クラウド・コンピューティングの現状と課題
—クラウド・コンピューティングの導入におけるリスクと対策—

城 川 俊 一

目次

1．ICT活用の広がりとクラウドコンピューティングの概要
2．クラウド・コンピューティングの分類と特徴
3．クラウド・コンピューティングの導入におけるリスクと対策
3．1　クラウドコンピューティングのリスクと対策
3．1．1　国内の動向
3．1．2　海外の動向
3．1．3　クラウドコンピューティングの利用者が考慮すべきリスク対策
3．2　国内外のデータセンタを利用する上での法的な検討
4．まとめ
参考文献

1．ICT活用の広がりとクラウドコンピューティングの概要

企業内における顧客情報管理（CRM:Costomer Relation Manegiment)、電子調達、社会サービスにおける電子マネー、個人・家庭における携帯メール、ネットショッピング、SNS、ブログ、e-ラーニング等にクラウド型の新たなサービスが入り込んできつつある。クラウドコンピューティングとは、大幅に拡張可能なコンピューティング環境を、ネットワーク経由でサービスとして利用するクラウドコンピューティング・スタイルであり、企業・個人のクラウド利用環境としては、所有から利用へ、クラウド提供環境としては、スケーラブルかつオンデマンドへと流れが変わった。

米国標準技術研究所［NIST］の定義では、「クラウド・コンピューティングとは、システムを構成する要素（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）がどこかに共有を目的としてプールされており、利用者はネットワークを介して必要なときに容易に使うことができると同時にその「利用量」を変更することができる（つまり、スケーラブル）もの、また、「利用量」の変更時には最小限の管理作業もしくは提供者とのやりとりによって迅速に対応されるもの」となっている。

2．クラウド・コンピューティングの分類と特徴

(1) クラウド・コンピューティングの４つの展開モデル（Deployment Models）

①パブリック・クラウド（Public Clouds）：パブリッククラウドとは、クラウドコンピューティングによって運用されるサービス（クラウドサービス）のうち、一般利用者を対象に提供されるクラウドサービスのことである。

②プライベート・クラウド（Private Clouds）：プライベートクラウドとは、企業が自社内でクラウドコンピューテングのシステムを構築し、企業内の部門やグループ会社などに対してクラウドサービスを提供する形態のことである。

③コミュニティー・クラウド（Community Clouds）：いくつかの組織によって運用されるクラウド。パブリッククラウドのような一定程度の規模やセキュリティを担保しつつ、プライベートクラウドの柔軟性も併せ持つ。

④ハイブリッド・クラウド（Hybrid Clouds）：パブリック・クラウドとプライベートクラウドを組み合わせたクラウドのこと。

Forrester Research社が2011年に行った調査「クラウド コンピューティングに関する意識調査」では、プライベートクラウド、パブリッククラウドといったさまざまなクラウド活用の選択肢がある中で、日本企業の３割以上がハイブリッドクラウドを支持しており、大規模企業ではその割合は５割以上になるという結果が出ている（Forrester Research社［2011］）。

その理由として、何もかもをクラウドに載せるのでなく、可用性やセキュリティ、プライバシーなどシステムやデータの性質を考慮し、特定のシステムについてはパブリック・クラウドを利用しない判断をすることも十分にあり得る。例えば、金融システムの中には数分間停止しただけで数百億円の損失が出るものもある。それをパブリック・クラウドに載せる必然性はない。事業者にとっても、そうした要件を満たす基盤を作るのは割に合わない仕事である。

