〈クラウドの技術課題，将来展望〉

8 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

浦本直彦　日本アイ・ビー・エム（株）東京基礎研究所

はじめに

クラウドコンピューティング（Cloud Computing）は，要求に応じたサービス提供，ユビキタスなネットワークアクセス，場所に依存しない計算機資源のプーリング，迅速な弾力性，従量サービスなどの特徴を持つIT技術の新しい利用形態やビジネスモデルとして現在注目を集めている．クラウドコンピューティングがIT基盤技術として普及するために重要なチャレンジの1つがセキュリティやコンプライアンス（法令やそれに基づく企業規則の順守）の問題である．たとえば，IDCが2008年にまとめたクラウドコンピューティングにおける問題に関するサーベイでは，最大の問題としてセキュリティが挙げられている[1]（ちなみに第2位がパフォーマンス，第3位が可用性である）．また，カリフォルニア大バークレー校のArmbrustらがまとめたレポート"Above The Clouds"[2]では，クラウドコンピューティングにおける10個の阻害要因を指摘しているが，その中でも，可用性，データのロックイン，データの機密性と監査性など，セキュリティ関連の問題が挙げられている．特に，企業がクラウドコンピューティングを活用し，サービスを提供するためには，セキュリティやコンプライアンスの問題は避けて通ることができない．

クラウドコンピューティングは，物理的なデータセンタからSoftware as a Service（SaaS）のようなサービス層までを含むため，必要とされるセキュリティやコンプライアンス技術は多岐にわたる．クラウドコンピューティングが技術革新としてというより，パラダイムシフトとして語られるコンテキストにおいて，クラウド固有の技術が何かを議論することは難しいのと同じように，クラウドコンピューティング特有のセキュリティ・コンプライアンスに関する技術的な問題があるかどうかは議論が分かれるかもしれない．既存のIT基盤におけるセキュリティ技術との最大の違いは，個人や企業が所有するデータを，自己のコントロールが効かない環境で処理し，保存することに起因している．大企業を中心に，自社内，すなわち自己のコントロールが可能な場所において，上述したクラウドの特長を享受するプライベート・クラウドが注目されているのもこのためである．

本稿では，クラウドコンピューティングにおけるセキュリティやコンプライアンスに関する問題や技術，関連する法律，コミュニティの動向などについて解説する．

最初に，本稿で用いるクラウドコンピューティングの参照モデルとセキュリティフレームワークを定義する．このフレームワークに沿って，セキュリティに関するトピックを紹介し，さらに代表的な問題について解説する．

最後に，今後の課題や方向性について議論する．クラウドコンピューティングそのものについての解説は，本特集の他の解説を参照されたい．

クラウドコンピューティングの参照モデル

本章では，クラウドコンピューティングにおける簡略化された参照モデル（図-1）を定義し，本稿で用いる用語を説明する．

まず，クラウドコンピューティングの提供モデル（Delivery Model）として，以下の3つの分類を用いる．

- **Infrastructure as a Service（IaaS）**：仮想サーバ，ストレージ，ネットワークなどの計算機資源を提供するサービス．Amazon S3やEC2などがIaaSの代表例である．
- **Platform as a Service（PaaS）**：クラウド利用者が作成したアプリケーションを実行するための環境を提供するサービス．Google App EngineなどがPaaSの代表例である．
- **Software as a Service（SaaS）**：クラウド環境が提供するソフトウェアサービス．クラウド利用者はブラウザ経由で用いることが多い．Salesforce.com

