クラウドコンピューティング環境における セキュリティ上の課題と対策

Security Issues and Countermeasures in Cloud Computing Environment

山　田　英　孝

要　約　2010 年現在，クラウドコンピューティングは，システムの新規導入や更新を検討している企業から注目を集めている技術のひとつである．その利便性，コスト削減効果が脚光を浴びており，企業の情報システムは内製から SaaS 化・クラウド化へと進んでいく方向にある．しかしながら，情報セキュリティ対策の実施状況について不安を抱くユーザ企業は少なくない．クラウドコンピューティング環境における情報セキュリティ対策の技術や体制にベストプラクティスが存在しないのが現状であるからだ．よって，情報セキュリティ対策はサービス提供者側，利用者側の双方にとって非常に重要な課題である．

クラウドコンピューティング環境において，どのような脅威，リスクが存在するのか，サービス利用者側とサービス提供者（プロバイダ）側，各々の視点から課題や内在する問題を整理し，サービス提供者（プロバイダ）として取り組むべき情報セキュリティ対策について考察する．

Abstract　Nowadays, the cloud computing is one of trendy technologies attracting the attention of enterprises which study to introduce new systems or restructure their current systems. Cloud computing services provide the benefit of excellent utilization and IT budget reduction. In general, enterprise IT systems are in state of change from ‘on-premise’ to SaaS or ‘clouds’ in progress. However, some prospective users do not have much confidence in the implementation of the information security measures for the cloud computing services, and the best practice of the information security measures has not be defined yet. Therefore, it is the very important challenge to specify the proper information security measures for cloud computing service providers and users.

In this paper, we clarify what kind of threats and risks exist in cloud computing and analyze security concerns and undiscovered issues from the viewpoint each of cloud computing service providers and users. Additionally, we discuss the secure items which any cloud computing provider should consider.

1. は　じ　め　に

これまで，ユーザ（企業，個人など）が，コンピュータのハードウェアやソフトウェア，データなどを所有した場合，購入費用や運用・管理などのメンテナンスにかかるコストなどがユーザにとって大きな負担となっていた．これに対し，クラウドコンピューティング環境においては，必要な時に必要なリソースやサービスを，ネットワーク経由で利用することが可能である．2010 年現在，情報システムに対するニーズは，「所有」から「利用」に変化してきており，これを実現するクラウドコンピューティングサービスが注目を浴びている．

クラウドコンピューティングの特筆すべきメリットとして，三つ挙げられる．一つ目はシステムの柔軟性である．必要な時に必要なリソースやサービスをネットワーク経由で利用するこ

とができ，拡張も容易である．二つ目は導入の容易さである．必要なリソースやサービスをすばやく提供・利用することが可能である．三つ目は購入するためのコストや運用・維持管理などのメンテナンス費用を削減可能なことである．

一方で，サービス提供者側の運用や維持管理の実態がサービス利用者（以降，ユーザとも呼称する）側に見えにくく，特に情報セキュリティに関して不安を抱くユーザも多い．このようなユーザの不安を解消しサービスを提供することが，サービス提供者が競争に生き残っていくための重要な課題である．

本稿ではこのようなクラウドコンピューティング環境における情報セキュリティ課題を追求し，対策の手法を提示する．

2. クラウドコンピューティングにおけるサービス提供モデル

クラウドコンピューティングとは，従来ユーザが保有していたハードウェアやソフトウェア，アプリケーションなどを，インターネットなどネットワークを通じて利用する利用形態のことである．イメージ図でインターネットを雲（cloud：クラウド）のように図示することから，このように呼ばれている．これまでにも提供されていたASP（Application Service Provider）のサービス（以降，単にASPと呼ぶ）と類似しているので，本章では，これらのサービスモデルの相違点について考察する．