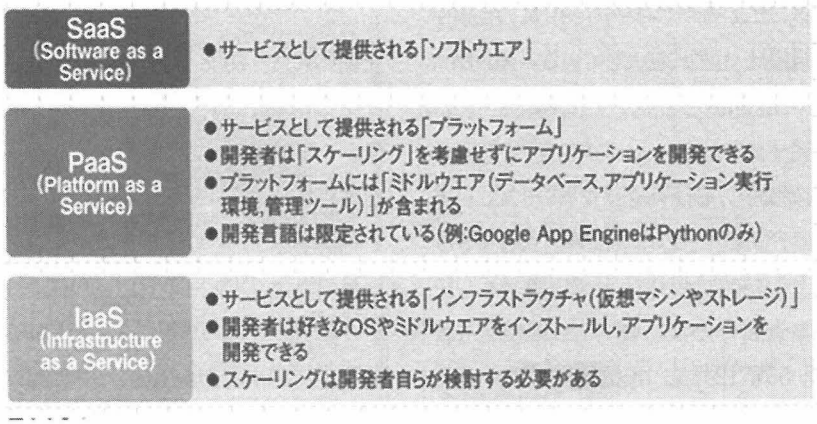
そのような場合の選択肢がプライベートクラウドである。一方、パブリック・クラウドを利用する場合、クラウド事業者のデータセンターの運用方法は、明らかに一般企業のそれよりも優れているからである。つまり、ハイブリッド・クラウドが企業の取るべき戦略であるといえる。

(2) クラウドコンピューティングの３つのサービスモデル（Service Models）

2012年５月８日に発表されたIDC Japanの国内パブリッククラウドサービス市場の予測によると、2011年の国内パブリッククラウドサービス市場規模は前年比45.9％増の662億円となる見込みである。国内パブリッククラウドサービス市場は拡大を続け、2016年の同市場規模は、2011年比5.2倍の3,412億円になるとIDCは予測している。

2011年の国内パブリッククラウドサービス市場は、同サービスを本格的に提供するベンダーが増加すると共に、サービス内容の拡充が急速に進んだ。なかでも、クラウドプラットフォーム（PaaS:

図表１　３つのサービスモデル



出典：ITpro Magazine [2008], p.24.の図２.

Platform as a Service)、クラウドインフラストラクチャ（IaaS: Infrastructure as a Service）および産業特化型SaaS（Software as a Service）は著しく発展した。また、パートナーエコシステムも充実が見られた。2012年以降の国内パブリッククラウドサービス市場は、市場規模の拡大に伴い2012年をピークとして前年比成長率が低下していくものの、高い成長を継続するとみられる。なかでも、インフラストラクチャとアプリケーションプラットフォームが「密結合」から「疎結合」へと変わる次世代サービスアーキテクチャに基づくPaaSが本格的に発展し、同市場の成長を促進する。国内PaaS市場は、2015年に1,000億円規模を超え、国内パブリッククラウドサービス市場において、最大規模のセグメントになるとIDCは予測される（IDC Japan［2011］）。

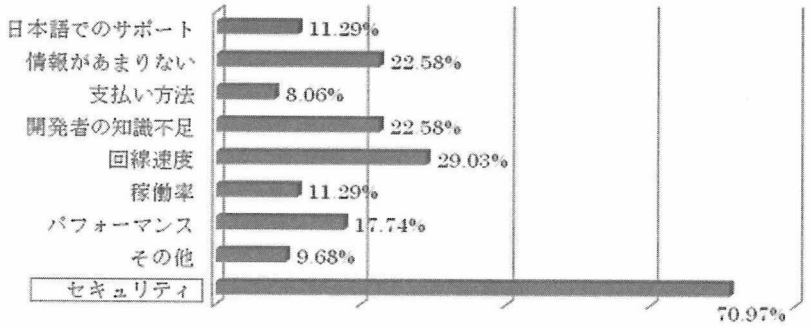
３．クラウド・コンピューティングの導入におけるリスクと対策

昨今、東日本大震災の影響から、国内において事業継続（BCP：Business Continuity Plan）の強化策としてクラウド・コンピューティングの需要が急激に増加している。また、今後海外進出を加速させる日本企業にとって、システムを迅速に展開するにはクラウドが欠かせないとの認識がある。伊藤忠ITRが2012年６月、従業員500名以上の日本企業を対象に行った調査の結果を見ても、クラウドサービスを積極的に活用していくべきだと考える企業は77.8％と全体の４分の３を超える。しかし、現状では、多くの企業が本格導入に至っていないのが実情だ。クラウドのメリットを感じながらも、移行への懸念／不安を持っており、二の足を踏んでいる企業が多い。その理由の背景としては、以下のことが考えられる。

最近の事例でも、Amazon社Amazon Web Serviceのシステム障害による停止（2011年４月）（Amazon［2011］）なども発生し、多くの企業・利用者に影響が及ぶ等、クラウド・コンピューティ

