クラウド・コンピューティングにおける情報セキュリティ管理の課題と対応

宇根正志（うねまさし）／鈴木雅貴（すずきまさたか）／吉濱佐知子（よしはまさちこ）

要　旨

金融機関の情報システムにおいてオープン化や複雑化が進んでおり、情報システムの安全かつ効率的な構築・運用が求められている。こうしたなか、情報システムの導入・運用コストの軽減等を期待することができる計算資源の新しい利用形態として「クラウド・コンピューティング」（以下、クラウドという）」が、金融分野においても注目されている。ただし、そうしたメリットを享受するためには、クラウドに向いている処理を見極め、クラウドにおける情報セキュリティ管理を適切に実行することが求められる。特に、新しいサービスであるクラウドにおける未知の脅威や脆弱性が今後顕現化する可能性があり、そうした問題発生時の対応について検討しておく必要がある。また、一部のパブリック・クラウド等、クラウドの利用機関がクラウドにおける情報セキュリティ管理の実態を把握困難なケースがある。クラウドにおける情報セキュリティ管理の実態をクラウドの利用機関がどのように把握するかを明確にすることも求められる。クラウドの利用機関がクラウドの利用に関する検討を行う際には、こうした課題に留意することが求められる。

本稿では、クラウドの特徴について整理したうえで、クラウドを利用する際の情報セキュリティ管理上の課題を金融機関によるクラウドの利用に焦点を当てて整理する。さらに、そうした課題への対応のあり方や関連する最新の技術研究の動向を説明する。

キーワード：脅威、クラウド・コンピューティング、情報セキュリティ管理、脆弱性、セキュリティ・ポリシー

本稿を作成するに当たっては、株式会社富士通研究所クラウドコンピューティング研究センター長代理の岸本光弘氏、九州大学教授の櫻井幸一氏、九州大学准教授の堀　良彰氏、財団法人九州先端科学技術研究所の高橋健一氏、同研究所の江藤文治氏から有益なコメントを頂いた。ここに記して感謝したい。ただし、本稿に示されている意見は、筆者たち個人に属し、日本銀行あるいは日本アイ・ビー・エム株式会社の公式見解を示すものではない。また、ありうべき誤りは、すべて筆者たち個人に属する。

宇根正志　日本銀行金融研究所企画役
（現 システム情報局企画役、E-mail: masashi.une@boj.or.jp）
鈴木雅貴　日本銀行金融研究所（E-mail: masataka.suzuki@boj.or.jp）
吉濱佐知子　日本アイ・ビー・エム株式会社東京基礎研究所
（E-mail: sachikoy@jp.ibm.com）

1. はじめに

金融機関の情報システムにおいてオープン化や複雑化が進んでおり、情報システムを安全かつ効率的に構築・運用することが求められている。そうしたなか、金融分野をはじめとする幅広い分野において、計算資源の新しい利用形態としてクラウド・コンピューティング（以下、クラウドという）が有効な方策の1つとして注目を集めている。クラウドは、「ネットワークを介して計算資源を必要なときに必要な量だけ利用するというサービスの利用形態」を指して使われることが多く、クラウドの活用によって、計算資源を所有することなく利用可能となる。その結果、①計算資源の導入・運用コストを軽減できる、②情報システムで使用するリソースの量や仕様変更を柔軟かつ迅速に実行できる、③豊富なノウハウを有するクラウドのサービス提供者（以下、クラウド提供者という）に対して情報セキュリティ管理の実施を委託できるなどのメリットが考えられる。既に、クラウドはさまざまな分野において活用されはじめており、金融分野においても利用事例が報告されるようになってきている[1]。また、複数の利用機関が共同で利用するクラウド（パブリック・クラウドと呼ばれる）に向いた処理に関する考察が金融情報システムセンター［2010］において行われており、①リアルタイム性を必要としないもの、②データ更新の少ないもの、③個人情報や機密情報を扱わないものなどが挙げられている。

ただし、クラウドを金融分野において活用するうえで、どのような処理がクラウドに適しているかを検討するとともに、情報セキュリティ上の課題に留意する必要がある。第1に、金融機関は自社のセキュリティ・ポリシーがクラウドのサービスにおいて満足されていることを随時確認する必要があるが、同サービスに係る情報セキュリティ管理の実態を金融機関が十分に把握できない可能性がある。特に、海外のデータ・センターを利用する場合、情報漏洩のリスクに加えて、国境を越えたデータ移送に対する法律の準拠やクラウドが所在する国のデータの開示請求等のカントリー・リスクについても配慮することが求められる。

第2に、クラウドが新しいサービスであるがゆえに、クラウド特有の脅威や脆弱性に関する研究の蓄積が少なく、新たな脅威等が今後顕現化する公算が高い。例えば、クラウドでは、同一のサーバーにおいて複数のユーザーのプロセスや仮想サーバー[2]が同時に実行されるケース[3]があり、その際に、攻撃者のプロセスや仮想サーバーが他のユーザーのプロセスに問題を引き起こす可能性がある。具体的には、サー

1 わが国におけるクラウドの利用事例については情報処理推進機構［2010］において、金融機関業務におけるクラウドの利用事例については金融情報システムセンター［2010］において紹介されている。

2 仮想サーバーは、1つの計算機を実質的に複数の計算機（仮想マシン）のように見せかける技術（仮想マシン技術）である。仮想マシン技術により、1台の物理サーバー上で複数の仮想サーバーを稼働させたり、負荷分散のために物理サーバー間で仮想サーバーを移動させたりすることが容易になる。

3 例えば、パブリック・クラウドと呼ばれる不特定多数のユーザーが同一のクラウドの計算資源を利用するケースである。こうしたユーザーによる計算資源の共用は、アプリケーションやプラットフォームでは「マルチテナンシー」（multi-tenancy）と、サーバーやネットワーク、ストレージなどのインフラでは仮想化と、それぞれ呼ばれる。

バー上でファイルを共有・編集するSaaS[4]において、攻撃者が不正なプログラムを含むファイルをそのサーバーに保管し、当該ファイルにアクセスした別のユーザーから認証用のデータ（クッキー）を盗取してそのユーザーになりすますという事例が知られている（Vamosi [2008]）。また、1つのCPUにおいて同じ種類の処理が複数実行される可能性が高く、例えば暗号処理の場合、それらの処理時間を測定することによって当該CPU上における他の暗号処理の情報（例えば、暗号鍵）を効率よく推定可能な場合があるとの研究成果が報告されている（Ristenpart, Tromer, Shacham, and Savage [2009]）。こうした問題に関する検討が本格化しつつあり（堀・江藤・高橋・櫻井［2009］、須崎［2010］）、今後も新たな脅威や脆弱性が報告される可能性が高い。

金融機関においては、金融取引に関するサービスに利用される情報システムが第三者の管理下にあったとしても、金融機関自身が管理する場合と同様の情報セキュリティを確保することが求められる（日本銀行［2001］、日本銀行金融機構局［2008］）。その意味で、クラウドのサービスに利用される計算資源が金融機関のセキュリティ・ポリシーに基づく一定の管理下におかれ、そのような管理が継続的に実施されていることを確認する必要がある。管理の実態をどのように把握するかについてはクラウドの形態に依存する。例えば、パブリック・クラウドの場合、クラウド提供者における管理状況の把握が金融機関にとって困難なケースがある。

現在、こうした課題に関して技術と制度の両面から検討が進められている（例えば、Armbrust *et al.* [2009] やENISA [2009]）。技術面では、クラウドを利用するユーザーが当該クラウドのセキュリティ要件の充足度合いを確認するための情報を（クラウド提供者を介さずに）オンラインで確認する手法の研究が活発化しつつある（堀・江藤・高橋・櫻井［2009］）。例えば、クラウドで処理されているデータの一貫性や可用性を検証する手法（Wang, Wang, Ren, and Lou [2009]、Bowers *et al.* [2010]）や、データの機密性を確保したまま処理を実行する手法（Gentry [2009]）が挙げられる。他方、制度面では、クラウドを対象とした情報システムにおける管理体制の監査制度について検討が開始されている（経済産業省［2009］）。金融機関がクラウドの金融サービスへの適用を考える際には、こうした取組みをフォローしつつ、クラウドにおける適切な情報セキュリティ管理をどのように確保するかについて十分に検討することが求められる。

本稿では、クラウドの技術的な特徴や主なメリットやリスクを説明する。そのうえで、金融機関がクラウドを活用する際の情報セキュリティ管理上の主要な課題として、①クラウドにおける未知の脅威や脆弱性にどのように対応するか、②クラウド提供者における情報セキュリティ管理の実態をどのように把握するかを説明する。さらに、これらの課題への対応のあり方について、技術的な検討状況を説明しつつ考察する。