総務省「ASP・SaaSの普及促進策に関する調査研究」[1]において，ASPと類似の用語として「ユーティリティコンピューティング」,「オンデマンドコンピューティング」,「SaaS（Software as a Service）」などが存在するが，ほとんどASPと同一の意味で使用されていると定義されている．しかしながら，これまでのサービスと異なり，「クラウドコンピューティング」はユーザに受け入れられている．その最大の要因として，アプリケーションの操作性向上が挙げられる．インターネット環境の整備によるネットワーク接続の高速化により，インターネットを介してもストレスを感じることなくアプリケーションを利用できるようになった．また，安価にサービスを提供，利用できるようになったことも要因のひとつである．これまでのサービスにおいては，1サービス，1ユーザといった「シングルテナント」でのサービス提供が主であったのに対し，クラウドコンピューティングにおいては，1サービス，多ユーザといった「マルチテナント」でのサービス提供を実現している．さらに，クラウドコンピューティングによって，ユーザの利便性が高まったことも挙げられる．これまで提供されていたサービスの多くでは，パッケージソフトウェアをインターネット越しに利用していたのに対し，クラウドコンピューティングは，ユーザが自由に変更，修正，利用できることを目的としていることで，ユーザの利便性が高まり，付加価値の高いサービスを提供，利用することが可能となった．これらの要因により，これまでの類似したサービスに比べ，クラウドコンピューティングに注目が集まり，ユーザが拡大している．

こうしたクラウドコンピューティングのサービスモデルは，三つに分類することが多い．まず一つ目は，SaaSと呼ばれている，ソフトウェア（主にアプリケーションソフトウェア）をインターネット経由のサービスとして提供・利用する形態である．二つ目は，PaaS（Platform as a Service）と呼ばれる，アプリケーションソフトが稼働するためのハードウェアやOSなどの基盤（プラットフォーム）を，インターネット経由のサービスとして提供・利用する形態である．三つ目は，IaaS（Infrastructure as a Service）である．IaaSとは，コンピュータシ

ステムを構築，稼働させるためのハードウェアやネットワークなどのインフラストラクチャーを仮想マシンとしてインターネットを通じてサービスとして提供・利用する形態のことである．ハードウェアをインターネット経由のサービスとして提供・利用する形態であることからHaaS（Hardware as a Service）と呼ばれることもある．

また，Amazon Web Services（AWS）やGoogle Appsに代表されるような，申請すれば誰でも即座にインターネット経由でサービスを利用することが可能なパブリッククラウド，自社でインフラを用意し，不特定多数にサービスを公開せず，社内の各部門が必要な時にサービスを利用するプライベートクラウド，その両方を活用するハイブリッドクラウドというように，サービス提供・利用形態により分類することもある．

3.　クラウドコンピューティング環境における情報セキュリティの課題

自社システムをSaaS化，クラウド化することのメリットは，必要なリソースを必要なときに，必要なだけ利用できるため，ユーザの利便性が高いことである，また，ネットワーク上のサーバ，ネットワーク機器に関する専門的な知識，保守/運用管理も不要になることから，コストを削減できるということも大きなメリットのひとつである．

しかし，見過ごすことのできないデメリットも少なくない．クラウドコンピューティング環境における情報セキュリティに関しては，今日もベストプラクティスの確立に向け，試行錯誤が重ねられている．本章では，サービス利用者，サービス提供者のそれぞれの視点から，課題を分析する．

3.1　サービス利用者側からの視点

クラウドコンピューティングという名前にあるように，ユーザ側からはクラウドの先，つまりサービス提供者側の技術や運用・管理の実態については見えない．たとえば，ユーザが利用しているシステムに対して不正アクセスがないか調査する場合を考える．マルチテナントの場合，他社の機密情報も含まれる可能性があるため，アクセス履歴を入手することは困難である．そのため，不正アクセスを把握することができない．ユーザにとって管理をしなくても良いという反面，どのように管理されているのかわからないという不安がつきまとうことになる．こうした運用・管理の実態の不透明さも課題のひとつである．