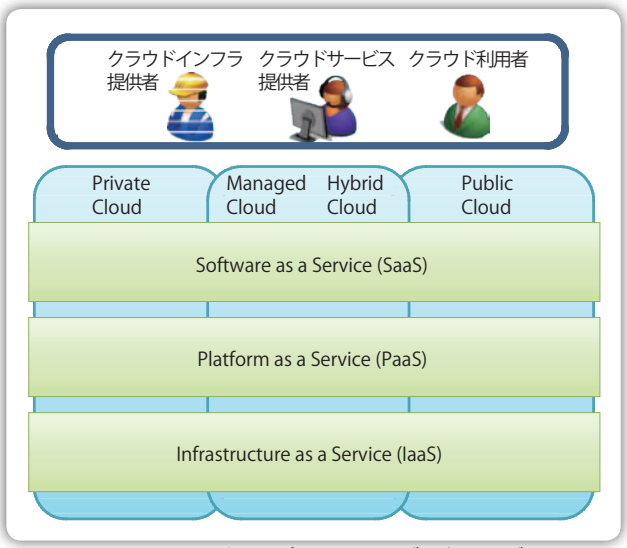

図 -1　クラウドコンピューティングの参照モデル

や Google gmail などが SaaS の代表例である．

また，配置モデル（Deployment Model）の観点からは，次の 4 つに分類される．

- **パブリック・クラウド（Public Cloud）**：インターネット経由で誰でもアクセスできるクラウド
- **プライベート・クラウド（Private Cloud）**：企業・組織内で利用されるクラウド
- **ハイブリッド・クラウド（Hybrid Cloud）**：パブリック・クラウドとプライベート・クラウドの組合せ
- **マネージド・クラウド（Managed Cloud）**：企業内（プライベート・クラウド）で，第三者が運用するクラウド，あるいは，第三者（パブリック・クラウド）がある企業専用のクラウドを提供するような形態を指す．

さらに，誰に対するセキュリティかを議論する上で，役割モデル（Role Model）も重要である．本稿では，以下の 3 つの役割を想定している．

- **クラウドインフラ提供者**：データセンタを運営する事業者．各種サービスを提供する場合もある．
- **クラウドサービス提供者**：クラウド上で，さまざまな（複合）サービスを提供する事業者．クラウドインフラおよびサービス提供者をまとめてクラウド提供者と呼ぶ．
- **クラウド利用者**：クラウドサービスを利用する企業および個人ユーザ．

クラウドコンピューティングにおけるセキュリティフレームワーク

クラウドコンピューティング全体は物理層からサービス層に至る多層のスタックで構成され，個々の層において，異なるセキュリティ上の問題が生じる．本稿では，セキュリティフレームワークとして，IBM が用いているセキュリティフレームワーク [3] を用いる．このフレームワークは，一般的な IT システム向けに設計されたものであるが，クラウドコンピューティングの各層に対応付けることが可能であり，本稿での議論ではこれを用いる．図 -2 に，セキュリティフレームワークのスタックを示す．

1. **人とアイデンティティ管理**：適切なアクセス権を持つ人物が，適切な資産，適切な時間にアクセスすることを保証する．クラウド環境においては，クラウド環境ごとに異なる認証（ログイン）・認可（アクセス制御）の仕組みを統一的に用いるために，アイデンティティ（たとえば，ユーザ ID や，物理的なトークン，公開鍵証明書などで表現される）をどのように連携するか（Federated Identity）が大きな問題となっている．
2. **データ保護・情報管理**：重要データの移動，保管のライフサイクルにおける保護を行う．前述したように，セキュリティの観点からは，クラウドコンピューティングと従来のコンピューティングとの違いは，データ処理を自前で行うのではなく，他者が所有しコントロールする計算機環境上で行う点にある．クラウド環境においては，複数のユーザが同一の計算機資源を共有するため，データやその処理手順が他のユーザに漏洩する危険性がある．また，クラウド提供者に対しても，データを隠ぺいすることが必要とされる場合もある．データの暗号化（とそれに付随する鍵管理）や情報漏洩防止などのデータセキュリティの問題は，クラウドコンピューティングにおける基礎問題の 1 つである．また，情報の作成あるいはロード，処理，削除といった情報のライフサイクルに沿った管理が行われる必要がある．たとえば，必要でなくなった情報の消し込みが確実に行われたかどうかを保証する仕組みが必要である．
   さらに，大規模データをどのようにしてクラウド環境に import/export するかといった問題も生じている．米 Amazon 社のクラウドサービスである Amazon Web Services（AWS）では，大規模データの移動のためにクラウド利用者がハードディスクを郵送するオフラインのサービスを開始している．ただ，ディザスタリカバリのような緊急度の高い状況にお