ングならではの問題も発生している。また、現在のウイルスの発生速度は、1.5秒に１つウイルスが作成されている状況（亜種等も含む）といわれている。標的型攻撃の危険性も叫ばれている今、図表２に示すように、企業におけるセキュリティ対策が重要性を増している。この論文では、今後、ビジネスシーンにおけるクラウド・コンピューティングの位置づけは非常に重要なものとなっていくことが予測されることから、クラウドコンピューティングを安全に活用できるよう、そのリスクと対策について考えてみたい。

図表２　クラウドの不安な要素



出典：学び ing 株式会社：第２回クラウドコンピューティング意識調査　2009

３．１　クラウドコンピューティングのリスクと対策

３．１．１　国内の動向

クラウドコンピューティングでは、クラウド独自の特性に応じたセキュリティ対策が必要となっている。クラウドの普及が進む中、公的機関・業界団体などがクラウドセキュリティに関する各種のガイドラインを策定している（図表３参照）。

図表３　国内の主なクラウドセキュリティー対策ガイドライン
（公的機関・業界団体などからガイドラインが提示されている。）

発行省庁	ガイドライン	対象範囲		特徴	備考
		利用対象	適用対象		
総務省	ASP・SaaSにおける情報セキュリティ対策ガイドライン	クラウドサービス事業者	SaaS（ASP）	・ASP/SaaSに焦点 ・ISO/IEC 27002を参考	事業者の情報公開に関する認定制度
経済産業省	クラウドサービス利用のための情報セキュリティマネジメントガイドライン	クラウドサービス事業者（事業者への要望事項を含む）	クラウドサービス全般	・ISO/IEC 27002をベース ・利用者向け：手引き事項 ・事業者向け：要望事項	ISO/IEC 27000シリーズに日本から提案
内閣官房情報セキュリティセンター（NISC）	政府機関の情報セキュリティ対策のための統一基準群（管理基準，技術基準）	政府機関担当者，官公庁調達担当者など	政府機関担当者	・官公庁共通の情報セキュリティ対策の統一基準	2011年版からクラウド利用の観点が追加

注：略語説明　ASP（Application Service Provider），SaaS（Software as a Service），NISC（National Information Security Center）

総務省による「ASP（Application Service Provider）・SaaS（Software as a Service）における情報セキュリティ対策ガイドライン」は、安全性・信頼性に対する事業者の情報開示を促進することを目的としている。一般財団法人マルチメディア振興センターは、このガイドラインなどを根拠として「ASP・SaaS安全・信頼性に係る情報開示認定制度」を運用している。この認定制度では、事業者やサービスの安全・信頼性に関する情報について開示項目を規定している。外部システムの利用に関し、利用者がその評価を可能とすることを目的とした制度と言える。経済産業省が策定した「クラウドサービス利用のための情報セキュリティマネジメントガイドライン」では、利用者向け手引き事項、事業者向け要望事項を中心としつつ、事業者が対応すべき要望事項が整理されている。このガイドラインは、情報セキュリティ規格群ISO/IEC 27000シリーズでの標準化に向けて日本から提案され、現在、標準化作業が進められている。双方のガイドラインに共通する点は、ISO/IEC 27002を基本に、クラウドの特性に応じた管理策の応用を行っていることにある。主な観点として次の三つが挙げられる。

① 事業者から利用者へのセキュリティ対策情報の開示

② セキュリティ対策責任分担の明確化

③ 利用者資産や利用サービス状況の利用者への可視化

官公庁調達事案では、以前から内閣官房情報セキュリティセンター（NISC：National Information Security Center）が政府機関の情報セキュリティを全体的・共通的に向上するために「政府機関の情報セキュリティ対策のための統一基準群（管理基準、技術基準）」を発行している。クラウド利用の要件として、最近の改訂で以下の項目などが加えられた。