また，自システムのデータの管理，バックアップ，復旧についてサービス提供者側次第であることも非常に重要な問題である．サービス提供者側の障害により，自システムの利用停止，データの損失，情報漏えいなどが発生する可能性もある．

このように，システムへのアクセス状況を把握するためのアクセスログであったり，監査の際に必要なデータであったり，自システムのデータであったとしても，クラウドコンピューティング環境においては，それらのデータへのアクセスが制限される可能性がある．さらに，海外に自システムのデータが保管されている場合，保管されている国や地域の法律が適用されるということも認識しなければならない．

3.2　サービス提供者側からの視点

サービス提供者が考慮すべき問題点として，システムの柔軟性，拡張性，可用性，堅牢性，継続性があげられる．例えば，ネットワーク障害やシステム障害時の対策について考える．ユ

ーザの重要なシステムがインターネットを介した場所に設置されるため，もしシステムに接続することができなくなり，業務が行えなくなった場合，ユーザにとって大きな損失につながる可能性がある．そのため，サービス提供者にとって，可用性，継続性の問題は重大である．

次に，クラウドコンピューティングサービスを複数のベンダによって提供している場合について考える．図1に示すクラウド環境は，二つのクラウドコンピューティングサービスベンダが共同でサービスを提供する場合のシステム構成例である．この例では，アプリケーションとミドルウェア部分をアプリケーションベンダが，仮想OS以下のシステム基盤をシステム基盤ベンダが，それぞれサービス提供していることを想定している．

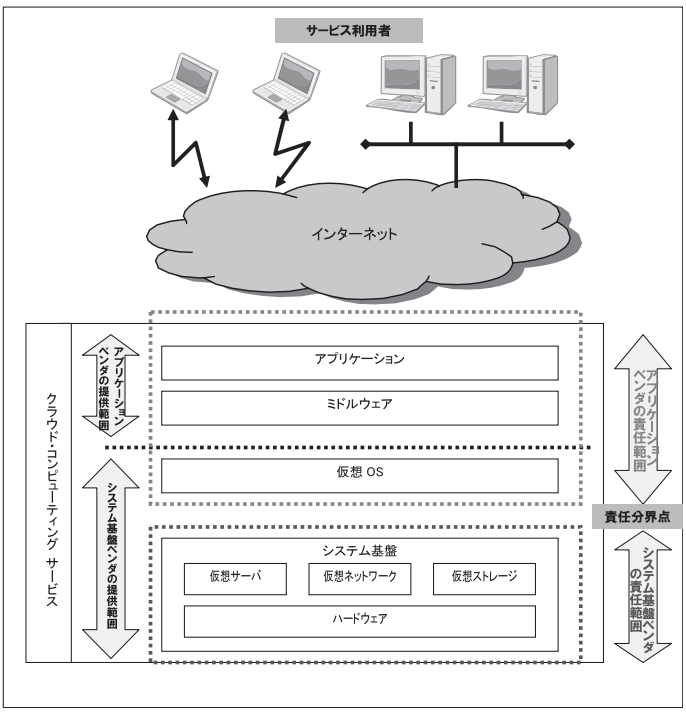

図1　クラウド環境のシステム構成

この構成において留意すべき点は，仮想OSの部分である．仮想OSは，システム基盤ベンダより提供されるが，アカウント管理，修正パッチの適用，障害監視等の責任はアプリケーションベンダにある．このようにクラウドコンピューティング環境では，提供範囲と責任範囲が必ずしも一致しないため，責任分解点が曖昧になりやすいという課題が挙げられる．

また，ユーザ企業の内部統制への対応においては，サービス提供者は重要データへのアクセスログ，アプリケーションログ，特権ユーザログなどを提供する必要があるが，どのように，どの程度提供するのか，といったコンプライアンスの課題も挙げられる．

