クラウドにおけるデータ保全とプライバシー問題

北　原　宗　律

（受付　2011 年 5 月 31 日）

要　　旨

クラウドコンピューティングにとって，その普及・発展の障壁になると考えられている，情報セキュリティとプライバシーの問題に焦点を当てる。そして，それらの問題状況を明示し，解決方法を探る。

キーワード　クラウド，クラウドコンピューティング，データ保全，プライバシー，個人情報保護，SaaS, PaaS, IaaS，仮想化，サーバ，ストレージ，合理的期待テスト，第三当事者原理

1. は じ め に

ここ数年来の現象であるが，コンピュータ関係の雑誌上では毎号，「クラウド」あるいは「クラウドコンピューティング」に関する特集記事が組まれている。また，それらの言葉を冠とするコンピュータ関連のカンファレンス，イベントやセミナーも大都市圏では毎日のように開催されている。あるいは，まだクラウドへの入口にいるので，その種のイベントが開催される必然性があるという見方もあろう。テレビの CM で，クラウド（雲）からキューブ状のアプリケーションが飛んでくるような様子を流しているコンピュータ企業もある。したがって，その用語だけは，すでに一般の家庭にまで入り込んでいると考えていいだろう。ただ，このコンピューティングが，これから，3 年，5 年，10年，20年継続して利用されるのだろうか，ということを考えるのは，現段階では早すぎるのだろうか。

いや，その用語だけではなく，クラウドサービスが，すでに一般の家庭にまで提供され，それとは意識しないで利活用していると考える方が現実的である。そういうことが，むしろクラウド提供企業のセールスポイントになっている。エンドユーザにとって，クラウドコンピューティングの定義，そのフレームワーク，その関連技術，その法律関係等とは無縁であっていいわけである。一般のユーザはインターネットに接続できるキーボードとモニタだけのコンピュータ（いわゆる「シンコンピュータ」）を用意するだけでいい。コンピューティングに必要なものはすべてクラウドで提供されるのである。何か問題が発生した場合には，クラウドサービスプロバイダー（CSP）が全責任を引き受けるのである。それも無過失責任

が原則であるべきである。情報事故のすべてがそうであるように，ユーザあるいはクライアント側での立証は不可能であるからである。

新しい技術に対しては，常に，同じ状況が脳裏をかすめる。クラウドあるいはクラウドコンピューティングについても例外ではない。つまり，法律及び標準機関が「仮想化」（virtualization）に対応するまでにはもう少し時間が必要である。多くの法律や技術標準が前提としているのは，物理的に顕著な事物としてサーバ（server）である。今までは，物理サーバと仮想サーバとの間の相違は現行の法律や標準の精神にとっては重要ではなかった。しかし，それにも関わらず，法律や標準は物理サーバを特殊化していた。というのは，その当時は，仮想サーバの概念は一般的ではなかったからである［Reese［2009］63］。したがって，クラウドに移動する前に，使用するアプリケーションやインフラストラクチュアに関わる法律や標準について十分理解しておかなければならない。ただ，少なくとも，CSP の SLA（Service Level Agreement）を慎重に検討する必要がある。

しかし，企業がクラウドコンピューティングを導入する場合にそれでは心許ない。当然のことながら，エンドユーザとは別の対応が求められる。ある著書において，企業がクラウドコンピューティングを導入する際の障壁が例示されている［ティム・マザー［2010］30–33］。その障壁の項目として，「セキュリティ」，「プライバシー」，「接続性とオープンアクセス」，「信頼性」，「相互運用性」，「CSP から独立」，「経済的価値」，「IT ガバナンス」，「グローバル境界による政治的問題」が挙げられている。それらの中でも，セキュリティとプライバシーが最大の障壁であると指摘されている。

本小論の目的は，前述の最大障壁の要因あるセキュリティ，すなわち，データ保全とプライバシーの問題を解明することにある。そもそも，クラウドコンピューティングとプライバシーはどこで，どのように関係するのか。プライバシーのインフレーションは留まるところを知らない。そのため，プライバシーがクラウドとも関係を持つことになる。

