



[小特集] クラウド・セキュリティ

1. クラウドコンピューティングのリスクとガバナンスに関する調査・研究について
2. IaaS 型クラウドにおける仮想マシンのセキュリティ課題
3. クラウドにおけるアイデンティティ管理の課題
4. クラウドセキュリティアライアンスとその活動について

編集にあたって

吉濱佐知子 日本アイ・ビー・エム(株) 東京基礎研究所



クラウドコンピューティング(以下クラウド)は、ITの機能をネットワーク経由でサービスとして提供するコンピューティングモデルである。クラウドは計算機資源の使用量によって課金するモデルであるため、初期導入費用が不要であるとともに、組織内のIT管理やメンテナンスのコストを削減できるという効果が期待されている。また、導入にかかる期間も大幅に短縮することができるため、新しいサービスを開始するときや一時的に多量の処理を行う必要があるときに、必要に応じた計算機資源をすばやく確保し、ビジネス規模の変化に伴って使用量とコストを柔軟に調整することが可能になるといったメリットがある。

一方で、クラウドサービスプロバイダ(CSP)の提供するサービスを利用することによる懸念、特にセキュリティやガバナンスに関する懸念を持つ組織も多くあり、クラウド導入の主要な阻害要因となっている。本小特集では、2009年11月号のクラウドコンピューティング特集で概略の示されたセキュリティやコンプライアンス上の問題^{☆1}をさらに掘り下げて、セキュリティ上の問題を考察する。

「クラウドコンピューティングのリスクとガバナンスに関する調査・研究について」では、ENISA^{☆2}が2009年11月に発行したクラウドのセキュリティに関するガイドライン^{☆3}を題材に、クラウドにおける脅威の対象となる情報資産、リスク、関連する脆弱性などを網羅的に概説する。

ENISAは、リスクを1)ポリシーや組織のガバナ

ンスにかかわるリスク、2)技術的なリスク、3)法的なリスク、4)クラウド以外のITシステムにも共通する一般的なリスク、の4つに分類している。このうち技術的なリスクに着目したとき、特にIaaS(Infrastructure as a Service)で使用される仮想化技術により発生し得るリスクが、クラウドにとって最も特徴的なものとして浮かび上がってくる。「IaaS型クラウドにおける仮想マシンのセキュリティ課題」では、仮想化技術の概略とクラウドでの利用の変遷について概説し、仮想マシン環境で発生し得るさまざまな脅威の種類について解説する。

クラウドにメリットがあるとはいっても、現実的にほとんどの企業にとって、すべてのIT環境を一挙にすべてクラウドに移行するということは考えられない。たとえば、ビジネスの根幹にかかわる重要システムは社内で維持管理し、それ以外の比較的軽微なシステム(たとえばグループウェアや顧客管理)だけはSaaS(Software as a Service)を利用する、といったケースが多く発生することが考えられる。このような場合に問題になるのが、社内システムとクラウド、または複数のクラウド間にまたがるアイデンティティ管理の問題である。「クラウドにおけるアイデンティティ管理の課題」では、主にWebアプリケーションの相互連携に用いられるいくつかの技術の概説を行うとともに、クラウド化によりあらためて顕在化するアイデンティティ管理にかかる課題や、将来への展望を述べる。

最後に、「クラウドセキュリティアライアンスとその活動について」では、クラウドのセキュリティのためのベストプラクティスの普及を目指すクラウドセキュリティアライアンス(CSA)の活動を紹介するとともに、2010年6月に発足した日本支部の活動を紹介する。

(平成22年11月1日)

☆1 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, pp.1099-1105 (Nov. 2009).

☆2 European Network and Information Security Agency (欧州ネットワーク情報セキュリティ庁)。

☆3 なお、2010年10月に(独)情報処理推進機構(IPA)によってこのガイドラインの翻訳版が公開された。http://www.ipa.go.jp/security/publications/enisa/