4 SaaS（Software as a Service）は、アプリケーション・ソフトウエアの機能をサービスとして提供するタイプのクラウドである。

2. クラウドとは

(1) クラウドの形態

現在、クラウドという用語について世界共通の定義は存在せず、文脈によってさまざまな意味に捉えられている。例えば、ガートナー社では、クラウドを「スケーラブルかつ弾力性のある IT による能力を、インターネット技術を利用してサービスとして企業外もしくは企業内の顧客に提供するコンピューティング・モデル」と、比較的広い概念として定義している（ガートナー・ジャパン株式会社［2009］）。一方、米国立標準技術研究所（National Institute for Standards and Technology; NIST）は、以下の 5 項目を本質的な特徴として具備するサービスをクラウドと定義している（Mell and Grance [2009]）。

- ユーザーが、クラウドのサービス提供者側の人間を介することなく、必要に応じてサービスの利用を開始したり設定を変更したりできること。
- 機能がネットワーク経由で提供され、標準的な仕組みを使って多様なクライアント・プラットフォームからアクセスできること。
- サービス提供者の計算資源が複数のユーザーに対してマルチテナント・モデルによって提供されるように確保されており、顧客のニーズに従って物理的・仮想的な資源が動的に割り当てられること。
- 機能が迅速かつ柔軟に提供され、ユーザーが必要に応じて使用する計算資源の量を動的に増減させることができること。
- クラウドの利用状況を監視・制御して計算資源の利用を最適化し、当該利用者とサービス提供者に報告すること。

NIST は米国政府機関向けのクラウドの定義を検討しているが、それは一般にも適用可能な定義となっている。実際に、多くのベンダーが参画しているクラウド関連の業界団体である Cloud Security Alliance や Open Cloud Manifesto、後述する ENISA[5]においても NIST の定義を採用している（CSA [2009]、ENISA [2009]、OCM [2010]）。こうしたことから NIST の定義が現時点で最も標準的とみられており、本稿では「狭義のクラウド」と呼んで検討の前提とする[6]。

5 ENISA（European Network and Information Security Agency）は、欧州議会の下部組織であり、欧州域内におけるネットワークや情報セキュリティに関する調査・研究や EU 各国への政策提言等を行っている。

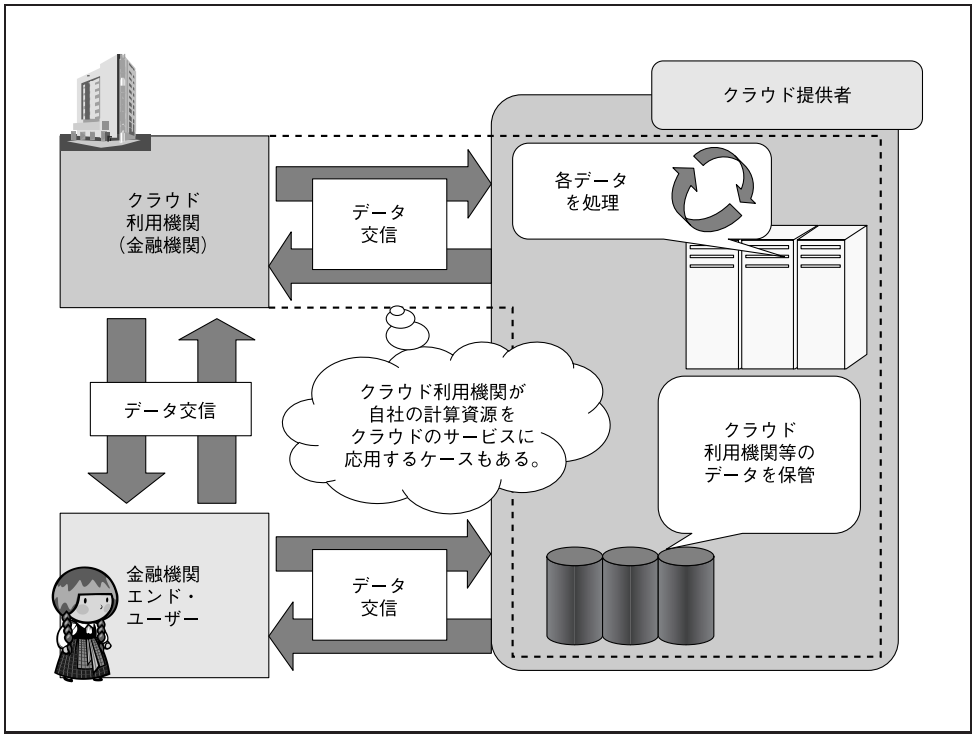
6 一般に、「クラウド」と呼ばれているサービスのなかには、マルチテナント・モデルではないサービスやセルフサービスを提供しないサービス等、狭義のクラウドに含まれないものもある。例えば、自社のサーバーやデータ・センターの管理の外部委託や複数の金融機関による共同センターのサービスにおいて、狭義のクラウドに類似したものが存在する。こうしたサービスにおいて本稿の議論がどの程度まで当てはまるかについては個々のサービスの形態に依存することとなる。

(2) クラウドの利用モデル

本稿における検討対象のクラウドの利用モデルを設定する。ここでは情報セキュリティ管理上の留意点について検討しやすくするために、「クラウド利用機関（金融機関）」「クラウド提供者」「金融機関エンド・ユーザー」というエンティティから構成される比較的簡素なものを考える（図表 1 参照）。

クラウド利用機関は、クラウドによって実現される金融サービスを提供する金融機関を意味する。クラウド提供者は、クラウド利用機関に対してクラウドのサービスを提供するエンティティであり、同サービスを提供するための計算資源を有するほか、同サービスに関連するデータを保管する。ただし、クラウドに用いられる計算資源をクラウド利用機関自らが保有するケースにおいては、クラウド提供者は登場しない。パブリック・クラウドの場合、NIST の定義に記述されているマルチテナント・モデルを前提とすると、当該クラウド利用機関以外の企業等が同じサービスを利用する。また、金融機関エンド・ユーザーは、クラウドによって実現される金融サービスを利用する末端の利用者であり、当該金融機関の従業員の場合や一般消費者の場合等がある。これらのエンティティは、必要に応じて他のエンティティとネットワーク経由で相互にデータを交信する。

図表 1　クラウドの利用モデル（概念図）



(3) クラウドの分類

提供される機能やクラウド利用機関の形態によってクラウドは分類される。それらの分類について上記のモデルに基づいて説明すると以下のとおりである。

イ．提供される機能による分類

- SaaS（Software as a Service）：クラウド上でアプリケーション・ソフトウエアの機能が提供されるもの。クラウド利用機関や金融機関エンド・ユーザーは、クラウド提供者が提供するアプリケーションをウェブ・ブラウザー等によって利用する。アプリケーションにおけるユーザー・インタフェースの構築においては、Ajax[7]に代表されるウェブ・プログラミング技術が使われている。また、SaaS では、複数のサービスを連携させること（マッシュ・アップと呼ばれる）が多く、そのために異なるサービス提供者の間でユーザー ID を統一的に扱う仕組みの標準化が進められている。
- PaaS（Platform as a Service）：クラウド上でウェブ・アプリケーション・サーバーやデータベース等のアプリケーションの実行環境が提供されるもの。クラウド利用機関が開発したアプリケーションを、クラウド提供者が提供するサーバーやミドルウエアにおいて実行するといったケースが該当する。PaaS を利用することで、アプリケーションの開発における生産性が向上することが期待される。PaaS においては、スケーラビリティを要求されるケースが多く、そのための分散ファイル・システム、分散データベース、分散キャッシュ技術などの分散処理技術が特に重要な技術として挙げられる。
- IaaS（Infrastructure as a Service）：仮想マシン技術によって実現される仮想マシンのほか、ストレージ、ネットワーク等の計算資源の基本要素がクラウド上で提供されるもの。クラウド利用機関は、クラウド提供者が提供する仮想マシン上に、OS、ミドルウエア、アプリケーションを含めて、自分にとって都合のよい環境を構築し使用することができる。このように、IaaS では、計算環境を提供するために仮想化技術を利用するという点に特徴がある。

ロ．クラウド利用機関の利用形態による分類

- パブリック・クラウド：複数のクラウド利用機関等がクラウドをインターネット経由で利用するもの。仮想化技術により複数のユーザー間で計算資源を共有して使用する。

7 Ajax（Asynchronous JavaScript＋XML）は、ユーザーの操作等に応じてウェブ・ブラウザーとサーバーが非同期通信を行うことで、ウェブ・ブラウザーに表示されたページ（の一部）の動的な書換えを可能にするウェブ・プログラミング技術である。