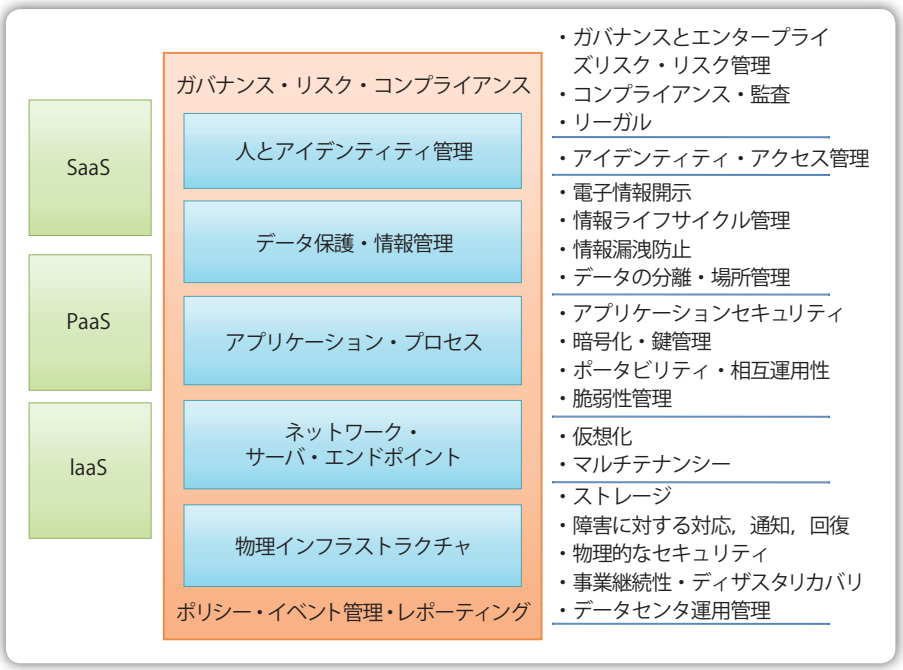

図 -2　セキュリティフレームワークのスタック

ける大規模データの移動に関しては，現在良い解決策がないのが実状である．

3. **アプリケーション・プロセス：**アプリケーションとビジネス・サービスのセキュリティを確証する．SaaS や PaaS では，クラウドは，クラウド利用者に対して，アプリケーションサービス（例：Salesforce.com の CRM サービス）や，利用者のアプリや Web サービスが配置（deploy）される環境を提供する（例：Google の AppEngine）．この層では，いわゆる Web アプリケーション一般における脆弱性に関する問題が発生する．特に，SaaS においては Ajax ベースの Web 2.0 技術を元にしたソーシャルコンピューティングサービスも多いため，新しいタイプの脅威が発生し，クラウドサービス提供者や利用者は注意を払う必要がある．
4. **ネットワーク・サーバ・エンドポイント：**システム・インフラストラクチャに対する新出する脅威に対応する．クラウドコンピューティング環境においては，クラウドインフラ提供者が運営するデータセンタにおけるセキュリティ技術が中心であり，特に後述する仮想化環境に伴う問題に注意する必要がある．また，複数の組織のユーザが同一のサーバやミドルウェアにアクセスするため，システム，ミドルウェア，あるいはアプリケーションレベルでのマルチテナンシーを考慮する必要がある．
5. **物理インフラストラクチャ：**物理的な空間において，人や計算機資源に起きる問題に対応する（物理的なセキュリティ）．データセンタの運用管理や，障害・事故への対応・通知・回復の仕組みが必要である．さらに，利用者にとっては，サービスが長期間にわたって保証されるのか（事業継続性）や，災害などの緊急時対応（ディザスタリカバリ）の仕組みが整っているかどうかが提供者選定の際の大きな要因となる．