本小論において，まず，クラウドおよびクラウドコンピューティングの概念を明らかにしようと思う(2)。つぎに，クラウドの典型的サービスと言われるところの，クラウド・インフラストラクチュア・モデルについて検討する(3)。続いて，クラウドと情報セキュリティ(4)，および，クラウドにおけるプライバシー問題(5)について検討する。最後に，経産省が提示したクラウド社会の概略を紹介する(6)。

2. クラウドコンピューティング

2.1 クラウドコンピューティングの概念

クラウドコンピューティングを説明するほとんどの著書において，「クラウドコンピュー

ティング」（“Cloud Computing”）という言葉について，それが「バズワード」（buzzword）か否かという議論からはじまるのが通常である。ある著者によれば，「クラウドコンピューティング」という言葉は，「ウェブ」（the Web）と同じように，バズワードではないという［Reese［2009］1］。同著者は，続けて，クラウドコンピューティングとは，組織の情報技術基盤構築戦略を変更するために融合してきた様々な技術の進化した状態である，という。その証拠に，10年以上前のウェブと同様に，クラウドコンピューティングの構築においても，新技術は原則的には何も存在しない。多くの技術は，ネットスケープが現れて以降の10年以上もの間ウェブを支えてきたものである。同様に，クラウドコンピューティングを支えるほとんどの技術も何年間も身近にあったものである［Reese［2009］1］。

2.1.1　クラウド

クラウド（the cloud）はインターネット（the Internet）を表す最近の流行語ではない。クラウドにとって，インターネットは不可欠の基盤ではあるけれども，それ以上のものである。つまり，クラウドは，必要な時に必要な限り技術を利用するために移動する場所である。自分のデスクトップに何もインストールしなくてもいいし，利用していない技術に利用料金を払う必要もない。クラウドは，ソフトウェアでも技術基盤でもあり得る。ウェブや用意したサーバを介してまさに必要な時にアクセスできるアプリケーションなのである。「図書館かインターネットカフェに入り，OS やブラウザの選り好みをせずにコンピュータの前に座っても一定のサービスが受けられる。そういうサービスこそクラウドベースなのである」［Reese［2009］2］。Reese は，クラウドサービスの評価基準を以下のように述べている［Reese［2009］同］。

・そのサービスにウェブブラウザ（非所有）か API（アプリケーションプログラミングインタフェース）を介してアクセスできること。
・初期費用がゼロであること。
・利用している時間に利用しているものだけに支払うシステムであること。

クラウドサービスは，基本的には，ソフトウェアサービス，プラットフォームサービス，およびインフラストラクチュアサービスからなる。

2.1.2　ソフトウェア

「サービスとしてのソフトウェア」（SaaS：Software-as-a-Service）はクラウドにおいて提供されるソフトウェアを意味する。SaaS は，ウェブベースのソフトウェア展開モデルであり，ウェブブラウザを介してソフトウェアにアクセスできるようにしている。SaaS ソフトウェアのユーザとしては，そのソフトウェアがどこで起動しているのか，それを動かしている OS の種類は何か，どんな言語（例えば，PHP，Java，.NET）で記述されているのか，ということを気にする必要はない。もちろん，そのソフトウェアの一片たりとも自分のマシンにイン

ストールすることもない。

SaaS システムは以下のような特徴を有するものである［Reese［2009］3］。

・ウェブブラウザ上で利用できること。

・オン・デマンド方式であること。

・利用部分に対する支払方式であること。

・最少限の技術的知識で利用可能であること。

2.1.3　ハードウェア

クラウドのハードウェアを概念的にとらえるのは困難である。クラウドのソフトウェアほど簡単ではないという意味である。クラウドのハードウェアに関して，「サーバ」が必要なときには，それを注文する。約10分もすれば，それは用意（リース）されている。それとの仕事が終了した段階でリースが終了し，サーバはクラウドの中に消えてなくなる。どんな物理サーバがクラウドベースのサーバを動かしているのか知るよしもない。まして，地理上のどこに設置してあるのかさえ知る必要もない［Reese［2009］4］。