- プライベート・クラウド：独立したクラウドを個々のクラウド利用機関が占有して利用するもの。クラウド利用機関がクラウドのインフラを所有する場合や、ホスティング・サービスと同様に、クラウド提供者がインフラを所有し、それをクラウド利用機関が占有的に使用する場合がある。
- コミュニティ・クラウド：複数のクラウド利用機関が共同体（コミュニティ）を形成し1つのクラウドを共有して利用するもの。共同体としては、目的やコンプライアンス上の制約を共有する組織群等が挙げられる。例えば、金融分野であれば、共同センターを利用する複数の金融機関群が相当するほか、公共部門であれば自治体クラウドや霞ヶ関クラウドを利用する公的機関群が相当する。
- ハイブリッド・クラウド：複数の異なるクラウドを組み合わせてアプリケーションやデータを統合するもの。

組織がこうした各種のクラウドを活用する際には、クラウドだけを利用するケースのほかに、当該組織の既存のシステム（あるいはその一部）をそのまま利用し続けるとともに、クラウドと既存のシステムを連携させながら利用したり、複数のクラウドを用途によって組み合わせて使用したりするケースが少なくないと考えられる。このようなシステム連携を検討する際には、各システムにおける業務やデータの重要性を評価してクラウド適用可能性を検討するとともに、クラウドと既存システムにまたがるデータの切分けや管理、またアイデンティティ管理の方法等について検討することとなる。

(4) クラウドの利用による主なメリット

一般に、クラウドを利用することによって、計算資源の導入・運用のコストを大幅に引き下げることが可能になるほか、アプリケーションの開発の生産性向上、データ共有やアプリケーション連携による新サービスの提供が可能になるとの見方が多い。具体的には、以下のメリットがあるとみられている。

- 計算資源の初期導入費用が不要であるほか、計算資源の使用量（例：仮想マシン数やユーザ数）と期間によって課金されることから、ビジネス規模の変化に伴ってその使用量やコストを柔軟に調整可能である。
- 導入の期間を大幅に短縮可能であり、新サービスの開始時や一時的に大量の処理の実施が必要なときに計算資源を迅速に確保可能である。特に、エンド・ユーザー（図表1では「金融機関エンド・ユーザー」に対応）からの利用のリクエスト量が予想できない場合に有用である。
- 計算資源を自社内で保持する必要がなく、計算資源の管理やメンテナンスにかかるコストを削減可能である。

情報セキュリティの観点からは、計算資源にかかわる技術がクラウド提供者に集約され、クラウド利用機関が自社で管理を行うよりも高度なセキュリティを実現可

能であるケースが考えられる。例えば、計算資源の脅威・脆弱性対策のためには、常に情報収集や分析を行ったりパッチを当てたりすることが必要となる。多くのノウハウや経験を有するクラウド提供者であれば、そうした対応をクラウド利用機関よりも効率的に実行可能と考えられる。ただし、そのためには、クラウドの計算資源が適切な管理下におかれている必要がある。

また、クラウドの計算資源がクラウド利用機関から分離されていることによるメリットもある。例えば、遠隔地にあるクラウドにおいてデータを多重にバックアップしておくことで、災害時のデータの復旧をより確実なものにすることができると考えられる。

ただし、実際にこうしたメリットをどの程度享受することができるかに関しては、個々のアプリケーションの内容や要件のほか、利用するクラウドのサービス内容にも依存する。特に、情報セキュリティ上のメリットという意味では、本稿の3節以降で議論するように、情報セキュリティ管理上のリスクや、さまざまな課題をクリアするためのコストについても留意することが必要となる。そうした点も踏まえて、クラウドを利用することによるメリットを総合的に評価していくことが重要であるといえる。

3. クラウドにおける情報セキュリティ管理

本節では、前節(2)におけるクラウドの利用モデルを前提に、主として金融機関によるクラウド利用を想定して情報セキュリティ管理の課題を検討する。

(1) PDCAサイクル[8]による情報セキュリティ管理

金融サービスにおける情報セキュリティ管理に関して、クラウドを利用するケースに特化したガイドライン等は、現時点ではわが国には存在していない。ただし、金融機関自身がプライベート・クラウドを保有するケースでは、当該システムは金融機関による情報セキュリティ管理の対象になる。また、金融機関がパブリック・クラウドを利用するケースでは、当該金融機関によるクラウドの利用がクラウド提供者への「金融機関業務のアウトソーシング[9]」に該当するときは、金融機関自らが行う業務と同程度のリスク管理レベルがクラウド提供者の情報システムにおいても確保されていることが求められる（日本銀行［2001］）。

8 PDCAサイクルは、①情報セキュリティ管理を計画する（Plan）、②同管理を実施する（Do）、③管理の状況を点検・監査する（Check）、④点検・監査の結果を踏まえて管理の内容を適宜見直し・改善する（Act）という一連の流れを指す。本サイクルを継続的に実施し、情報システムを実際に運用しつつ改善を図るという点が特徴である。

9 ここでの「アウトソーシング」は、「他の企業に業務委託を行い当該企業の日常的な管理の下で業務執行が行われる」というケースを意味する（日本銀行［2001］）。

一般に、金融機関における情報セキュリティ管理の基本方針は「セキュリティ・ポリシー[10]」として示され、具体的な実施内容は「セキュリティ・スタンダード」として記述される（金融情報システムセンター［2008］、日本銀行金融機構局［2007］）。セキュリティ・スタンダードはPDCAサイクルに基づいて実施されるケースが多く、PDCAサイクルは通常以下の手順によって実施される。

① 保護の対象となる情報や情報システムを明確にする。
② 管理範囲となる情報システムとそのライフ・サイクルを明確にする。
③ 想定する脅威や脆弱性を明確にする。
④ リスク（＝ 被害額 × 発生確率）とその許容レベルを明確にする。
⑤ リスク軽減策（情報セキュリティ対策）を決定する（以上、“Plan” に相当）。
⑥ 上記⑤のリスク軽減策を実施する（“Do” に相当）。
⑦ リスク軽減策を含め、対策の効果を適宜評価する（“Check” に相当）。
⑧ 効果の評価結果に基づいて対策の見直しを実施する（“Act” に相当）。

2節(2)の利用モデルに基づき、クラウドにおける情報セキュリティ管理について検討を行う。

(2) PDCAサイクルの各フェーズ

イ．“Plan” フェーズ

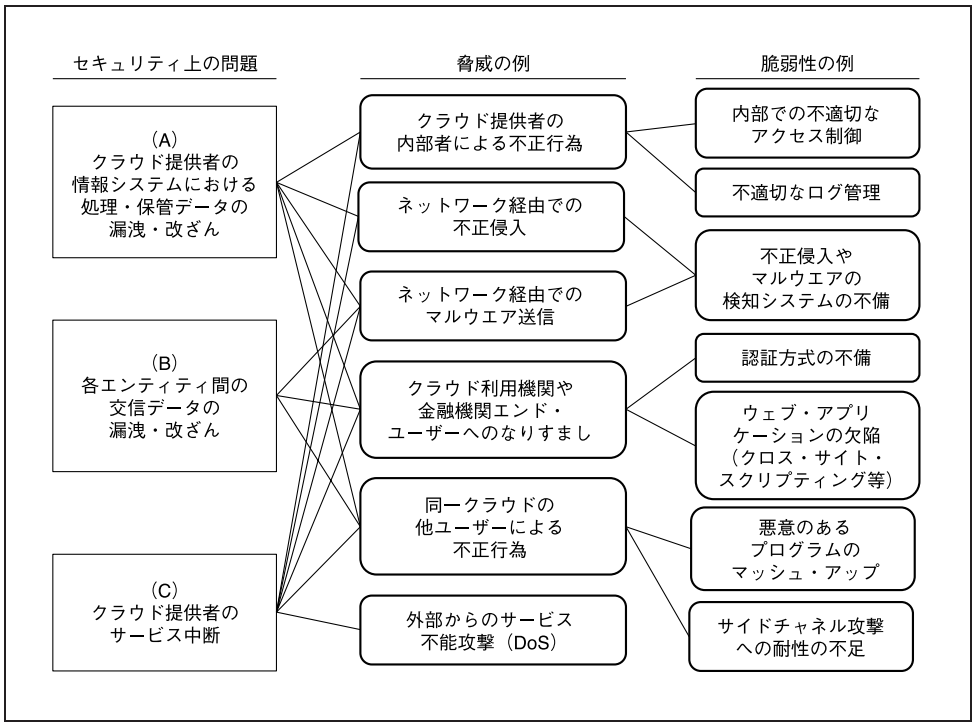
まず、保護対象となる情報と情報システム（本節(1)の手順①に相当）については、クラウド利用機関自身の情報システム、クラウド提供者の計算資源において処理・保管されるデータ、各エンティティ間で交信されるデータが想定される。これらの保護対象について、どのような情報セキュリティ（機密性、一貫性、可用性等）を確保すべきかを明確にする必要がある。