前述したように，セキュリティ的な観点から見たクラウドコンピューティングの最大の特徴は，処理を行うデータの所有者（クラウドサービス利用者）が，自分でコントロールできない計算機環境や人員を使って処理を実行する点にある．このため，利用者は，自分のデータは安全に保管されているのか，クラウド提供者のセキュリティ管理は十分か，ユーザが求めているコンプライアンス基準を満たしているのか，サービスの可用性が保証されるのか，といった懸念を持つことになる．**図 -3** に従来の環境とクラウド環境における IT サービスの対比をまとめた．これらの懸念に対して，いかに提供者側が答えることができるかが，クラウド環境の信頼性を高めることに繋がり，そのための技術が求められている．

また，ガートナー（Gartner）の報告書[4]では，クラウドコンピューティングが抱えるセキュリティリスクとして，以下の 7 つを挙げている．

- 特権ユーザのアクセス（Privileged User Access）
- コンプライアンス（Regulatory Compliance）
- データの場所（Data Location）
- データの分離（Data Segregation）
- データのリカバリ（Recovery）

- 調査・監査に対するサポート（Investigative Support）
- 長期間の事業継続性（Long-term Viability）

ここで挙げられたどれもが，ユーザのコントロールが直接及ばない環境での処理において特に重要な項目ばかりである．また，クラウドコンピューティングにおけるセキュリティに関する非営利団体である Cloud Security Alliance（CSA）では，15 個のセキュリティに関するトピックを紹介している[5]．

従来のIT環境	クラウド環境
サーバやデータが自社で管理されている	誰が管理するのか？
サーバはXという場所にある	サーバはどこにあるのか？
データはサーバY, Zに保管されている	データはどこに保管されているか？
適切にバックアップされている	誰がどのようにバックアップを取るのか?
管理者がアクセス権を管理している	誰がアクセス権を持っているか?
稼働時間は十分である	弾力性を持ち期待されたレベルで稼働するか?
監査がきちんとなされている	どのように監査するのか?
自社のセキュリティチームが関与している	どのように自社のセキュリティチームが関与するのか？

図 -3　従来の IT 環境とクラウド環境の違い

- Cloud Architecture
  （1）クラウドコンピューティングのアーキテクチャフレームワーク
- Governing in the Cloud
  （2）ガバナンスとエンタープライズリスク管理
  （3）リーガル
  （4）（裁判などにかかわる）電子情報（証拠）開示（Electronic Discovery）
  （5）コンプライアンスと監査
  （6）情報ライフサイクル管理
  （7）ポータビリティと相互運用性
- Operating in the Cloud
  （8）事業継続性，ディザスタリカバリ
  （9）データセンタ運用管理
  （10）障害に対する対応，通知，回復
  （11）アプリケーションセキュリティ
  （12）暗号化と鍵管理
  （13）アイデンティティとアクセス管理
  （14）ストレージ
  （15）仮想化

これらのトピックを，前述したセキュリティフレームワークの各層に対応する形で示したものが図 -3 の右側である．ここから見て取れるように，技術的な問題，法律的な問題も含めて，多岐に及ぶ問題を含んでいる．本稿では，紙面の都合上，これらすべての問題について触れることはできないが，これらのトピックの中から，特に大きな議論が起こっている以下の話題について説明していく．

- 仮想化におけるセキュリティ
- データの分離と管理場所の問題
- 可用性
- アプリケーションレベルにおけるセキュリティ
- パブリッククラウドサービスにおける問題
- ガバナンス，リスク管理，コンプライアンス
- アイデンティティの連携と管理

仮想化におけるセキュリティ

クラウドコンピューティングの発展を支える技術要素の代表的なものが仮想化技術である．大規模データセンタやプライベート・クラウドにおいては，サーバ仮想化技術を使うことでサーバの稼働率を高め，コストを下げることが可能となった．パブリック・クラウドでは，Amazon EC2 や S3 に代表される仮想サーバや仮想ストレージが提供され，必要なときに必要な計算機資源を提供するための技術基盤となっている．