さらに，これまで存在しなかった新たな問題も考えられる．例えば，SaaS化・クラウド化におけるサーバの仮想化には，仮想化環境内でのウィルスの拡散などの新たな問題点が考えられる．攻撃を受けた仮想サーバが，同じ物理サーバ上のすべての仮想サーバを感染させる可能性がある．そして，一つのゲスト仮想サーバから，同じ物理サーバ上にある他の仮想サーバに攻撃が移っていくことが，仮想化環境での最大のセキュリティリスクとなる．

もし，仮想サーバを狙った攻撃手法を簡単に入手できるようになれば，一つの仮想サーバを攻撃し，成功すれば，そこから他の仮想サーバを攻撃し，最終的には物理サーバにアクセスするということが考えられる．逆に，物理サーバを攻撃し，成功すれば，その環境上の仮想サーバすべてにアクセスすることが可能となることも考えられる．そのため，一つのハードウェア上で複数の仮想サーバが動作している大規模な仮想化プラットフォームでは，特に注意が必要となる．

加えて，仮想化環境においては，物理サーバに対してセキュリティパッチを適用する必要がある．しかし，その際，すべての仮想サーバをシャットダウン，もしくは再起動させなくてはならないという問題がある．仮想化技術は，必要なときに必要なだけ，かつ短期間にリソースを提供するというクラウドコンピューティングを実現するための要素技術であるだけでなく，リソースの余剰を削減して利用効率を上げ，消費電力や設置面積を削減してグリーン IT を推進するといった，今後の IT 環境における重要な技術である反面，新たな課題も多い．

4.　課題と対策

総務省からクラウドコンピューティングサービスを提供する企業向けに「ASP・SaaS における情報セキュリティ対策ガイドライン」[2]が発行されているが，セキュリティの基本原則は情報の機密性，完全性，可用性であり，これはクラウドコンピューティング環境においても例外ではない．Cloud Security Alliance が公開している Security Guidance for Critical Areas of Focus in Cloud Computing[3]では，サービス提供にあたり，クラウドコンピューティングアーキテクチャとフレームワーク，ガバナンス，運用・管理方法の課題という三つの観点から対策を述べている．

4. 1　課題の分類

3 章において，サービス利用者側，サービス提供者側，それぞれの視点からクラウドコンピューティングにおける課題や問題点を列挙した．3 章の課題を各種ガイドラインに照らし合わせると，以下のように大きく三つに分類することができる．これらを認識し，それぞれ対策を実施しなくてはならない．

1）　コンプライアンスにおける課題
2）　ガバナンスにおける課題
3）　技術面における課題

4. 2　取り組むべき対策

SaaS，PaaS，IaaS といえども，言い換えるとアウトソーシングサービスである．クラウドコンピューティングにおける課題や問題点の対策を実施する前に，サービス提供者は想定される最も厳しい顧客要件をベースラインとして対策を検討しなければならない．また，サービス利用者は自社で運用する場合のセキュリティ対策やセキュリティレベルと比較し，運用コストのバランスを考慮して，システムのクラウド化/SaaS 化を検討する必要がある．これらを踏まえた上で，4. 1 節の三つの課題に対応する情報セキュリティ対策を列挙する．

1） コンプライアンスにおける対策
- ・「情報セキュリティに関する基本的な方針」を定める
- ・最高情報責任者などの職務機能を持つ代表者を定める
- ・連携 ASP・SaaS 事業者から ASP・SaaS サービスの提供を受ける場合には，契約や SLA を締結する
- ・情報資産へのアクセスを管理・制限する
- ・個人情報，機密情報，知的財産等については，適切な情報セキュリティ対策を実施する
- ・一元的なユーザサポートを実施する

2） ガバナンスにおける対策
- ・取り扱う各情報資産について，管理責任者，およびその利用範囲を明確にし，文書化する
- ・情報資産の価値，法的要求に基づき，情報資産を分類する
- ・情報システムに対して，定期的に点検・監査を実施する