情報セキュリティ管理の範囲（手順②に相当）については、クラウド利用機関の情報システム、および、クラウド提供者の情報システムが管理の範囲に含まれる。クラウド提供者と金融機関エンド・ユーザー間のネットワークや金融機関エンド・ユーザーの情報システムに関しては、オープンなネットワークの場合のように、金融機関が直接管理困難なケースが想定される。

ライフ・サイクル（手順②に相当）については、クラウド利用機関による当該金融サービスの開始から終了までが対象となる。サービス終了のタイミングは、金融機関エンド・ユーザーが当該サービスを享受できなくなる時点のほか、過去の取引に関する係争等に備えたデータ保管の期限等が相当すると考えられる。サービス終了時のデータの移管・消去についてもライフ・サイクルに含まれ、情報セキュリティ管理の一環として検討することが必要である。

10 セキュリティ・ポリシーでは、主に、組織として守るべき情報資産、当該資産に関する脅威やリスク、情報資産の保護に関する責任の所在等が規定される。

図表２　これまでに知られている主な脅威や脆弱性



脅威や脆弱性（手順③に相当）に関しては、主に、(A)クラウド提供者の情報システムにおける処理・保管データの漏洩・改ざん、(B)各エンティティ間の交信データの漏洩・改ざん、(C)クラウド提供者のサービス中断につながるものが想定される。こうした問題発生の源となる脅威や脆弱性は個々のサービスや情報システムの形態に依存するが、共通して想定される代表的なものは図表２のようにまとめることができる。

また、同一のCPU上で複数のプロセスが動作するなどのクラウド特有の処理形態において新しい脆弱性が指摘されており（Ristenpart, Tromer, Shacham, and Savage [2009]）、今後も未知の脅威や脆弱性が顕現化する可能性がある。さらに、クラウドにおいて処理されるデータに関して適用される法律については、システムの設置されている（例えば、当該データが記憶媒体に保管されている）国や地域の法律が適用されることから（例えば、濱野［2009］）、そうしたデータ・センターの位置によって発生する法律上の問題も脆弱性の１つと考えることができる[11]。こうしたクラウ

11 例えば、米国愛国者法（US Patriot Act）のように、政府によるデータ・センターへの立入り調査を認めている場合、同センターに保管されている金融機関エンド・ユーザー等のデータが開示され、個人情報保護の観点から望ましくないケースが想定される。こうした問題を考慮し、一部のサービスでは、米国と欧州にデータ・センターを設置し、顧客がどちらを使うか選択できるようにしているケースもある。また、EUの個人データ保護指令第25条は、EU加盟国に対して、同データの保護に関する法制度が十分な国や地域に対してのみ個人データの転送を許可するように制限を課すことを求めている。このため、個人データの

ド特有の脅威や脆弱性に関する代表的な分析事例として、ENISA による分析が挙げられる（ENISA [2009]）[12]。ENISA の分析では、リスクを、①ポリシーや組織に関するリスク、②技術的リスク、③法的リスク、④クラウド特有でないリスクに分類し、そのインパクトの評価に関する目安を提供している。クラウドに関する脅威・脆弱性分析を実施する際には、クラウドにおいて利用されている技術の特性を十分に把握しておくことがまず必要となるが、それに加えて ENISA の分析事例等を参照することが有用であると考えられる[13、14]。

リスクとその許容レベル（手順④に相当）については、情報セキュリティ上の問題の発生に伴う被害額とその発生確率に基づいて評価するケースが一般的である。そのためには各問題を引き起こす脅威の発生頻度の見積もり等が必要となるが、同様に、クラウドを利用したサービスにおける脅威の発生頻度に関する検討が必要となる。そうした検討を行ったうえでリスクを評価し、当該リスクが許容レベルを超えていると判断される場合にはリスク軽減策を検討することになる（手順⑤に相当）。

以上の手順の結果、当該クラウドにおけるセキュリティ要件やリスク軽減策が決定される。これらを踏まえ、クラウド利用機関はクラウド提供者を選定し、サービス・レベルの合意（service level agreement; SLA）を行うことになる[15]。既にクラウド提供者の選定が完了している場合、そのサービス内容とセキュリティ要件等を照らし合わせ、必要があれば、セキュリティ要件等が満足されるようにサービス内容の変更をクラウド提供者に依頼することが求められる[16]。

保護に関する法制度が整備されていない国のクラウドを EU 域内から利用することができないというケースもありうる。

12 ENISA の分析によって抽出されたリスクのリストについては補論 1 を参照されたい。

13 また、Armbrust *et al.* [2009] では、クラウドの課題として、①サービスの可用性の確保、②サービス提供者によるデータの囲込み、③データの機密性と監査、④データ転送に関するボトルネック、⑤クラウドの性能の予測困難性、⑥使用するストレージの量の拡張・縮小のしやすさ、⑦分散システムの大規模化による不具合の検知困難さ、⑧使用するリソースの量の変更に要する時間の短縮、⑨クラウド利用機関のレビュテーションが、同一のクラウドを利用する他のクラウド利用機関による不正行為の影響を受ける可能性、⑩クラウドに適したソフトウエア・ライセンス形態の確立を挙げている。

14 このほか、一般に、クラウドにおいては従来の分散処理システムとは異なる特性を有しているケースが多いといわれている。すなわち、クラウドにおいては、①分散化により高い可用性を実現し、原則としていつでもデータの読出し・書込みができること（basically available）、②個々のノードの状態が、内部的状態だけでなく外部から情報を与えることによって決定する（soft state）、③データ間の整合性が（タイミングを特定できないが）いつかは確保されること（eventual consistency）の 3 つの特性によって特徴づけられる（これらは総称して “BASE” と呼ばれる。情報処理推進機構［2010］）。したがって、クラウドを利用する際には、情報セキュリティ上の特性を検討するとともに、各クラウドの上記特性がアプリケーションの要件を満足していることを確認しておくことが求められるといえる。

15 クラウド提供者の選定に当たっては、情報セキュリティ管理の側面に加えて、クラウド提供者の経営状況等についても考慮しておく必要がある。例えば、日本銀行［2001］においてアウトソース先の選定の際に留意すべき事項として示されているように、(A)候補先の経営体力（資本構成や信用度等）、(B)業界内での地位や今後の見通し（他社からのサービスの受託状況等）、(C)業務サポート体制・陣容やサービスの品質（事務ミスやシステムトラブル発生状況等）、(D)内部管理体制（人材育成や検査・監査体制等）等についても分析を行うことが重要である。

16 例えば、PaaS の場合、クラウド提供者がミドルウエアを、クラウド利用機関がアプリケーション・ソフトウエアを準備することになるが、同ソフトウエアに関するセキュリティ上のリスクをクラウド利用機関と

ロ．“Do” と “Check” のフェーズ

リスク軽減策の実施（手順⑥、“Do” のフェーズに相当）については、クラウド利用機関、クラウド提供者、金融機関エンド・ユーザーが “Plan” のフェーズにおいて決定される一定の役割分担に基づいてそれぞれ行うことになる。

リスク軽減策の評価（手順⑦、“Check” のフェーズに相当）においては、リスク軽減策の各実施主体が自分の情報セキュリティ管理に関して行うとともに、当該金融サービスの運営主体であるクラウド利用機関がそれらの評価結果をベースに「同サービスに関する情報セキュリティ管理が適切に行われているか否か」を評価することになる。したがって、クラウド利用機関には、クラウド提供者や金融機関エンド・ユーザーにおける情報セキュリティ管理の状況を把握しておくことが求められるが、どの程度把握できるかはクラウドの形態やサービス内容に依存することになる。プライベート・クラウドの場合、その計算資源をクラウド利用機関が所有しており、比較的容易に把握可能であると考えられる。一方、パブリック・クラウドの場合には、サービスによっては詳細な情報セキュリティ管理の内容や実態が開示されず、リスク軽減策を把握困難なケースが想定される。このようなクラウドを利用している場合や、利用開始を検討する場合には、クラウド提供者における情報セキュリティ管理の内容を把握する方法を検討するとか、他のクラウドのサービスについても候補として検討を行うといった対応が必要となる。

ハ．“Act” のフェーズ

上記 “Check” のフェーズにおける評価を踏まえて、クラウド利用機関は既存のリスク軽減策の効果を評価し、効果が十分発揮されていないという判断であればリスク軽減策の見直しを行うことになる（手順⑧に相当）。こうした見直しを実施するうえで、クラウド提供者には、クラウド利用機関による要望に配慮し、既存のリスク軽減策やそれに伴う情報セキュリティ管理の内容を柔軟に見直す姿勢が求められる。