① 海外のデータセンターに情報を保存する場合の留意点

② 事業者間の管理責任範囲の明確化

3．1．2　海外の動向

海外でのクラウドセキュリティに関する動向としては、米国に本拠を置くクラウド・コンピューティングのセキュリティ確保を目指して、米eBay、米Qualys、米Salesforce.com、米INGなどが中心となって結成した非営利組織であるCSA（Cloud Security Alliance）の活動が挙げられる。CSAは、2009年４月にガイダンス初版を発表した。米Dell、米McAfee、米RSA Security、米PGP、米DuPontなども参加し、メンバー企業は23社にのぼる。CSAは、日本支部が設立されている。CSAは、クラウドサービス提供者が順守すべき重要な分野やベストプラクティスをテーマとした文書や調査報告書を発行し、クラウド領域のセキュリティ向上に取り組んでいる（ITpro［2009］）。今後大切なのは、競争が激化していくクラウド市場で生き残りをかける企業が、こうしたベストプラクティスや標準に対応することだ。クラウドサービス提供者が差異化につながる標準を導入

し、重要な認定（ISO 27001など）を取得すれば、クラウド利用者もサービス提供者を実際の使用環境で比べる手段が増えるし、今後もクラウドサービス市場で事業展開し続けることに真剣なサービス提供者と、この流行に乗って次の流行が来る前に手早く稼ぎたいだけのサービス提供者を区別できるようになる。また、独立行政法人情報処理推進機構（IPA：Information-technology Promotion Agency、Japan）は、クラウドセキュリティに関する調査研究、普及啓発、教育、対策・指針策定などを目的に、CSAと相互協力協定を締結している。

欧州では、ENISA（European Network and Information Security Agency：欧州ネットワーク情報セキュリティ庁）が、「クラウドコンピューティングの情報セキュリティ確保のためのフレームワーク」、「クラウドコンピューティングの情報セキュリティに関わる利点、リスクおよび推奨事項」を発行するなどの活動を行っている（ENISA［2009］）。対象者はクラウドコンピューティングを利用する企業（特に中小企業）あるいは個人であり、それらの文書により、クラウドコンピューティングの既存および潜在ユーザーが、クラウドコンピューティングを利用する際のセキュリティ上のリスクと利点の評価をすることが可能になる。そこでは、リスクの評価に関しては、①「ポリシーと組織関連のリスク」、②「技術関連のリスク」、③「法的なリスク」、④「クラウドコンピューティングに特化していないリスク」の４つのカテゴリーにおいて、計35項目のリスクを提示し、そのリスクにどのような脆弱性と資産が関連するかを示している。なお、取り上げている脆弱性は53項目あり、一般的な情報セキュリティ上の脆弱性と、クラウドコンピューティングに特化した脆弱性の両方をとりまとめている。資産については、「企業の評判」、「顧客の信頼」、「個人の秘密データ」、「人材データ」など23項目について、その所有者と認識される価値の高低を明示している。

３．１．３　クラウドコンピューティングの利用者が考慮すべきリスク対策

以上のような内外のセキュリティーに関する標準やガイドラインに準拠しても、クラウドコンピューティングにおいては、扱う情報の所在やシステム管理権限の多くがプロバイダに委ねられているため、従来の情報システムと同じような対策を講じることが困難になる場合がある。そこで、以下に挙げる３つの観点からクラウドコンピューティングの利用者が考慮すべきリスク対策を考える。

(1)　クラウドコンピューティングを利用するための情報セキュリティマネジメント

クラウドコンピューティングを利用する場合、管理すべき情報や権限が社内に限定されなくなるが、一般に社内の情報セキュリティマネジメントは社外にまで及ばないため、ユーザ企業単独では十分な情報セキュリティマネジメントを実現することが難しい。そこで、セキュリティ対策状況や管理状況について利用者とクラウドプロバイダ間で共有するとともに、双方で必要に応じた対策を行い、双方がコントロールする情報セキュリティマネジメントを実現することが、クラウドコン

ピューティングを活用していく上では非常に重要であるといえる。具体的な対策については、経済産業省が「クラウドサービス利用のための情報セキュリティマネジメントガイドライン」（経済産業省［2011］）に定義しているので、ぜひ参考にしてほしい。

⑵　内部統制の観点に基づいたリスク対策

企業の内部統制においては、情報システムに係る統制（IT統制）が要求されており、クラウドコンピューティングの利用においても、同様にIT統制が要求されることに違いは無いことに留意したい。IT統制の観点から見る場合、クラウドコンピューティングの利用を外部ベンダへのIT業務の外部委託と位置づけて考えることが非常に効果的である。IT業務の外部委託先管理の観点では、委託元となる利用者に対し、委託先となるクラウドプロバイダの統制状況の把握・評価が要求されるが、それらを行うための手段として、以下に代表される手続の活用を検討するのが有益である。