自前の物理サーバについては，キャパシティ・プラニング，冗長化問題，サーバ崩壊，サーバ廃棄，サーバ地代，サーバ電気代，等々を，常に，考えておかなければならない。

しかし，妥当なクラウドインフラストラクチュアに関しては，上述の問題は一切発生しない［Reese［2009］4–5］。クラウドインフラストラクチュアに関しては，ほとんどの機能について自ら任意にスケールすることができる。したがって，ハードウェアの負荷についての不安は不要である。また，コンフィグレーションの異なる仮想サーバへの移動やデプロビジョニングも簡単にできる。クラウドサーバを利用する際には，前述の地代や電気代を支払う必要はないのは当然であるが，CPU がアイドル状態の電気代も支払う必要がないのである［Reese［2009］5］。

3.　クラウド・インフラストラクチュア・モデル

3.1　プラットフォームサービス（PaaS）

サービスとしてのプラットフォームは，“Platform-as-a-Service” と英語表記されることから，一般に，“PaaS” と表記される。

PaaS 環境は，インフラストラクチュアのみならずアプリケーションを展開するための完璧な実行環境および開発環境を提供する。クライアントはベンダの特定のアプリケーション開発プラットフォーム上でプログラム開発を実行する。この環境に関して，すべての責任をベンダに負わせることができる［Reese［2009］17］。つまり，アプリケーション開発者がアプリケーションを開発して，プロバイダのプラットフォーム経由でサービスを提供する仕組

みである。

PaaS ソリューションは，開発ツールがクラウドにホストされ，ブラウザ経由でアクセスできるようになっている開発プラットフォームである。PaaS を利用すると，開発者は自らのコンピュータにツールをインストールすることなく，Web アプリケーションを構築することができる。それも，一般的な開発者でも Web アプリケーション開発が可能である。結局は，サーバを購入して設定するといったコストや時間をかけることなく，個人開発者や新規企業が Web ベースのアプリケーションを展開できるところから，PaaS は，Web アプリケーション開発を民主化するものだとも言われている［ティム・マザー［2010］19］。

PaaS で最も一般的に利用されているのが Google App Engine である。Google ファイルシステムとデータストレージを利用するためのツールを使用して，開発フレームワークに向かって Python 言語でアプリケーションを書く。この方法は，瞬時に展開されなければならず，重要な統合的要求事項を持たないアプリケーションには最高に機能する［Reese［2009］17］。

3.2　クラウドデプロイモデル

クラウドという表現はインターネットの比喩であり，インターネットを形成する複雑に相互に接続されたデバイスとコネクションを模した表現であるという［ティム・マザー［2010］22］。つまり，プライベートクラウドおよびパブリッククラウドはインターネットのサブセットであり，企業との関係によって，前者が内部クラウド，後者が外部クラウドと呼ばれることもある。

クラウドコンピューティングのインフラストラクチュアの大部分は，データセンタ経由で提供され，各種仮想化技術を活用したサーバにより構築された，信頼できるサービスで構成される。ネットワークインフラストラクチュアにアクセスできるところであれば，どこからでもサービスにアクセスすることができる。コンピューティングを必要とするクライアントにとっては，クラウドは単一アクセス点として見える［ティム・マザー［2010］22］。

3.2.1　パブリッククラウド

パブリッククラウド（もしくは外部クラウド）が本来のクラウドコンピューティングのことを意味している。パブリッククラウドでは，Web アプリケーションや Web サービスを通して，外部のサードパーティプロバイダからインターネットへと，きめ細かなセルフサービスにより動的にリソースが割り当てられ，プロバイダはリソースを共有し，きめ細かなユーティリティコンピューティングにより課金する［ティム・マザー［2010］22］。

3.2.2　プライベートクラウド

プライベートクラウド（もしくは内部クラウド）は，プライベートネットワーク上でクラ

ウドをエミュレートして提供する。プライベートクラウド製品は，組織により購入，構築，管理する必要があり，そのため，先行投資や現場管理において低コストの恩恵を受けることはできない。その上，プライベートクラウドの運用責任はプライベートクラウドの顧客自身にある［ティム・マザー［2010］23］。プライベートクラウドでは，その性格上，ネットワーク，コンピューティングおよびストレージインフラストラクチュアは，その組織専用であって，他とは共有されていない。この点がパブリッククラウドとは異なっている。