（3）2 つの課題

上記の検討結果を踏まえると、クラウドのシステムを対象とした情報セキュリティ管理における主な課題を次の 2 点に集約することができる。

【課題 1】クラウドに特有のデータ処理やサービスの形態における未知の脅威・脆弱性をリスク評価においてどのように考慮するか。

【課題 2】クラウド提供者におけるリスク軽減策の実施状況等、情報セキュリティ管理の実態をどのように把握するか。

クラウド提供者との間でどのように負担するかについて SLA 等によって明確にしておくことが求められる。IaaS の場合では、クラウド利用機関が準備する OS やプラットフォームに関するリスクについて同様の対応が必要である。SaaS における SLA としてどのような項目を盛り込むかに関するガイドラインとしては、経済産業省によるガイドライン（経済産業省［2008］）が公開されている。

課題 1 は、未知の脅威や脆弱性への対応に関するものであり、情報セキュリティ技術を利用するシステム一般に当てはまる。ただし、現時点でのクラウドのような新しいサービスにおいては、脅威や脆弱性に関する情報や経験の蓄積が十分とはいえず、有意な問題が潜んでいる可能性に留意することが必要である。課題 2 については、金融機関が情報セキュリティ管理を直接実施しないケース、例えば、パブリック・クラウドの形態によってクラウドを利用するケースにおいて特に問題となる[17]。

ENISA [2009] においては、上記の課題 1 に関連したリスクとして、「(R.9)複数のクラウド利用機関が使用する場合に、クラウド利用機関間における計算資源の分離が不適切であり、情報漏洩等が発生する」というものが挙げられており、その結果として、「当該クラウドの脆弱性やセキュリティ上の問題の公表によって、そのユーザーすべてが風評被害の影響を受ける可能性がある[18]」と指摘されている。上記の課題 2 に関しては、「クラウド提供者の情報システムに対するクラウド利用機関による統制が十分取れない」というリスクが指摘されており、クラウド提供者における内部者による不正行為のリスク等が該当するといえる。

これらの課題は、金融機関であるクラウド利用機関に特有のものというわけではなく、あらゆる組織がクラウドを利用するうえで共通の留意事項であると考えられる。ただし、課題がどの程度深刻か、また、それに対してどのように対応するかに関しては、クラウドによって実現するアプリケーションの内容に依存する。したがって、金融機関においては、どのようなアプリケーションをクラウドによって実現するかを検討するなかで、上記の 2 つの課題それぞれの影響を評価し、対策の必要性を判断することになると考えられる。

4. 情報セキュリティ管理における課題への対応

本節では、クラウドにおける情報セキュリティ管理上の 2 つの課題について対応のあり方を検討する[19]。

(1) 未知の脅威・脆弱性への対応

未知の脅威・脆弱性への対応に関しては、事前にそのリスクを定量的に評価することは困難であると考えられる。そこで、未知の脅威や脆弱性によってクラウドに

17 パブリック・クラウドにおいては、そのサービスにおけるセキュリティに関して基本的に自己責任を前提とするケース（セキュリティの確保のための努力は行うものの、保証はできない）が少なくないのが実情であり、そうした傾向が今後普及する可能性があるとの見方もある（山崎［2010］）。

18 例えば不正なユーザーがクラウドを DoS（サービス拒否）攻撃などに使用した場合、そのクラウドの IP アドレスがブラックリストに載り、同じクラウドを利用する正当なユーザーがその影響を受けてしまう場合がある。

19 前節で指摘した法律面のリスクについても対応のあり方を検討することが求められるが、本稿では、技術や運用に関するリスクへの対応を取り上げることとする。

おけるセキュリティ特性（の一部）が満足されないという状況を想定したうえで、どのように対応するかを検討することが求められる。

本対応に関しては主に2つの方向性が考えられる。1つは、未知の脅威や脆弱性によって情報セキュリティ上の問題が発生したとしても、**アプリケーションへの影響を許容レベル以下に抑えるための緊急対応策を予め明確にしておく**というものである。もう1つは、**新たな脅威や脆弱性による影響を軽減するための技術的対策を柔軟に導入・実施できるようにしておく**というものである[20]。

イ．問題発生時の緊急対応に関する考察

クラウドに利用されている情報システムに問題が発生したという状況を想定し、**アプリケーションへの影響の軽減を目的として、金融機関の情報システムにおける緊急時対応計画（コンティンジェンシー・プラン）の整備と同様の検討を必要に応じて行っておく**必要があると考えられる。アウトソーシングにおける同計画の策定に関する日本銀行［2001］の記述を踏まえると、以下の事項についてアプリケーションに応じた検討が求められるといえる。

- 主要なシナリオ（システム・ダウン、センター被災、決済データの違算・紛失、顧客情報の流出など）を想定し、連絡・協調体制や代替手段の確保、必要な事務フロー等を予め書面で整備しておく。
- 緊急時対応計画の内容をクラウド提供者との間で協議し、内容の整合性を確認しておく。
- クラウド提供者と共同で定期的に実地訓練を行い、連絡体制や事務フローなどの検証および実務担当者の習熟を図る。
- クラウドのサービスにおいてセキュリティ上の問題が発生した場合、類似の問題の再発を防止するための対策を検討・実施し、その実施状況を適切にモニタリングしていく[21]。

こうした検討を行ううえで、クラウド利用機関においても当該クラウドにおける技術やその実装内容を理解し、それらの特性がどのようなセキュリティ上の問題につながる可能性があるかについてクラウド提供者と議論できるように準備しておくことが必要であるといえる。

20 これらのほか、未知の脅威・脆弱性が発生したとしても業務への影響をあまり及ぼさないようなアプリケーションをクラウドで実現するという方向性も考えられる。例えば、自社システム内でデータを暗号化し、それをクラウドにおいて保管しておきデータのバックアップとしてのみ利用するというケースが考えられる。この場合、クラウドに保管されたデータが読出しできなくなったとしても、業務への直接的な影響は小さいと考えられる。

21 2009年10月に発生したAmazon EC2のシステム障害では、同サービスを利用していた企業の一部のシステムが17時間ダウンするという事態が発生した。こうした長時間にわたるシステム・ダウンの背景の1つとして、当該企業が、同社に関する計算資源を管理する（アマゾン社の）システム管理者を特定困難であったという事実が指摘されている（スキャン・ネットセキュリティ［2009］）。クラウド提供者の計算資源に問題が発生した際に、情報共有と対応の検討をクラウド提供者との間で実施可能にしておくことが重要である。

ロ．技術的対策の実施に関する考察

技術的対策の導入という観点では、当該クラウドにおける情報システムのセキュリティの機能を柔軟に変更できる仕組みとなっていることが望ましい。現時点では検討段階であるが、そうした技術のコンセプトの例として、「オートノミック（自律型）・コンピューティング」が挙げられる（岩野［2010］）。本コンセプトは、事前に設定されたポリシーに基づき、当該情報システムが問題発生に対して自律的に判断・対応するというものであり、クラウドの情報システム等への活用方法について検討が進められている。今後、オートノミック・コンピューティングを実現するクラウドが利用可能になれば、クラウド利用機関は、検討対象となっているクラウドがこうしたコンセプトの技術を活用しているか、また、活用している場合にはどのようなポリシーの設定になっているか（どのような問題に対してどのように対応するよう設定されているか）を確認し、柔軟なセキュリティ機能を有するクラウドを選択できるようになると期待される。こうした観点から、本分野の今後の検討動向が注目される。

また、新たに発生した問題の種類によっては技術的な対策の実施が困難と判断されるケースも想定される。そうした際にも当該アプリケーションを中長期的に継続する必要がある場合、それまで利用していたクラウドのサービスを中止して他のサービスに乗り換えるという選択が求められる可能性がある。他のクラウドのサービスへの乗換えを考慮する際には、当初利用していたクラウドにおいて、処理対象のデータやソフトウエアの回収・廃棄と他のクラウドへの効率的な移入の方法を確認し、当該データ等が当該クラウド提供者においてロックインされたり、当該データ等が他のエンティティに流用されたりするといった状況に陥ることがないように留意する必要がある。

(2) 情報セキュリティ管理の実態の把握

クラウド提供者における情報セキュリティ管理の実態把握については、クラウド利用機関が自らクラウド提供者から情報を得るケースと、クラウド利用機関が信頼する第三者の評価結果を利用するケースが考えられる。

イ．クラウド利用機関が自ら実態把握を行うケース

クラウド利用機関は、クラウドにおける計算資源の動作状況に関するログ・データ等を入手し、情報セキュリティ管理の実態把握を行うことが考えられる。そうした手法に関する研究としてデジタル・フォレンジックの分野の研究が近年盛んに行われており（佐々木・芦野・増渕［2006］、佐々木［2010］）、例えば、同手法によって問題発生の予兆を把握し追加的な対策の検討につなげるといった運用も考えられる。そのような場合、デジタル・フォレンジック等の手法によって具体的にどのようなデータを入手する必要があるかに関して検討を行い、クラウドのサービス（お