3） 技術面における対策
- ・個人認証システムによる物理アクセス制御を実施し，入退出記録を一定期間適切に保管する
- ・情報システムに対して，稼働監視，障害監視，およびパフォーマンス監視を実施する
- ・脆弱性，および情報セキュリティインシデント（サービス停止，情報の漏えい・改ざん・破壊・紛失，ウィルス感染等）に対する記録方法，報告手順を定め，実施する
- ・情報システムに対する脆弱性情報の定期的な収集とパッチの適用を実施する
- ・利用状況，例外処理及び情報セキュリティ事象のログを取得し，一定期間適切に保管する
- ・情報システムに対して，ウィルス対策を実施する
- ・データベース内のデータの暗号化を実施する
- ・情報システムに対して，定期的なバックアップを取得する
- ・情報システムに対して，適切なアクセス制御を実施する
- ・情報システム管理者及びネットワーク管理者の権限の割当，および使用を制限する
- ・利用者及び管理者に対して，適切な認証方法によるアクセス制御を実施する
- ・外部，および内部からの不正アクセス対策を実施する
- ・送受信中のデータを保護するため，通信の暗号化を実施する
- ・情報処理施設に対して，災害対策を実施する
- ・運用管理端末を適切に管理する
- ・仮想サーバに対して，パッチ適用等の適切なセキュリティ対策を実施する

以上のように，これまでのセキュリティ対策とほとんど変わらない．しかしながら，これまで存在しなかった次のような課題についても検討する必要がある．

一つ目は，個々のユーザの要求に応じて日々の運用状況やデータの安全性を提示できる体制を整えることである．特に管理者権限のユーザの使用に対する統制と管理者権限やシステム全体の利用状況・統制状況を把握することが重要である．

二つ目は，クラウドコンピューティング環境では共有資源を利用するため，特にデータや各

環境へのアクセスを管理することである．これまでのネットワーク環境と異なり，クラウドコンピューティングでは，サービスを提供する側にデータが集中するため，内部からの不正アクセスに対するアクセス監視は必須の対策である．

三つ目は，仮想マシンに対するパッチ適用等，サーバの設定，要塞化も重要となることである．現在，システムのクラウド化に欠かせないといわれている仮想化技術において，セキュリティ技術に関しては，実装検討段階といえる．最も重要なことは，仮想 OS からホスト OS に侵入できない，仮想 OS から他の仮想 OS に侵入できないことを担保することである．つまり仮想化でのセキュリティとは，適切なアクセス制御によって，これまでの物理サーバと同等のセキュリティレベルを確保することである．

四つ目は，多くのサービス利用者が利用する DNS サーバ，メールサーバといったシステムについては，これまで以上にキャッシュポイズニングやメールリレーに対する対策を実施しなければならないことである．

五つ目は，セキュアプログラミングによる，アクセス制御対策，セッション対策，暴露対策，入力対策，エコーバック対策が，これまで同様必要なのに加えて，通信の暗号化，マルチテナント環境の個々のユーザデータに対するアクセス制御について，これまで以上に注意しなければならないことである．

5. 今後の課題

マルチテナント環境におけるインシデント分析や特定の顧客のインシデントに対応するため，アプリケーションレベルでログを取得し，アプリケーション毎に所有者情報を取得する必要がある．しかしながら，クラウド環境におけるログ管理については，これまでの企業内でのログ管理と同じで良いのか検討が必要である．また，仮想化環境においては，まだ仮想化技術が初期段階であるため，2010 年 2 月時点でセキュリティホールは報告されていないが，クラウドコンピューティングが注目され，仮想化技術が発展することで，新たなセキュリティホールが発見される可能性がある．これらに対して迅速に対処する必要がある．仮想化環境においては，複数台の仮想サーバが物理サーバに集約されているため，物理サーバと仮想サーバ，および，仮想サーバ間の通信の監視や管理も必要になると考えられる．