一方で，仮想化環境におけるセキュリティ上の問題も深刻になりつつある．IBM のセキュリティ部門である ISS の報告[6]によれば，仮想化に関する脆弱性は，2005 年頃から急速に増加している．たとえば，1 台の物理サーバの上で複数の仮想マシンが稼働している環境では，1 台のマシンがワームやマルウェアに感染した場合，仮想化環境内でのネットワークを伝わって，他の仮想マシンに感染が広がる危険性がある．また，仮想マシンを制御するレイヤであるハイパバイザーが攻撃されることで，その上で稼働する仮想サーバ群が危険にさらされる場合もある．ハイパバイザーがホスト OS 上で動いている場合には，マルウェアがホスト OS へのアクセス権を不正に取得する危険性がある．クラウド環境では，同一物理マシン上の仮想マシンが，異なる SLA やデータ機密レベルで実行されるユーザによって使用される可能性があり，サーバの孤立化や仮想ネットワークの監視などが重要な対策となる．

■データの分離と管理場所の問題

クラウドコンピューティングの特徴の1つは，データがクラウド上のどこに保存され，どこで処理されるかがユーザに対して隠ぺいされている点である．しかし，セキュリティおよびコンプライアンス上の立場からは，この問題は非常に深刻である．

米国では，2001年に米国愛国者法（USA Patriot Act）が制定され，電話や電子メール，医療情報，金融情報や他の記録について，米国当局の調査する権限が拡大された．この法律により，米国内に置かれたクラウドデータセンタのデータは，ユーザの意図にかかわらず米国当局に閲覧される可能性がある．

また，欧州では，1995年に「個人データ処理に係る個人の保持および当該データの自由な移動に関する1995年10月24日の欧州議会および理事会の95/46EC指令」が採択され，個人情報保護に関するさまざまな規定が定められた．各加盟国は，この指令を遵守するための法律や規則をそれぞれ施行している．この中で，個人データの処理のための第三国への移転は，その国が十分なレベルの保護を確保している場合に限って行うことができるとされている．このようにデータの国外あるいは地域外への移動を制限する動きは，各国にそれぞれデータセンタを置く必要がある可能性を示唆している（実際に，Amazon S3では，データの保管場所について，USとヨーロッパを指定することができるようになっている）が，クラウドの経済性を考えると，そもそも企業境界や国境を越えたサービスを提供するためには，従来の法令そのものを見直す必要があるのかもしれない．

日本では，2005年から施行されている個人情報の保護に関する法律（個人情報保護法[7]）によって，個人情報取扱事業者が個人データを第三者に委託する場合，委託先の監督責任が明記されている（第22条）．

また，クラウド利用者が何らかの事件や犯罪に関与し，そのデータが押収対象になる場合，データの保存場所によっては，当局の捜査権が及ばない可能性がある．また，物理的にデータを押収された場合に，同一ハードディスク上にあるまったく関係のないユーザのデータも押収されてしまうかもしれない．実際に，米国では，FBIがデータセンタを強制的に停止させ，機器を押収した結果，50社以上の顧客が突然サービスを受けられなくなった事例がある[8]．

そもそもクラウドコンピューティングは，企業や組織のみならず，国や地域の境界を越えた概念であるため，従来の規制や法律が適用できない場合がある．これは，クラウドコンピューティングが持つ大きな課題の1つである．