①　受託会社の統制手続きに関する保証報告（国際保証業務基準（ISAE）3402）

②　委託業務に係る統制リスクの評価（監査基準委員会報告第18号）

なお、国内においては日本公認会計士協会により監査基準委員会報告第18号をISAE3402に準拠する形で更新中（日本公認会計士協会［2011］）であるので、将来的な対応においては活用することが望まれる。

⑶　クラウドコンピューティングにおける契約内容（上山　浩［2012］）

クラウドサービスを選定する際、どうしても価格やサービス品質、性能などに目を向けてしまいがちである。しかし、もっと契約内容に注意を払うべきである。サービスの最低利用期間や損害賠償の上限規定の有無をチェックしておくことが必要である。「いつでもすぐに止められる」という手軽さからか、契約内容を精査せずにクラウドサービスを利用し始める企業が増えている。しかし、契約書や約款を調べてみると、ユーザー企業が不利益を被る条項が含まれているケースは少なくない。とくに、契約の拘束期間・サービス品質・サービス中止の猶予期間・損害賠償に関連する条項について契約内容を吟味する必要がある。クラウドサービスのベンダーサイドでシステムの障害が起きた場合のリスクについても認識することが必要である。どの程度のリスクがあるかについてはベンダーサイドで保証するサービスレベルを記述したSLA（Service Level Agreement）が参考になる。Paasに関する一般的なサービスレベルは99.9％であるが、このレベルでも１年間にするとその0.1％の約８時間はサービスが停止する可能性がある。航空会社の予約サービスや銀行の勘定系システムなどの数分程度のシステムの停止でも問題となる業務においては、このレベルでは使い物にならない。当然、クラウドコンピューティングに適した業務を選んで、サービスを活用していくということになろうが、サービスが停止した場合も一定割合の料金が差し引かれるだけで、障害に伴うビジネス上の損失に対する補償は行われないという問題がある。この点については、ベンダーサイド

で大口の需要家に対しては、特別のサービスを提供するということがある。しかし、その一方でコストが増大するので、クラウドコンピュータの価格面での優位性と相反することとなる（元橋一之[2010]）。

これらの内容は、システムの運用・保守サービスやBPO（ビジネス・プロセス・アウトソーシング）サービスなど、IT関連サービスを利用する際の契約にも当てはまる。

最後に、クラウドコンピューティングを利用する上でのリスク対策において、扱う情報そのものに対する責任は、これまでの情報システムの利用と変わらず、利用者側にあることを忘れてはならない。クラウドコンピューティングを安全に活用していくためには、リスク対策を行う責任が自分自身にあることを理解し、利用者が主体となって様々なリスク対策を講じていくことが何よりも大切であるといえるだろう。

3．2　国内外のデータセンタを利用する上での法的な検討

世界的潮流の中で、日本の企業もクラウド・コンピューティングを利用することを迫られている状況にある。しかしながら、クラウド・コンピューティングに関しては、その技術的な特性を踏まえた法的な検討が必ずしも追いついていない部分もあり、実務において、クラウド・コンピューティングに関する法的リスクの不透明性が、わが国におけるクラウド・コンピューティングの普及の早期の展開に向けての障害の一つとなっている。クラウド・コンピューティングの利用から生じる法的問題の特徴は、①データが保存されているサーバが物理的に存在するものの、②このサーバをクラウド・コンピューティングの利用者が直接に把握することができず、さらに、③サーバが存在する国が多数にわたり得るところにある。そこで、以下に国境をまたぐデータの取扱いに関わる米国とEU、日本の法令の概要と制約などについてまとめる。