3.2.3　ハイブリッドクラウド

ハイブリッドクラウドとは，内部プロバイダおよび外部プロバイダによって構成される。ハイブリッドクラウドを利用すると，コアでないアプリケーションはパブリッククラウドで実行し，コアとなるアプリケーションや慎重に扱うべき社内データの管理はプライベートクラウドで実行することができる［ティム・マザー［2010］24］。

4.　クラウドと情報セキュリティ

4.1　データセキュリティ

物理的セキュリティとは，情報インフラストラクチュアをサポートするサーバへの物理的アクセスコントロールを意味する。クラウドは，依然として，物理的セキュリティに関する制約を持っている。あるクラウドプロバイダを選択したときに，同社の物理的セキュリティ方針を熟知すべきであり，物理的脆弱性からシステムを守るために必要なことを理解すべきである［Reese［2009］99］。

実務上の問題は，自己のビジネスとは関係のない要因が業務及びそのデータを飲み込む場合である。例えば，クラウドプロバイダが破産宣告を受け，そのサーバが押収され，業務が止まってしまうことがある。また，自己とは無関係の第三者が，サービスを受けているクラウドプロバイダを訴え，そのクラウドプロバイダの保有するすべてのサーバへのアクセス権を与えるような白紙召喚状を手に入れることが考えられる。

データの暗号化は前述のシナリオへの対抗措置である。召喚状はデータ及びデータへのすべてのアクセス権限をプロバイダに引き渡すことを強制することになるであろう。しかし，プロバイダがクライアントが保有するアクセス権限や複号化キーを持っていることはない。問題のデータを入手するため，裁判所は，クライアントを召喚しなければならない。その結果，プライベートデータセンタで持っていたものと同レベルのコントロール権に終止符を打つことになる［Reese［2009］101］。

4.2　ネットワークセキュリティ

4.2.1　ファイヤーウォール

ファイヤーウォールは，典型的には，一つまたは数個のネットワークセグメントの周囲を保護する。メインのファイヤーウォールは外側の周囲を保護する。ただ，HTTP，HTTPS 及び FTP（時々）のトラフィックは許可する。ネットワークセグメント内では，ロードバランサ（負荷分散装置）のようなボーダシステムがあり，別のファイヤーウォールに保護された DMZ（非武装地帯）へとトラフィックを導く。最後に，DMZ 内では，アプリケーションサーバが高機密の内部ネットワーク上の保護されたシステムの中に第三のファイヤーウォールを介してデータベースやその他のリクエストを創出する［Reese［2009］106］。

このような構造は，ネットワーク保護のための複数のレイヤ（または周囲）を行き来することになるが，何層かのファイヤーウォールを構築することで，増加する一方の機密データへのアクセスを確実にしているのである。ペリメータ構造の利点は，DMZ の許可がない限り，内側に設定された脆弱なファイヤウォール・ルールが突然内部ネットワークをインターネットにさらけ出すことはないのである。その上，外側レイヤのサービスは，インターネットの脆弱性に対してより強固になっているのである。他方，内部サービスはインターネットの接続性は高くない。

4.2.2　ネットワーク侵入検知

ペリメータ・セキュリティには，Snort のような「ネットワーク侵入検知システム」（NIDS）を含むことが多い。NIDS はイレギュラーに見える何物かのためのローカルなトラフィックをモニタする。イレギュラーなトラフィックとして，ポートスキャン，DoS 攻撃や既知脆弱性悪用などがある。