■可用性

クラウドサービスにおいて，そのサービスがどの程度安定して稼働するかは非常に重要な問題である．可用性の尺度として，99.9%や99.99%といった稼働時間（uptime）が使われる．たとえば，99.9%の稼働時間は，1年のうち8時間45分間，99.99%では52分間，99.999%では5分間の停止（downtime）を許容することを意味する．商用のクラウドサービスでは，サービスレベル合意（SLA）によってユーザと稼働時間やサービス品質に関する合意を行う．たとえば，AmazonのIaaSサービスであるEC2のSLA（aws.amazon.com/ec2-sla/）では，稼働時間が99.95%を下回った場合，料金の一部を返還するとしている．また，GoogleのSaaSサービスであるgmailは各月で99.9%のサービスレベルを保証（www.google.com/apps/intl/ja/terms/sla.html）し，それを下回った場合には無料でサービスが受けられるクレジットを提供するとしている．これに対し，過去数年の間に，主要なクラウドサービスが数時間の規模で稼働を停止したニュースがいくつも報告されている（文献9），10）など）．

クラウド提供者の信頼性を図るためにも，このようなSLAの存在は重要である．しかし，ユーザから見たクラウドサービスは，その実行環境の詳細が隠蔽されているため，SLAだけで十分であるとは必ずしも言えない．たとえば，自社でデータセンタを運用している場合は，システム障害の時期がある程度予想できる可能性があるが（システムの更新や処理が集中する時期など），クラウドサービスの障害はユーザにとってはまったく予想できない．また，障害が発生した際に，原因が何なのか，回復の時期はいつ頃かといった情報をタイムリーに得ることが難しい．クラウドサービス提供者側でも，サービスの稼働状況や障害復旧の情報などをリアルタイムで公開するサービスを提供するなどの対策を講じているところが多い．

アプリケーションレベルにおけるセキュリティ

PaaSやSaaSとして提供されるミドルウェアやアプリケーションの層では，Webアプリケーションや Webサービス，特にAjax（Asynchronous JavaScript and XML）を用いるWeb 2.0アプリケーションで指摘されている問題点の多くが当てはまる．たとえば，Googleが提供するPaaSであるGoogle App Engineでは，クラウドサービス提供者やクラウド利用者がJavaやPythonで書かれたWebアプリケーションを配置し実行させることができるが，クロスサイトスクリプティングやSQLインジェクションなどの脅威に対応したプログラムを構築す

る必要がある．また，SaaS 形式のサービスを受けるクラウド利用者は，自分が利用するサービスにセキュリティ上の問題があった場合，個人情報が盗み出されるなどの危険性が生じる．セキュアな Web アプリケーションや Web サイトを構築するために，いくつかのガイドラインが公開されている．たとえば，セキュアな Web アプリケーションや Web サービスの構築のためのツールやガイドラインを提供している非営利団体 Open Web Application Security Project（OWASP）は，300 ページにも及ぶガイドライン[11]を公開し，開発者が注意すべき原則や詳細の対策について説明している．また，日本でも，情報処理推進機構（IPA）が安全な Web サイトを構築するために，典型的な攻撃手法とその対策について解説している[12]．

すでに構築されている Web アプリケーションが脆弱性を持っているかを，ソースコードに触ることなくテストするためのツールもいくつか提供されている．これらのツールは，Web ページを自動的に解析し，さまざまなテストパターンを自動生成して適用し，脆弱性の有無をチェックする．これらのツールそのものを SaaS として提供している例もあり，Security as a Service の一例となっている．

パブリッククラウドサービスにおける問題

2009 年 7 月に，Twitter の社員が Google Apps に保管していた機密データを盗まれるという事件が起きた．これは，Web メールのパスワード回復システムの脆弱性をついて，社員のアカウント情報を盗み出すことで可能となったものである．クラウドサービスの典型例である Web メールでは，パスワードを忘れたユーザの利便性を図るため，「ペットの名前は ?」といったユーザ本人しか知らないはずの質問をすることで，パスワードの再発行を行う仕組みを提供していることが多い．しかし，特に対象となるユーザが，blog や SNS で活動している場合には，本人しか知らないはずの情報が不用意に公開されている場合がある（たとえば，日記に，愛犬と散歩したといったエントリがあるかもしれない）．また，zabasearch，isearch，pipl といった人物検索サービスを使うことで，ユーザの個人情報を入手することも可能である．パブリックなクラウドサービスでは，ユーザのアイデンティティを認定し，正規ユーザかどうかを確認するための仕組みを慎重に構築する必要があるとともに，ユーザ側も，断片的な情報から重大な個人情報を推測されないように注意する必要がある．