(1)　米国愛国者法（USA Patriot Act）

(ア)　米国愛国者法の概要

クラウド・コンピューティングでは、技術的に国外にデータ・サーバを設置することも可能である。この場合には、サーバが所在する国の公権力が当該国の法令に基づいて、サーバに保存されたデータに対して法的措置を講じる可能性もあり、国外に設置されたサーバにデータが保存されるクラウド・サービスに関しては、このような観点からの検討が必要となる。経済産業省が2010年８月16日に公表した「『クラウドコンピューティングと日本の競争力に関する研究会』報告書」（以下「経産省研究会報告書」という）では、2001年９月11日に発生した同時多発テロ事件を受け、2001年10月に成立した「Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001（以下、米国愛国者法（USA PATRIOT Act））」により捜査機関の権限が拡大されたこと等を受け、米国では、日本の手続と比較して、裁判所の許可が不要である範

囲が広い等政府機関に付与されている権限が大きいため、クラウドを活用して、米国サーバへデータを保存する場合には留意が必要である旨の指摘がなされている（経済産業省［2010］pp. 30-31）。

(イ) 米国愛国者法の関連動向

カナダでは、アウトソーシング契約を結ぶ際に参照すべきガイドライン「Taking Privacy into Account Before Making Contracting Decisions」を策定した。アウトソーシング業務の委託先が米国企業の場合、もしくはカナダの企業であっても米国に関連企業が存在する場合には、個人情報を含むデータが国境を越え、米国に置かれる可能性がでてくる。この場合、愛国者法の適用対象となることから、本人の承諾なく個人情報が米国当局に閲覧されるリスクを懸念しての措置である。このガイドラインはカナダ連邦政府予算庁が作成したもので、プライバシー法に基づき、個人情報を取り扱う業務をアウトソースする場合は、国民のプライバシーを適切に保護するため、ガイドラインで示されているアドバイスに従うよう、強く推奨している。

(2) EUデータ保護指令(Data Protection Directive)

EUおよび英国ではデータ保護指令（Data Protection Directive）により、EU内の住民の個人情報に関して十分なデータ保護レベルを確保していない第三国へのデータの移動を禁じている。EUのデータ保護指令が要求する十分な保護水準を確保していると認められている国外地域は、スイス、カナダ、アルゼンチン、ガンジー島、マン島、ジャージー島の6つである。

このうち、カナダは、連邦政府部門対象の法律、民間部門対象の法律、州政府対象の州法など、複数の法律を組み合わせることにより、ほぼすべての機関を対象とした法的枠組みを形成し、十分性を認められている。 米国の場合は、包括法がないため、特定の認証基準を設け、その認証を受けた企業ごとに十分性を付与するセーフハーバー協定を2000年にEUと締結している。また、米国―EU間の航空旅客情報についても認められている。なお、Google、Amazon、salesforce.com、Microsoftなど多くのサービスプロバイダはセーフハーバー協定を遵守していることから、EU内の住民の個人情報を米国で保管することが可能となっている。セーフハーバーを遵守している組織リストについては、米国商務省のウェブサイトの「Safe Harbor List」（米国商務省［2012］）を参照。一方で、2010年にドイツから、米国に個人情報を提供するに当たり、セーフハーバー協定のみでは不十分であるとの表明がなされている。このため、国によっては、より厳しい制約を要求される可能性があることに留意する必要がある。EUは、日本を個人情報の保護に関して十分なレベルの法的措置を講じている国とはみていない。そこで、いろいろな例外措置で対処している。例えば、ヨーロッパで採用した本人の同意を得るとか、契約で個人情報の保護をするとかの対処を取っている。EUは個人データの保護規則を強化し、同規則を域外企業へ適用しようとしている。しかしながら、個人データを適切に保護した上で活用することは、利用者への革新的サービスの提供による新たな産業創出の鍵であり、過度な保護強化は、企業を萎縮させ、活動を抑制し、あるいは大きな負担を

強いることとなる。また、米国はEUとの間にセーフハーバー協定があるが、日本を含むアジア諸国等の多くはEUとの間にそのような協定がなく、個人データの保護が十分でないと見なされ、こうした地域の事業者は、EU域内からの個人データの移転に厳しい条件がかけられ、それに応じた追加コストが生じることを恐れている（経団連［2012］）。