4.3　ホストセキュリティ

ホストセキュリティとは，つぎの三つのタスクのためにサーバがどのように構築されているかを記述することである［Reese［2009］114］。

・アタックを防止すること。

・システム全体へのアタックが成功した場合，その影響を最小化すること。

・仕掛けられているアタックへ応答すること。

現実の世界では，アタックを防止する最善の方法は，ソフトウェアがセキュリティホールを持っていることを推測することである。

4.3.1　システム強化

ある特定のサービスプロファイルのコンフィグレーションを見つけたならば，イメージを作り上げる前に，そのシステムを強化すべきである。

サーバの強化することは，不必要なサービスを不能化または削除したり，不要なユーザアカウントを削除するプロセスである。

4.3.2　アンチウイルス・プロテクション

いくつかの規則や基準はサーバ上でのアンチウイルス（AV）システムの実行を求めている。それは明らかに議論の的になる問題である。というのは，効果的な AV システムは，それ自身，攻撃的機能を持っており，ある OS 上では，既知のウイルスに対する撃退率は比較的高い。個人的には，AV システムについては複雑な感情を抱いている。そのシステムは，確かに，ある環境においては必要ではあるが，他ではリスクになることもある。例えば，もし，ウイルスをばらまくために使用されるかもしれないような写真やファイルのアップロードを受け入れているならば，そのウイルスの広がりを手助けするようなことから自分のサイトを保護するために何らかのアンチウイルスソフトウエアを使用する義務がある。

不幸にも，すべての AV システムが同じように構築されるとは限らない。システム間で差があることは自明のことである。結局，あるサーバは，ウイルス，ワーム，トロージャン・ヴァイアブル・アタック・ヴェクタを作り出すようなオペレーショナルプロファイルをただ持っていないだけである。それゆえ，白紙の AV カバレッジを要求する基準，規制および要請が問題となる。AV 問題を見たときに，まず，要求は何かを理解すべきである。AV の実行を要求されているならば，確実にそれを実行すべきである［Reese［2009］114–115］。

5.　クラウドとプライバシー問題

5.1　クラウドにおけるプライバシー問題

それなりに知識のあるコンピュータユーザならだれもが，クラウドに個人メールを保存して，クラウドに写真を保存して，CSP（クラウドサービスプロバイダ）から楽曲を購入している。SNS サイト（Facebook，LinkedIn，MySpace など）には，友人とコラボレーションするためにプロフィールなどの個人情報を保存している。そして，クラウドで道案内を調べて，クラウドでサイトを開発し，クラウドで他人とコラボレーションしている［ティム・マザー［2010］27］。

クラウドコンピューティングにおいても，依然として，プライバシー問題を考えなければならない。「プライバシー」の意味，表現については，改めて議論さるべき重要な問題ではあるが，ここでは，深くそのことに立ち入らない。クラウドに固有のプライバシー問題を明らかにすることが本章の目的である。

プライバシー擁護派はクラウドコンピューティングについて，数々の懸念を挙げている。しかし，「こうした懸念は，『セキュリティとプライバシーを混同している』ことから生ずる

ものであり，知っておくべき検討課題について，さらにいくつか挙げておこう」と，マザーらはいう［ティム・マザー［2010］, 148］。その著者らによれば,「アクセス」,「コンプライアンス」,「ストレージ」,「保持」,「破棄」,「監査とモニタリング」，および,「プライバシー侵害」という項目について検討する必要があるという［[同書］148–150］。

5.1.1　アクセス

情報主体には，どんな個人情報が保持されているかを知り，場合によっては，保持するのをやめるよう要求する権利がある。これは特に，マーケティング活動において重要になる。管轄によっては，マーケティング活動にはさらなる規制が課せられている。このような規制を適用されている組織は，ほとんどの場合，エンドユーザプライバシーポリシーによって対処している。クラウドにおいて，大きな懸念となるのは,「組織が個人に対して，すべての個人情報へのアクセスを提供できるのか，そして，規定されている要求に従うことができるのか」ということである［ティム・マザー［2010］149］。さらに，情報主体がこの権利を行使して，データを削除するよう組織に求めたとき，組織はクラウドにある情報をすべて確実に削除することができるのかという疑問が提示される［同上］。

5.1.2　コンプライアンス

ここでは，まず,「クラウドにおけるプライバシーコンプライアンス要件」，つまり,「個人情報を管理する上で，どんな法律，規制，標準，契約上のコミットメントが適用されるのか」ということが問われる。つぎに,「コンプライアンスを維持する責任は誰にあるのか」，あるいは,「クラウドへの移行によって，既存のコンプライアンス要件はどのような影響を受けるのか」ということが問題となる［ティム・マザー［2010］149］。

