネットに接続しWebを表示する機能だけとなり、PCからだけでなく、携帯電話のWebブラウジング機能を用いることでも同じように利用できる。

クラウドコンピューティングサービスの提供の形態としては、アプリケーションを提供するSaaS(Software as a Service)、アプリケーションを動かすためのプラットフォームを提供するPaaS(Platform as a Service)、仮想ハードウェアとオペレーティングシステムを提供するIaaS(Infrastructure as a Service)、仮想ハードウェアのみを提供するHaaS(Hardware as a Service)といつたものがある。

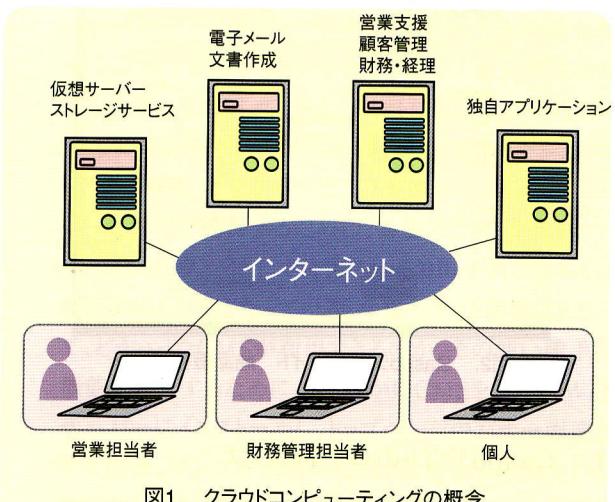


図1. クラウドコンピューティングの概念

2. クラウドコンピューティングとセキュリティ

学びing株式会社が2009年に行った「第2回クラウドコンピューティング意識調査」では、「クラウドコンピューティングで不安な要素は何か?」との問い合わせに対する回答として、圧倒的に多かったのは70.97%の「セキュリティ」というものであった。2番目に多い回答は「回線速度」であったが、これは29.03%であり、クラウドコンピューティング関連のセミナーなどに参加するようなクラウドコンピューティングに関心のあるユーザーが持つ不安要素としては、セキュリティ面が圧倒的であることがわかる。

セキュリティリスクとして検討されるべき点としては、具体的には次のような項目が考えられる。まず、ハードウェア面からは、分散コンピューティング環境を支えているコンピュータ、メモリ、ストレージ、ネットワーク、地政学的リスクといった点がある。クラウドの統制・マネジメント面からはシステムおよび業務監査適正化があり、運用・オペレーション面からはオペレータや保守要員のアクセス管理、データ／プロセスの隔離などのリスク検討事項がある。運用・オペレーション面からはバージョン管理や脆弱性対策がある。そして利活用面では、端末のセキュリティ、通信路のセキュリティ、データポータビリティのリスク

などがある。具体的にいくつかの面から、セキュリティを確保するために求められる事項を以下に挙げる。

(1) ベンダー従業員によるアクセスの管理

クラウドコンピューティングにより外部で管理されるデータは、通常の社内システムでは有効な管理ポリシーの適用を受けない状態となるというリスクを持っている。ベンダー側の従業員の情報を把握することも必要な場合があるかもしれない。またデータへのアクセス権限を持つベンダーの管理者らに対するアクセス監視が求められる。

(2) コンプライアンス

データの安全性と完全性については外部監査や安全性チェックを受ける必要も考えられる。

(3) データ保管に関する管理、隔離

データの保管に関して明確な手続きが定められ、その実施には実効性がなければならない。クラウドシステムを共有している他の顧客のデータとの隔離は適切に行われるのか。暗号化処理は適切であることを確認する。

(4) データの保全と復旧

データ保管場所などで災害が起こった場合のデータおよびサービスの保全、復旧について具体的な方策が立てられていないければならない。データやアプリケーションの多重化を行っていないと顧客は致命的なダメージを受ける恐れもある。また復旧までの時間なども定められているべきである。

(5) 調査に対する協力姿勢

不適切な処理や違法行為の調査のための体制の確立と調査協力の確保が得られるよう契約などで定める。

(6) 事業継続性

倒産や買収される可能性は低いほうが多いのはもちろんである。仮にそうした事態が発生した場合にはデータの保全やサービスの継続が受けられるような準備が必要である。また他のベンダーに移行する場合のデータの回収方法、フォーマットの移植性について確認しておく。

3. 教育機関におけるクラウドコンピューティングの利用

前項にあげたようなセキュリティに関する留意事項は、クラウドコンピューティングの利用にあたって、一般的に考慮されねばならない事項であるが、教育機関においてはクラウドコンピューティング利用では、特に検討しておかねばならない部分も存在する。そこで本研究では、「SaaSとセキュリティの両立」をテーマに、次の2点を研究テーマとして検証を行うこととしている。

- ①公的機関等がユーザーとしてクラウドコンピューティングを利用促進するための前提条件を明確化する。
- ②事業者側が解消すべき、制度面・技術面・運用面の各分野における課題の洗い出しを行う。

本研究を通じて明確にしたい技術的課題は以下のようない項目である。

● 実際に事業者が保有する個人情報の精査

事業者はどこまでの機密情報を保有しなければならないか。

機密情報に該当するデータを保有する場合、どのレベルまでの対策が必要か。

● リンク情報の精査

プライバシーを考慮したアカウントのリンクが行われているのか。

各サービス事業者が知り得ない情報を共有していないことを証明できるか。

● SASS70 Type II のボリュームの精査

利用者・事業者共に必要な監査証跡が取れるか。

こうした課題を実証実験により解明していくために、1次検証としてユーザー単位での利用環境を構築し、この実証実験環境内で、制度的課題の検証、ユーザーの意見収集、監査内容検証を実施していく。実装検証のイメージを図2に示す。

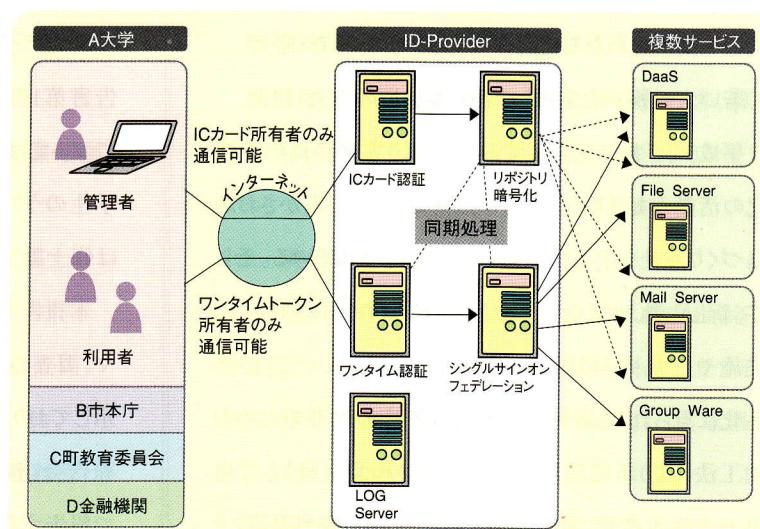


図2. 大学におけるクラウド・コンピューティング実装イメージ