図表 3　管理の実態把握のための手法に関する最近の研究

目的	各手法の概要	備考（今後の課題等）
①データの一貫性確認	・【Wang, Wang, Ren, and Lou [2009]】クラウドの計算資源において処理されたデータに対してデジタル署名を生成しておく。後日、一貫性確認が必要な場合には当該データに対する署名検証を実施。	・クラウド利用機関は署名生成・検証の機能をローカルで準備する必要がある。 ・現時点では一部の署名方式（RSA）にのみ対応可能。
②データの可用性確認	・【Bowers *et al.* [2010]】データが特定のハード・ディスクに偏って記録されていないことを、データの読出しの応答時間によって確認。	・クラウド利用機関は個々のデータが記録されているハード・ディスクを特定する必要がある。
③データの秘匿	・【Gentry [2009] ほか】公開鍵暗号を利用してデータを暗号化し、その暗号化データをクラウドにおいて処理。処理後に復号することで、暗号化しないデータを処理した場合と同一の結果を得る。	・データの処理が他のクラウド利用機関のデータに連動して実施される場合、（暗号だけでなく、）一連の処理の一貫性を保証する別の機構（例えば、耐タンパー・ハードウエア*）がデータの秘匿に必要（van Dijk and Juels [2010]）。

備考：* 耐タンパー・ハードウエアは、外部からの機能の改変や内部データの読出しに対して耐性を有するハードウエアである。

よびクラウド提供者）を選択する際に、そうしたデータの入手の可否を確認する必要がある[22]。

また、クラウド利用機関が技術的な手段で（クラウド提供者を介さずに）当該情報を入手することができれば望ましい。こうした問題意識に基づき、クラウド利用機関による情報入手や検証を支援する技術の研究が進められている。主な事例として、①クラウドにおいて処理されているデータの一貫性を確認する手法（例えば、Wang, Wang, Ren, and Lou [2009]）、②クラウドにおいて保管されているデータの可用性を確認する手法（例えば、Bowers *et al.* [2010]）、③データをクラウド提供者に対して秘匿する手法（例えば、Gentry [2009]、van Dijk and Juels [2010]、van Dijk, Gentry, Halevi, and Vaikuntanathan [2010]）が挙げられる（図表 3 参照）[23]。

これらの研究は現時点では検討途上のものであり、実際のクラウドに直ちに適用可能というわけではない。しかし、クラウド利用機関自らがクラウドの情報セキュリティ管理の実態を把握するという方向性での重要な研究であり、今後の研究動向をフォローし、実際のサービスへの適用可能性について検討することが有用であると考えられる。

また、実際に金融機関がクラウドを活用する際に、上記の 3 つのセキュリティ特性（データの一貫性、可用性、秘匿）が必要になるか否かはアプリケーションに依

22 こうした情報提供の要望に関して、クラウド提供者側がどの程度応じてくれるかという点については一定の限界があるというのが実情であり、応じてくれない場合には、当該サービス提供者を利用するか否かという選択にならざるをえないとの見方もある（浦野［2010］）。

23 これらの各手法に関する研究事例の概要については、補論 2 を参照されたい。

存する。例えば、公表されている統計データの解析をクラウドによって実施するといった場合、当該データおよびその処理の結果を秘匿することが必要でないと判断されるケースもありうる。したがって、どのようなセキュリティ特性を満足させる必要があるかを、個々のアプリケーションの要件を明確にしながら検討することが求められるといえる。

ロ．信頼できる第三者による評価結果を利用するケース

もう 1 つの方向性は、クラウド提供者における情報セキュリティ管理の実態を第三者が評価し、その結果をクラウド利用機関が活用するというものである。例えば、米国公認会計士協会によるアウトソーシング事業者の内部統制に関する監査基準 SAS-70（Statement on Auditing Standards 70）に基づく認定を取得し、一定の情報セキュリティ管理を実施済みであることを示すクラウド提供者も既に存在している（浦本［2009］）。また、情報セキュリティ管理に関する評価・認定の制度的な枠組みである ISMS 適合性評価制度[24]に基づく評価・認定をクラウド提供者が受け、その結果をクラウド利用機関が確認するという方法も考えられる。ただし、これらの認定は必ずしもクラウドのサービスを前提としたものではない。したがって、同認定を参照する場合には、認定付与の前提となっている調査項目が適切か否かを確認しておく必要がある[25]。

また、クラウドに特化した情報セキュリティ監査の制度的枠組みの構築に向けた検討が経済産業省の公募事業の一部として現在進められている（経済産業省［2009］）。経済産業省［2009］によれば、①クラウド利用機関から情報セキュリティ監査の依頼を受けた監査者がクラウド提供者と守秘契約を締結して監査を実施し、当該クラウド利用機関に対して監査結果を報告するという形態や、②クラウド提供者から情報セキュリティ監査の依頼を受けた監査者が監査を実施し、その結果をクラウド利用機関に対して開示するという形態等、どのような監査の形態が望ましいかの検討が行われる予定となっている。また、情報セキュリティ監査に対するニーズの調査、監査基準案の作成についても検討される見込みである。

情報セキュリティ管理の実態把握を行ううえで、既存の監査制度や評価・認定制度をどのように活用することができるか、また、現在検討が進められている新しい

24 ISMS（Information Security Management System）適合性評価制度は、企業等が自社の情報システムにおける情報セキュリティ管理を一定の枠組み（ISMS）に沿って適切に実施していることを、第三者機関が評価し認定するという制度である。本制度における「一定の枠組み」である ISMS は、情報セキュリティ管理に関する国内標準 JIS Q 27001 に規定されている。詳細については田村・宇根［2008］を参照されたい。

25 ENISA [2009] においては、「業界標準等において定められた認証（例えば、ISMS 適合性評価制度に基づく認証や PCI DSS に基づく認証*）をクラウド利用機関が得るうえで、利用しているクラウド提供者が認証要件に適合しない場合がある」と指摘されている。

* PCI DSS（Payment Card Industry Data Security Standard）は、クレジットカードの加盟店や決済代行業者が取り扱うカード会員の情報を保護するために、国際カードブランド 5 社（Amex、Discover、JCB、MasterCard、VISA）が共同で策定したセキュリティ基準である。本基準に基づく認定については、セキュリティ対策を実施している加盟店等に対して、カードブランドによって認定された第三者評価機関が加盟店のセキュリティ対策の状況を審査し、それにパスした加盟店等が認定を得るというものである。

監査制度が必要であるかなどは重要な論点である。クラウドの活用を検討する際には、こうした論点に関する議論の動向を見極め、適用対象となるアプリケーションに応じて望ましい対応を検討することが求められる。

5. おわりに

クラウドには、ユーザーであるクラウド利用機関の情報処理において発生する諸々のコストの大幅な低減を可能にするとともに、アプリケーションの開発の生産性向上や新サービスの創造可能性という観点で大きな期待が寄せられている。ここでの「諸々のコストの低減」には、計算資源の新規購入や維持・管理に伴って発生する金銭的な出費の低減だけでなく、クラウド提供者による一元的な情報セキュリティ管理によって、当該アプリケーションのセキュリティ対策を効率化することができるという面も含まれる。従来の情報システムに関するアウトソーシングも同様の傾向を有しているといえるが、パブリック・クラウドのような形態への移行によって、上記のメリットをさらに拡大させることが可能になると期待されている。

ただし、こうしたメリットを享受するためには、「雲の中」にあるクラウドをある程度「雲の外」に出すことが求められる。例えば、金融機関がクラウドを利用する場合、自社のセキュリティ・ポリシーが当該クラウド提供者の計算資源において満足されているか否かを必要に応じて把握しておく必要がある。また、新しいサービスであるクラウドにおいては、その脅威や脆弱性に関する経験が相対的に少なく、未知の脅威や脆弱性に加えて、運用上の課題等が今後明らかになっていく公算が高い。クラウド提供者における情報セキュリティ管理の実態把握に関して、クラウド利用機関がクラウド提供者を介さずに必要な情報を入手するための手法の研究が進められているが、実際のクラウドのサービスに適用可能なレベルにまでは至っていないのが実情である。

クラウドの利用を検討する金融機関においては、まずクラウドにおいて利用されている技術について理解しておくことが求められる。そのうえで、クラウドにおける情報セキュリティ管理の実態を把握し、未知の脅威等を前提とした緊急対応策の策定や技術的対策の柔軟な導入・実施についてクラウド提供者と共同で行うことが必要であろう。

参考文献

岩野和生、「オートノミックコンピューティングからレジリエンシーへの道」、『第12回情報セキュリティ・シンポジウム発表資料』、日本銀行金融研究所、2010年3月5日

浦野祐介、「クラウド・コンピューティングとコーポレートガバナンス（5）」、『NBL』第928号、2010年5月、56～61頁

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』第50巻第11号、情報処理学会、2009年11月、1099～1105頁