5.1.3　ストレージ

クラウドのデータはどこに格納されるのか。別の国にある別のデータセンタに転送されるのか。同じ CSP を使っている別の組織の情報と混在してしまうのか。各国のプライバシーに関する法律では，組織が個人情報のような情報を別の国に転送することを制限している。データをクラウドに格納すると，組織の知らないところでこうした転送が行われてしまい，現地の法律に違反するおそれがある［ティム・マザー［2010］149］。

5.1.4　保持

クラウドに転送された個人データは，どれくらいの期間保持されるのか。どんな保持ポリシーでデータを管理しているのか。データを保持しているのは組織なのか，それとも CSP なのか。だれがクラウドにおける保持ポリシーを実施するのか，ポリシーの例外（訴訟ホールド（証拠保存：訴訟，調査，監査に関する文書の保存義務）など）はどのように管理されるのか［同上］。

5.1.5　破棄

保持期間終了時，クラウドプロバイダはどのように PII（パーソナリティ・アイデンティファイアブル・インフォメーション）を破棄するのか。CSP が正しい時点で PII を破棄して，他のクラウドユーザからその情報が利用できなくなったことを，組織はどのように確認するのか。CSP が余計なコピーをしていないという保証はあるのか。

クラウドストレージプロバイダは通常，複数のシステムやサイトにデータを複製している。これによって可用性が高まるが，しかし，組織がデータを破棄するとき，クラウドにあった情報は本当に破棄できたのだろうかという疑問が残る。つまり，CSP は本当にデータを破棄したのか。ただ，組織からアクセスできないようにしただけではないのか。CSP は情報を必要以上に保持しており，CSP 自身がデータマイニング（データの解析）に利用しているのではないかという懸念が残る［同上］。

5.1.6　監査とモニタリング

組織はどのように CSP をモニタリングするのか。どのようにすれば，PII がクラウドにあってもプライバシー要件が満たされていると，関連するステークホルダに確約できるのか［［同上］150］。

5.1.6　プライバシー侵害

どうすればプライバシー侵害が発生したことがわかるのか。その侵害発生を CSP が知らせてくれるのか。侵害通知プロセスを管理する責任は誰にあるのか。もし CSP の過失によるプライバシー侵害の法的責任が契約に含まれているなら，どのようにその契約を行使するのか。誰の過失であるかをどのように判断するのか［同上］。

5.2　クラウドにおけるプライバシー保護

5.2.1　データのライフサイクル

個人情報は組織で利用するデータの一部として管理されなければならない。そして，個人情報については，その収集から廃棄（消去）に至るまでの，いわば「個人情報の一生」が把握されていなければならない。

「データのライフサイクル」に言及するのは，プライバシー問題ではなく，「個人情報保護」に関する議論をする場合である。筆者は，プライバシー保護と個人情報保護は多くの点で重なり合うことがあるが，峻別して議論すべきである，という立場である。以下のように，ここでのみ，「個人情報の保護」という用語が登場する。

クラウドにおける個人情報の保護について検討するには，その「個人情報の一生」の各段階（フェーズ）において，クラウドがどのように影響するかを検討する必要がある［ティム・マザー［2010］146ff.］。以下で，マザーらの検討を紹介する。

フェーズ 1：情報の生成（所有権，分類，統制）

このフェーズでは，「個人情報の所有権」，つまり「データ保有に関する権利」が問題になる。組織のだれが PII（Personally Identifiable Information：個人を識別できる情報，すなわち，「個人情報」の意味である。）を保有しているのか。クラウドコンピューティングを利用しているなら，当該権利はどのように管理されているのか。

また，「いつどのように PII を分類したのか」や「クラウドコンピューティングの利用に固有のデータクラスは存在するか」という「分類」の問題がある。さらに，ガバナンス構造の問題がある。すなわち，たとえクラウドコンピューティング環境で PII が格納，処理されていたとしても，その全ライフサイクルにわたって管理，保護されていたことを確認するガバナンス構造が存在するか，ということである。