(3) 外国為替及び外国貿易法

「外国為替及び外国貿易法（以下、外為法）」（外為法［1949］）では、国際的な平和及び安全の維持を妨げることがないように、特定の技術を特定の外国において提供する際や特定の外国人名を外国企業に提供する際には、経済産業大臣の許可が必要と定めており、第25条第3項では「特定国において受信されることを目的として行う電気通信による特定技術を内容とする情報の送信」も許可の対象として規定している。したがって、日本国内から海外の外部サーバに情報を送信する際や、当初から外国の利用者に情報を提供することを目的に自社の海外サーバに情報を送信する際、国内サーバのリソースを演算処理等のために提供してその結果を送信する際等も、許可の対象となる場合がある。この特定技術とは、核兵器等の大量破壊兵器や通常兵器に関連した技術を指しており、例えばこの技術の中には暗号技術などの汎用的な技術も多く含まれるため、これらの情報を取り扱う際には留意が必要である。一方、米国の「米国輸出管理規則」のように自国で開発されたソフトウェアの輸出に規制を設けている国もあるため、日本国内のクラウド事業者が他国のソフトウェアをクラウドサービスの中で提供する場合には、各国の輸出規制に準拠しているかどうかに留意する必要がある。

4．まとめ

米国政府のようにクラウド・コンピューティングは時期尚早という判断もあるが、ポテンシャルという意味ではクラウド・コンピューティングは今後伸びると評価できる。実際の利用は漸進的なアプローチとなる。その際には、前節で言及した法的なリスクを含めたセキュリティー対策への考慮が重要であるとの認識とそのための人材開発が各組織の課題である。具体的には、セキュリティを専門に担当するチームと、それを統括するCSO（Chief Security Officer）がその役割を担う。一方でITに関わるメンバーも、開発であろうが、テストであろうが、セキュリティに責任を持つ業務体制が必要である。また、どのような強固なセキュリティ製品を導入したとしても、管理者に負荷が掛かりすぎてしまっては意味がない。特にIT要因の少ない中小企業にとって、その悩みは深刻だろう。そこで今注目されているのが、クラウド型セキュリティソリューションがある。

参考文献

(1) Amazon［2011］：Summary of the Amazon EC2 and Amazon RDS Service Disruption in the US East Region（英語）
http://aws.amazon.com/jp/message/65648//185-2402776-0325357

(2) 米国商務省［2012］：セーフ・ハーバーリスト https://www.export.gov/safehrbr/list.aspx

(3) ENISA［2009］：Cloud Computing: Benefits, risks and recommendations for information security（英語）
http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment

(4) Forrester Research社［2011］：
http://www.vmware.com/jp/company/news/releases/cloud-survey-11-08-11.html

(5) 外為法［1949］http://law.e-gov.go.jp/htmldata/S24/S24HO228.html

(6) IDC Japan［2011］：「国内パブリッククラウドサービス市場予測を発表」
http://www.idcjapan.co.jp/Press/Current/20120508Apr.html

(7) ITpro［2009］：「クラウドのセキュリティ確保を目指すCSA、ガイダンス第2版を公開」
http://itpro.nikkeibp.co.jp/article/NEWS/20091218/342355/

(8) 経団連　［2012］:日米クラウドコンピューティング民間作業部会　報告書
http://www.keidanren.or.jp/policy/2012/073_honbun.html

(9) 経済産業省［2010］:『クラウドコンピューティングと日本の競争力に関する研究会』報告書」
http://www.meti.go.jp/press/20100816001/20100816001.html

(10) 経済産業省［2011］：クラウドサービス利用のための情報セキュリティマネジメントガイドラインの公表
http://www.meti.go.jp/press/2011/04/20110401001/20110401001.html

(11) 元橋一之［2010］「クラウドコンピューティング時代の日本企業の課題と将来展望」RIETI（経済産業省）：
http://www.rieti.go.jp/jp/papers/contribution/motohashi/10.html）

(12) 日本公認会計士協会［2011］：監査基準委員会報告書402「業務を委託している企業の監査上の考慮事項」(案)
http://www.hp.jicpa.or.jp/specialized_field/main/402.html、監査・保証実務委員会実務指針第86号「受託業務に係る内部統制の保証報告書」（案）http://www.hp.jicpa.or.jp/specialized_field/86_1.html

(13) 上山　浩［2012］：「寄稿　クラウド時代のIT法務（第2回）～最低利用期間は長すぎないか　損害賠償の上限規定にも注意」、日経コンピュータ　第800号　2012.1.19