ガートナー・ジャパン株式会社、『クラウド・コンピューティングに関するガートナー社の見解』、ガートナー・ジャパン株式会社、2009年10月9日（http://www.gartner.co.jp/press/html/ref20091009-01.html）

金融情報システムセンター、『金融機関等におけるセキュリティポリシー策定のための手引書（第2版）』、金融情報システムセンター、2008年

――、「クラウドコンピューティングの課題と展望」、『金融情報システム』第308号、金融情報システムセンター、2010年4月、44～78頁

経済産業省、『SaaS向けSLAガイドライン』、経済産業省、2008年1月

――、『平成21年度新世代情報セキュリティ研究開発事業（クラウドコンピューティングセキュリティ技術研究開発）公募仕様書』、経済産業省、2009年7月

佐々木良一、「クラウドとITリスクに関する考察」、『情報処理学会研究報告』第2010-CSEC-48巻第4号、情報処理学会、2010年3月

――・芦野佑樹・増渕孝延、「デジタル・フォレンジックの体系化の試みと必要技術の提案」、『日本セキュリティ・マネジメント学会誌』第20巻第2号、日本セキュリティ・マネジメント学会、2006年9月、49～61頁

情報処理推進機構、『クラウド・コンピューティング社会の基盤に関する研究会報告書』、情報処理推進機構、2010年3月

スキャン・ネットセキュリティ、『Amazon EC2へDDoS攻撃、クラウドの弱点が浮き彫り』、スキャン・ネットセキュリティ、2009年10月8日（http://www.netsecrity.ne.jp/2_14112.html）

須崎有康、「仮想マシンに潜むセキュリティ問題」、『日経コンピュータ』2010年3月号、日経BP社、2010年、144～149頁

田村裕子・宇根正志、「情報セキュリティ製品・システムの第三者評価・認証制度について：金融分野において利用していくために」、『金融研究』第27巻別冊第1号、日本銀行金融研究所、2008年、79～114頁

日本銀行、『金融機関業務のアウトソーシングに際してのリスク管理』、日本銀行、2001年4月17日

日本銀行金融機構局、『リスク管理と金融機関経営に関する調査論文―事例からみたコンピュータ・システム・リスク管理の具体策』、日本銀行金融機構局、2007年

――――、『金融機関におけるシステム外部委託の現状について―地域金融機関 377 行庫へのアンケート調査結果から―』、日本銀行金融機構局、2008 年
濱野敏彦、「クラウド・コンピューティングの概念整理（2）」、『NBL』第 919 号、2009 年 12 月、58～63 頁
堀　良彰・江藤文治・高橋健一・櫻井幸一、「クラウドコンピューティングにおけるセキュリティ研究動向」、『情報処理学会研究報告』第 2009-CSEC-47 巻第 4 号、情報処理学会、2009 年 12 月
松本　勉・加藤光幾・今井秀樹、「秘密を漏らさずに IC カードが端末を用いて計算するには」、『第 10 回情報理論とその応用シンポジウム予稿集』、情報理論とその応用学会、1987 年、17～22 頁
山崎文明、「クラウドの浸透で常識が変わる」、『日経コミュニケーションズ』2010 年 5 月号、日経 BP 社、2010 年 5 月、64～67 頁
Armbrust, Micheal, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy H. Katz, Andrew Konwinski, Gunho Lee, David A. Patterson, Ariel Rabkin, Ion Stoica, and Matei Zaharia, “Above the Clouds: A Berkeley View of Cloud Computing,” Technical Report No. UCB/EECS-2009-28, Electrical Engineering and Computer Sciences, University of Berkeley, 10 February, 2009.
Bowers, Kevin, Marten van Dijk, Ari Juels, Alina Oprea, and Ronald L. Rivest, “How to Tell if Your Cloud Files Are Vulnerable to Drive Crashes,” IACR ePrint 2010/214, IACR, 2010.
Cloud Security Alliance (CSA), *Security Guidance for Critical Area of Focus in Cloud Computing, V2.1*, CSA, December, 2009.
van Dijk, Marten, Craig Gentry, Shai Halevi, and Vinod Vaikuntanathan, “Fully Homomorphic Encryption over the Integers,” *Proceedings of Eurocrypt 2010*, LNCS 6110, Springer-Verlag, May, 2010, pp. 24–43.
――――, and Ari Juels, “On the Impossibility of Cryptography Alone for Privacy-Preserving Cloud Computing,” IACR ePrint 2010/305, IACR, 2010.
European Network and Information Security Agency (ENISA), *Cloud Computing—Benefits, Risks and Recommendations for Information Security*, ENISA, 20 November, 2009 (http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/).
Gentry, Craig, *A Fully Homomorphic Encryption Scheme*, A Dissertation Submitted to the Department of Computer Science and the Committee on Graduate Studies of Stanford University, September, 2009.
Mell, Peter, and Tim Grance, *The NIST Definition of Cloud Computing, Version 15*, NIST, 7 October, 2009 (http://csrc.nist.gov/groups/SNS/cloud-computing/).
Open Cloud Manifesto (OCM), *Cloud Computing Use Cases White Paper Version 3.0*, OCM, 2 February, 2010 (http://www.opencloudmanifesto.org/).

Ristenpart, Thomas, Eran Tromer, Hovav Shacham, and Stefan Savage, “Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds,” *Proceedings of the 6th ACM Conference on Computer and Communications Security*, ACM, 2009.

Vamosi, Robert, *Gmail Cookie Stolen via Google Spreadsheets*, CNET, 14 April, 2008 (http://news.cnet.com/8301-10789_3-9918582-52.html).

Wang, Cong, Qian Wang, Kui Ren, and Wenjing Lou, “Ensuring Data Storage Security in Cloud Computing,” IACR ePrint 2009/081, IACR, 2009.

補論 1. クラウドを利用するうえで留意すべき主なリスク

ここでは、クラウドを利用するうえで留意すべき主なリスクとして、ENISA [2009] において指摘されているものを説明する。本文献では、以下のとおり、同リスクを①ポリシーや組織に関するリスク、②技術的リスク、③法的リスク、④クラウド特有でないリスクに分類したうえで、発生確率や影響度からリスクの大きさを定性的に評価している。

このようにみると、発生確率、影響度、リスクがいずれも「高」と評価されてい

項番	リスク	発生確率	影響度	リスク
ポリシーや組織に関するリスク				
R.1	データやサービスを他のクラウド提供者に移行困難である。（ロックイン）	高	中	高
R.2	クラウド提供者の情報システムに対するクラウド利用機関による統制が十分取れない。	非常に高	非常に高	高
R.3	アプリケーション特有の要件や規制への適合性をクラウド利用機関が確認できない。	非常に高	高	高
R.4	特定のクラウド利用機関等による不正行為によって、他のクラウド利用機関のアプリケーションが風評の被害を受ける。	低	高	中
R.5	クラウド提供者が営業を停止し、クラウド利用機関のアプリケーションの提供が困難になる。	（不明）	非常に高	中
R.6	クラウド提供者が買収され、同サービスの内容等が変更されてしまう。	（不明）	中	中
R.7	クラウド提供者の業務委託先において問題が発生し、クラウドのサービス提供が困難になる。	低	中	中
技術的リスク				
R.8	計算資源の配分方法等が不適切であり、必要な計算資源がタイムリーに供給されない。	中～低	（不明）	中
R.9	複数のクラウド利用機関が使用する場合に、クラウド利用機関間における計算資源の分離が不適切であり、情報漏洩等が発生する。	（不明）	非常に高	高
R.10	クラウド提供者の従業員が不正を行い、クラウド利用機関のアプリケーションにおいてセキュリティ上の問題が発生する。	中	非常に高	高
R.11	クラウドのサービスを管理するためのインタフェースに脆弱性が存在し、問題が発生する。	中	非常に高	中
R.12	クラウドの情報システム内における通信データが傍受され、機密データが漏洩する。	中	高	中
R.13	クラウド提供者とクラウド利用機関との間の通信データが傍受され、機密データが漏洩する。	中	高	中
R.14	サービスの利用終了時に、クラウドにおいて管理されるデータを完全に消去困難である。	中	非常に高	中
R.15	分散型サービス拒否攻撃（Distributed Denial of Service）が実行される。	中～低	高	中