フェーズ 2：利用（内部－外部，第三者，妥当性，証拠開示手続／召喚状）

PII はそれを収集した組織の内部で利用されるのか，または外部でも利用されるのか。外部利用とする場合は，パブリッククラウドがその対象となる。第三者としての，下請業者や CSP（クラウドサービスプロバイダ）と共有している個人情報は存在するか。妥当性とは，情報利用がその収集目的と一致しているか，あるいは，クラウド内で利用することは，書式が情報主体（個人情報の本人）と結んだコミットメントに基づいて適切か，という判断に関係する。最後は，クラウドで管理されている情報は，組織が法的手続の際（ある訴訟の当事者となる）の法的要件に従えるようになっているか，という問題である。

フェーズ 3：転送（パブリックネットワークとプライベートネットワーク間，暗号化要件，アクセスコントロール）

パブリックネットワークを利用している場合，個人情報はいつクラウドに転送されるのか。そしてそれは適切に保護されているのか。また，PII は暗号化されているのか。クラウド経由で PII を送信する際，暗号化を要求する法律もある。PII がクラウドにあるとき，適切なアクセスコントロールがなされているか。

フェーズ 4：変換（派生，集約，完全性）

派生とはデータがクラウドで変換され，処理されるとき，オリジナルを保護したり利用制限を維持する必要があるか，集約とは，データがクラウドに集約されると，もはや識別される個人と合致しなくなるのか（したがってもはや PII と見なされなくなるのか），完全性とは PII がクラウドにあるとき，その完全性は維持されるのか，というような問題が発生する。

フェーズ 5：保管（アクセスコントロール，構造化－非構造化，完全性／可用性／機密性，暗号化）

アクセスコントロールとは，PII がクラウドに格納されているとき，適切なアクセスコントロールにより，知る必要がある個人だけがアクセスできるようになっているか，ということである。将来，組織がアクセス，管理できるようにするため，データはどのように格納されているかという「構造化－非構造化」の問題がある。また，情報セキュリティの目標である「完全性／可用性／機密性」は，クラウドのなかではどのように維持されているかという問題である。また，ある種の PII については，暗号化が要件にしている法律もあり，こうした要件は CSP によって遵守されているか，という問題である。

フェーズ 6：アーカイブ（法令遵守，オフサイトの考慮，メディアの懸念，保持）

法令遵守とは，PII について，アーカイブする期間，保管方法等の要件に関して，CSP がどのように遵守しているかどうかが問題となる。また，CSP が長期間オフサイト保管機能とうアーカイブ要件をサポートしているのか。さらに，情報は将来にわたってアクセス可能なメディアに保管されているのか，あるいは，ポータブルメディアに保管されているのか，誰がそのメディアを管理しているのか，もし CSP からそうしたメディアを回収する必要があったとき，組織は何ができるのか，というような「メディアの懸念」と呼ばれる問題がある。保持については，データはどれくらいの期間，CSP に保持されるのか，その保持期間は組織における保持期間と一致しているのか，という問題である。

フェーズ 7：破棄（安全，完全）

CSP は顧客から得た PII を，情報侵害の恐れなく安全に破棄しているのかという「安全性」の問題，および，情報は完全にはきされているのか，はきすると完全にデータは消去されるのか，それとも復旧できるのか，という「完全性」の問題が存在する。

5.2.2　経産省のプライバシー保護

クラウドコンピューティングを活用することにより，個人の行動履歴やセンサ情報に基づく新しいサービス創造や効率的な実空間制御実現可能性が拡がっている。現在のところ，データを保有する事業者は，プライバシー保護などへの配慮からデータの二次利用や流通には慎重になっているが，新サービスの利便性が広く認知されるに従って，サービスの受益者でもある情報主体のデータ二次利用に対する受容度が増し，データ利活用が進むことが期待される。