クラウドコンピューティング，ICT サービスがこれから成長していくためには，多くのセキュリティ問題を解決し，拡張可能で柔軟な IT 機能を，サービスとして安全に提供しなければならない．また，今後はセキュリティの問題だけでなく，必要な時に必要なだけ利用できるというクラウド/SaaS のメリットを最大限に活かせるソフトウェアのライセンス体系の確立なども検討しなければならない．

6. お　わ　り　に

1990 年代以降，多くの企業において IT 技術の導入が促進されてきた．同時に情報漏洩事故などにより総合的な情報セキュリティリティ対策が必要となってきた．クラウドコンピューティングも 2008 年後半から注目を浴びはじめ，導入が促進されてきている．しかしながら，クラウドを利用することによるコスト削減という部分のみが注目され，問題発生時の対策，対応については，技術的にもサービス的にも十分議論されていない．クラウドコンピューティング環境下においても，今後セキュリティ問題が表面化してくると思われる．セキュリティ面に注

目しつつ，効果的かつ継続的に運用しサービスを提供する，クラウドコンピューティング環境下におけるセキュリティアーキテクチャの確立が必要である．

本稿の内容が，システムのクラウド化を検討している企業，クラウドコンピューティングサービスを提供している企業のお役に立てば幸いである．

参考文献
［1］「ASP・SaaSの普及促進策に関する調査研究」，総務省，2007年4月，http://www.soumu.go.jp/menu_news/s-news/2007/pdf/070427_14_bt.pdf
［2］「ASP・SaaSにおける情報セキュリティ対策ガイドライン」，総務省，2008年1月，http://www.soumu.go.jp/menu_news/s-news/2008/pdf/080130_3_bt3.pdf
［3］ Security Guidance for Critical Areas of Focus in Cloud Computing V2.1, Cloud Security Alliance, 2009.12, http://www.cloudsecurityalliance.org/csaguide.pdf
［4］ Cloud Security Alliance，馬場達也，独立行政法人 情報処理推進機構 セキュリティセンター，2009年9月，http://www.ipa.go.jp/security/fy21/reports/tech1-tg/a_09.html
［5］ ASP・SaaSインダストリ・コンソーシアム（ASPIC），http://www.aspicjapan.org/index.html
［6］「ASP・SaaSの普及促進策に関する調査研究」，ASPIC JAPAN，総務省，2007年4月，http://www.soumu.go.jp/menu_news/s-news/2007/pdf/070427_14_bt.pdf
［7］「セキュアプログラミング講座」，独立行政法人 情報処理推進機構 セキュリティセンター，2007年 http://www.ipa.go.jp/security/awareness/vendor/programmingv2/index.html
［8］ ビル・ブレナー，「SaaS/クラウドで求められるセキュリティ対策とは？」，Computerworld，（株）IDGインタラクティブ，2010年2月1日，p.26-31.
［9］ ルーカス・ミーリアン，「SaaS/クラウドのデータ管理に取り組む」，Computerworld，（株）IDGインタラクティブ，2010年2月1日，p.32-33.
［10］ ケビン・フォガティ，「レガシー・アプリケーションのSaaS/クラウド化を妨げる5つの壁」，Computerworld，（株）IDGインタラクティブ，2010年2月1日，p.34-36.
［11］ ゲイリー・ハミルトン，「SaaS/クラウド・プロジェクト管理の「課題」と「挑戦」」，Computerworld，（株）IDGインタラクティブ，2010年2月1日，p.37-39.

執筆者紹介 山 田 英 孝（Hidetaka Yamada）

1999年日本ユニシス（株）入社．日本ユニシス実業団バドミントン部選手活動を経て，2006年ユニアデックス株式会社へ出向．セキュリティソリューションの構築，保守，脆弱性検査を担当．2009年より現在の共通利用技術部ミドルウェア技術室にて脆弱性検査業務を担当．

2000年シドニーオリンピック，2004年アテネオリンピック，バドミントン日本代表．最高世界ランキング10位．