（続き）

項番	リスク	発生確率	影響度	リスク
R.16	クラウド利用機関のアカウントを乗っ取る等の手段によって、クラウド利用機関に経済的な損害を与える攻撃（Economic Denial of Service）が行われる。	低	高	中
R.17	暗号鍵やパスワードの紛失・漏洩が発生する。	低	高	中
R.18	攻撃者がクラウドのサービスを利用し、当該クラウドの脆弱性等に関する情報を収集する。	中	中	中
R.19	仮想マシン等、クラウドの管理機構（service engine）に対して攻撃が行われる。	低	非常に高	中
R.20	クラウド利用機関とクラウド提供者の責任範囲が不明瞭であり、問題発生時にクラウド利用機関が想定外の損害を被る可能性がある。	低	中	中
法的リスク				
R.21	法執行機関によるハードウエア没収や電子証拠開示（e-discovery）により、想定外の情報漏洩が発生する。	高い	中	高
R.22	データ・センターの場所によって司法管轄が変更され、想定外の法的措置等が取られる可能性がある。	非常に高	高	高
R.23	クラウドにおいて処理されるデータの保護形態が関連法令に適合しているか否かの確認が困難である。	高	高	高
R.24	クラウドにおけるソフトウエアの利用形態がその使用規約に違反している可能性がある。	中	中	中
クラウド特有ではないリスク				
R.25	クラウドにおいて使用されるネットワークに障害が発生する。	低	非常に高	中
R.26	クラウドにおいて使用されるネットワークの管理が不適切である（輻輳、接続ミス等）。	中	非常に高	高
R.27	ネットワーク上のデータが改ざんされる。	低	高	中
R.28	クラウドの管理やサービス利用における権限が乗っ取られる。	低	高	中
R.29	クラウドにおける運用上の問題から無権限者によるなりすましが可能となってしまう。	中	高	中
R.30	操作ログの紛失・改ざんが発生する。	低	中	中
R.31	セキュリティ・ログの紛失・改ざんが発生する。	低	中	中
R.32	バックアップされたデータの紛失・盗難が発生する。	低	高	中
R.33	計算資源への不正アクセスが発生する。	非常に低	高	中
R.34	計算機等のハードウエアの盗難が発生する。	非常に低	高	中
R.35	自然災害が発生し、クラウド利用機関のアプリケーションが停止する等の影響が及ぶ。	非常に低	高	中

るものは、①クラウド利用機関によるガバナンス統制の欠如（R.2）、②アプリケーションの要件や規制に対する適合性の確認困難性（R.3、R.23）、③問題発生時の司法管轄の変更（R.22）となっている。リスクに関する検討を行ううえで、これらの項目についてまず留意しておくことが重要であるといえよう。

補論 2. クラウドにおける情報セキュリティ管理の実態把握の手法に関する研究事例

クラウドにおける情報セキュリティ管理の実現に関して技術的なアプローチでの研究が、暗号や情報セキュリティの分野においても本格的に実施されはじめている。以下では、4 節(2)において説明した各手法の内容をやや詳しく紹介する。

(1) データの一貫性確認の手法

クラウド利用機関がデータの一貫性を確認するためには、データの処理に関するログ等、証拠となるデータを生成・保管しておくことが考えられる。そうした手法として、Wang, Wang, Ren, and Lou [2009] は、クラウドにおいて処理されたデータの内容をクラウド利用機関が随時確認し当該データに対してデジタル署名を生成するという手法を提案している。本手法の概略を説明すると、①クラウド提供者は、処理が実行されたデータを一定サイズに分割し（分割後のデータは“ブロック”と呼ばれる[26]）、ブロック（群）を代表するデータ（ハッシュ値）を生成する、②クラウド提供者は処理結果のデータの一部とハッシュ値をクラウド利用機関に送信する、③クラウド利用機関は、当該ハッシュ値の整合性を確認してそれに対するデジタル署名を生成するとともに、署名付きハッシュ値等をクラウド提供者に送信するという流れとなる。後日、クラウド利用機関が処理を実行したデータの一貫性を確認する際には、上記③における署名付きハッシュ値等をクラウド提供者から入手し、署名検証等を実行することになる。

本手法では、クラウド利用機関がデジタル署名を生成・検証する機能をローカルで準備する必要がある。また、頻繁に更新されるデータに関しては署名生成に伴う処理が追加的に発生するほか、署名方式として現時点では RSA 以外は利用できないといった課題が残されている[27]。

(2) データの可用性確認の手法

クラウドは、一般に、計算資源の一部がある程度の確率で故障することを前提に構成されており、(故障していない) 残りの計算資源を使用して処理を継続するなどの仕組みが採用されている。そのうえで、例えば、「本サービスにおける稼働保証は 99.9% である」といった情報がクラウド提供者から示される。ただし、データが特

26 例えば、グーグル社の分散ファイル・システム（Google File System）の場合、ファイルを 64 メガ・バイトのブロックに分割して複製を行い、それらのブロックを異なる複数のサーバーに分散させて処理を行っている。

27 このほか、クラウド提供者が自身の計算資源におけるデータ処理に関するログを取得し、第三者に証拠として提出できるように保管しておくシステムの研究も進められている（佐々木［2010］）。

定のハード・ディスクに偏って処理・保管されていた場合は、一部のハード・ディスクが故障した際にデータが失われてしまうおそれがある。

こうした問題への対策として、「一定数のハード・ディスクにおいてデータを均等に分散して処理する」というものが考えられる。そこで、Bowers *et al.* [2010] は、データが適切に分散されているか否かをデータの読出時間を手掛りにリアルタイムで検証するという手法を提案している[28]。データが複数のハード・ディスクにおいて均等に分散されている場合、各ハード・ディスクからのデータ読出しは並列的に1回で実行可能であり、読出しにかかる時間は1つのハード・ディスクからの読出しにかかる時間とほぼ同じになると予想される。これに対して、均等に分散されていない場合、データ読出しが2回連続で実行されるハード・ディスクが存在し、当該ハード・ディスクにおけるデータ読出しの時間は他のハード・ディスクの2倍程度になると予想される。こうした点を踏まえ、クラウド利用機関はデータの読出しをクラウド提供者に対してオンラインで依頼し、その応答時間が一定範囲内に納まっている場合に「データが均等に分散処理されている」と判断する。

Bowers *et al.* [2010] は、通信の遅延時間やハード・ディスク上でのデータ読出時間の分布を計測し、①検証可能なハード・ディスク数、②読出しを行うデータの量、③判定しきい値（応答時間）がそれぞれ変化したときのデータ読出時間の変化を示している。ただし、本手法を実現するためには、クラウド利用機関が「検証対象となるデータ」と「それらを処理するハード・ディスク」の対応関係を知っている必要があり、クラウド提供者による一定の情報開示が必要となる。

(3) 処理されるデータの秘匿性を確保する手法

クラウド利用機関がクラウド提供者に対して処理対象のデータを秘匿したい場合、例えば、クラウド利用機関が当該データを暗号化し、その暗号化されたデータをクラウド提供者に渡して処理を行うという手法が考えられる。このように、秘匿したいデータに関する演算（例えば、公開鍵暗号の演算）の実行を他のエンティティに依頼するというアイデアの研究（依頼計算プロトコル）が従来から行われている（松本・加藤・今井［1987］）。

最近では、データの秘匿に関する安全性が証明可能であることに加えて、当事者間におけるデータ通信量と計算量の観点で実用性が高い手法が提案されるようになってきている。例えば、Gentry [2009] や van Dijk, Gentry, Halevi, and Vaikuntanathan [2010] は、暗号方式として公開鍵暗号を利用した手法を提案しており、①インターネットのサーチ・エンジンへの検索キーワードを暗号化して当該サーバーに送信し処理を依頼するというアプリケーションや、②暗号化された電子メールをメールサーバーが復号しないでフィルタリングを行い、その結果を当該メールの受信者に

28 Bowers *et al.* [2010] は、クラウド提供者が意図的にデータを喪失させるという状況を想定した場合、技術的な対策は存在しないと記述している。

送信するというアプリケーションに適用可能であるとしている。ただし、上記論文においては当該手法の実装結果が示されておらず、今後、クラウドのサービスを想定した実験等が行われ、その有効性の確認が行われることになると考えられる。

また、van Dijk and Juels [2010] は、クラウドにおける処理の形態を分類したうえで、データの秘匿に必要な条件について検討している。その結果として、①各クラウド利用機関のデータの処理が他のクラウド利用機関のデータと独立である場合、Gentry [2009] の手法はデータの秘匿性を確保するうえで有効であることを示している。ただし、②データの処理が他のクラウド利用機関のデータに依存して実行される場合には、Gentry [2009] の手法に加えて、データ処理のプロセスの一貫性を何らかの手段[29]（例えば、耐タンパー性を有するハードウエアの利用）で確保することがデータの秘匿性を確保するうえで必要であることを示している。これらを踏まえると、クラウドにおける処理の形態によっては、暗号を用いた手法（暗号プロトコル）のみによってデータの秘匿性を確保することが困難なケースが存在する点に留意することが求められる。

29 例えば、こうした手法として、耐タンパー・ハードウエアを利用する手法や、暗号化等に用いられる秘密の情報を複数のエンティティにおいて分散管理する技術（秘密分散技術）等が候補として紹介されている。