■ガバナンス，リスク管理，コンプライアンス

ガバナンス，リスク管理，コンプライアンス（英語の頭文字をとって GRC と呼ばれる）は，企業活動における最優先課題となっており，2001 年のエンロン社，2002 年のワールドコム社倒産の引き金となった不正会計の反省から生まれた SOX 法，2004 年に発表された銀行の自己資本比率規制のフレームワークである BASEL II などの規制を遵守することが求められている．また，医療分野における HIPAA，クレジットカード業界における PCI-DSS など，業界ごとの基準が定められており，それをクリアする IT 基盤を構築することが求められている．IaaS，PaaS，SaaS といった IT サービスを，物理資源を所有せずに利用するクラウドコンピューティングでは，利用するサービスが，ユーザにとって必要なコンプライアンス・ガバナンスレベルを満たしているかを検証する必要がある．

クラウドコンピューティングが注目される以前から，業務を外部業者に委託（アウトソーシング）することは広く行われていた．アウトソーシング事業者の内部統制に関する監査基準として知られているのが，米国公認会計士協会によって作成され，国際的にも認められている SAS-70（Statement on Auditing Standards 70）である．SAS-70 報告書にはタイプ I とタイプ II があり，タイプ I は，基準日時点における内部統制の仕組みの有効性の評価を，タイプ II は一定期間内での内部統制の運用の有効性の評価を行うものである．SAS-70 は，業務委託者と会計監査人が，受託者であるアウトソーシング事業者を評価するために用いられるものであるが，クラウド提供者が，提供するインフラおよびサービス環境の客観的評価尺度の 1 つとして，この基準を採用する場合が増えている．たとえば，Saleforce.com，Google Apps，Amazon EC2 といったクラウドサービスは，すべて，SAS-70 タイプ II の認定を受けていることを公開している．日本では，日本公認会計士協会監査基準委員会の報告書第 18 号（「委託業務に係る統制リスクの評価」）が同様の指針を示している．

また，情報セキュリティマネジメントシステム（ISMS）は，企業や組織が保護すべき情報資産についてそのセキュリティ（機密性，完全性，可用性等）を確保し，維持していくための仕組みであり，その指針が国際規格（ISO/IEC 27001）および国内規格（JIS Q 27001）として規定されている．日本では，（財）日本情報処理開発協会（JIPDEC）が，ISMS 適合性評価制度を運営している．ISMS もまたクラウド提供者の評価尺度として用いることが可能であるが，セキュリティの技術的な詳細を明確化しているわけではないため，必ずしもクラウド提供者が実際に高いレベルでセキュリティ対策を行っているかを保証するものではない．

一方で，業界ごとに具体的なセキュリティ標準を定めている場合もある．PCI DSS（Payment Card Industry Data Security Standard）は，クレジットカード業界において，カード情報および取引情報を保護するためのグローバルなセキュリティ標準であり，情報セキュリティに対する実装レベルでの要求が詳細に記載されている．また，HIPAA（Health Insurance Portability and Accountability Act）は，米国における医療情報に対するプライバシー保護やセキュリティ基準を規定した法律である．クラウドサービスが今後，企業活動の一端を担うためには，これらの基準に適合していくことが必要である．

アイデンティティの連携と管理

複数の SaaS サービスを結合させたり，パブリックな SaaS サービスと社内のサービスを連携させたりする場合，いかにユーザの認証と認可（アクセス制御）を連携（federation）し，シングルサインオン（SSO）やサービスに跨るアクセス制御を行うかも大きな問題の 1 つである．たとえば，認証については，Web サービス /SOAP の世界で使われている SAML や Liberty，Web 2.0 アプリで注目を浴びている OpenID などがあげられるが，各クラウドサービスでは，提供される認証の仕組みは現在まちまちなのが現状である．

一方で，アイデンティティ管理をクラウドサービスとして提供するベンダも登場している．たとえば，Ping Identity 社が提供するサービスでは，Salesforce.com や Google Apps のアカウントを用いて，他の SaaS サービスにログインすることができる SSO の仕組みを提供している．

おわりに

本稿では，さまざまな観点からクラウドコンピューティングにおけるセキュリティやコンプライアンスの問題について述べた．

ここで述べたように，セキュアで企業が求めるコンプライスに準拠したクラウドコンピューティングを実現するには，現時点でいくつかの課題がある．しかし，このことは，クラウドコンピューティングの普及そのものをいたずらに阻害するものであってはならないと筆者は考える．たとえば，米国国立標準技術研究所（NIST）が公開している資料 “Effectively and Securely Using the Cloud Computing Paradigm” [13] においては，クラウドが持つセキュリティ上の課題だけではなく，その利点も以下のように併記されている．

- （データの機密性を明確にし）公共データを，外部のクラウドに移すことで，内部のセンシティブなデータが公開されてしまう危険性を軽減することができる．
- クラウドが持つシステムやサービスの均質性によって，セキュリティ上の監査やテストを簡略化することができる．
- 自動化されたセキュリティ管理を導入できる．
- 冗長化やディザスタリカバリに有用である．

クラウドインフラおよびサービス提供者が実施しているセキュリティやコンプライアンスに関する方策や SLA を把握し，同等以上のレベルを自社で提供するためのコストや，処理するデータの機密性やプライバシー性を考慮しながら，いかにクラウド環境を使っていくかを考えていくことが重要である．そのために，いかにリスクを計量し，IT 基盤を設計運用していくかが，今後とも大きなチャレンジである．

参考文献

1）Balding, C.：Biggest Cloud Challenge, Security (2008). http://cloudsecurity.org/2008/10/14/biggest-cloud-challenge-security/
2）Armbrust, M., et al.：Above the Clouds, A Berkeley View of Cloud Computing (2009). http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.html
3）Introducing the IBM Security Framework and IBM Security Blueprint to Realize Business-Driven Security, IBM Redbook. http://www.redbooks.ibm.com/abstracts/REDP4528.html.
4）Gartner：Seven Cloud-computing Security Risks (2008). http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853.
5）Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing (2009). http://www.cloudsecurityalliance.org/csaguide.pdf.
6）Reports, IBM X-Force Threat (2009). http://www-935.ibm.com/services/us/iss/xforce/trendreports/.
7）個人情報の保護に関する法律, http://www5.cao.go.jp/seikatsu/kojin/houritsu/index.html
8）FBI Agents Raid Dallas Computer Business, http://cbs11tv.com/local/Core.IP.Networks.2.974706.html. http://sites.google.com/site/mnsclec/index　も参考になる．
9）Google Apps - Gmail Incident Report, http://www.google.com/appsstatus/ir/1nsexcr2jnrj1d6.pdf
10）EC2 API outage, http://developer.amazonwebservices.com/connect/thread.jspa?threadID=17211
11）OWASP：Guide to Building Secure Web Applications and Web Services, http://www.owasp.org/index.php/Category:OWASP_Guide_Project
12）情報処理推進機構（IPA）：安全なウェブサイトの作り方　改訂第 3 版，http://www.ipa.go.jp/security/vuln/documents/website_security.pdf
13）NIST, Information Technology Laboratory, Effectively and Securely Using the Cloud Computing Paradigm, http://csrc.nist.gov/organizations/fissea/2009-conference/presentations/fissea09-pmell-day3_cloud-computing.pdf.

（平成 21 年 9 月 8 日受付）

浦本直彦（正会員）

URAMOTO@jp.ibm.com

日本 IBM（株）東京基礎研究所勤務．現在は Web 基盤における性能向上やセキュリティに関するプロジェクトを担当している．博士（工学）．著作に，「XML and Java-Developing Web Applications」（Addison Wesley, 共著），「クラウド大全」（日経 BP 社，共著）などがある．