データの利活用がイノベーションの源泉として価値を生み出すようになると，大規模なデータを収集・蓄積した事業者が，当該データの第三者利用を制限することで，競争制限的な市場支配力を行使する可能性もある。そのため，データ解析がもたらす社会的便益を踏まえつつ，データ保有者とデータ利用者，更に当該データの情報主体の間で，データ利活用に関する健全な市場形成が進むよう，適切な競争政策や知的財産権政策を実施することが求められる［経産省［2010］27–28］。

個人情報の取扱いに関しては，「個人情報保護法第23条において，本人の同意を得ずに，個人データを第三者に提供することが禁じられており，同法第16条においては，収集時に特定された利用目的以外の目的で，本人の同意を得ずに，個人情報を取扱うことも禁じられている」とする［経産省［2010］29］。

しかし，個人情報の保管場所に関する制約はなく，委託先の監督など，個人情報保護法で規定される事項を遵守する限りにおいて，国外も含め第三者の提供するサーバ上に個人情報を保管することは可能であるとする［同上］。

データの外部保存に関しては，データを第三者のサーバへ保存することが制約される場合があるとしている。つまり，不正競争防止法の営業秘密管理指針においては，営業秘密の保護を受けるためには当該情報と他の情報とを区別して，より高度な管理を行うことを要件としていることから，社外サーバへの情報の保管が管理状況によっては，その要件を満たさない場合，その情報が営業秘密としての保護を受けられないこともあるということである［経産省［2010］33］。

5.2.3　アメリカのプライバシー保護

プライバシーは，合衆国憲法修正第４条の下で保護されているとみるのが一般的である。同条との関係で，合衆国最高裁判所は，扱ったプライバシー事件から，一つの原理，つまり，「プライバシーの合理的期待テスト」（the reasonable-expectation-of-privacy test）を生み出した［Couillard［2009］2207］。このテストでは，２つの要件が求められる。すなわち，「人が物体（object）に対してプライバシーの主観的期待を明示していたこと」(1)と「その期待は合理的であったこと」(2)である。

プライバシーの合理的期待は，内容物を隠蔽するための容器（コンテナ）の状況及び利用に照らして評価される。したがって，鍵のかかっていない入れ物（コンテナ）でも，その内容物が合理的に隠蔽されている限り法律的な保護を受ける。また，隠蔽の方法に加えて，内容物の中身も考慮される。高校生のバックパック（リュックサック）と財布の中身については，以下のように判断されている。すなわち，「高校は，生徒にとって，家とは異なるもうひとつの家である。高校生は，鍵や小銭，写真，手紙，日記のような高度に個人的なものを持ち歩くのである。高校生たちはその持ち物にプライバシーの合理的期待を抱いており，それらの持ち物は修正第４条の下で保護される」［Couillard［2009］2210］。

プライバシーに関する判決の中で，「第三当事者原理」（the third-party doctrine）が取引データに適用されることもある。つまり，電話通話において，通話内容に関して，相手方に対しては，プライバシーの期待は喪失するというものである。税務記録，銀行記録，通話に使用した電話番号等は本人の同意の下に相手方に送信されたものであるため，それらに対するプライバシーの期待は保持できないとされている［Couillard［2009］2214］。

Web2.0 の社会において，裁判所も変化してきた。その数年間において，消費から参加へとインターネットの利用方法が変化してきた。ユーザは様々なアプリケーションを駆使し，自己のパソコンよりも遠くにデータを格納するようになってきた。すなわち，電子メールや写真，カレンダー，自作の文書などをアウトソースする方法で Google のようなサービスプロバイダのストレージを利用するようになった［Gouillard［2009］2215］。

裁判所は従来の技術への類推によって新技術に対応してきた。同様に，先例への類推によって新しい法理論の適切な根拠を発見してきた。しかしながら，それらの裁判所の判断からは，クラウドに格納されたデータに修正第 4 条が如何に適用されるかについてのガイドライン的なものはほとんど見えてこない［Couillard［2009］2219］。

そこで，個人及び組織がビジネスを行い，データを格納するのにクラウドを利用することが増えている状況下で，政府が憲法の要請を満たすような調査を実施する明確なフレームワークを持つことが重要である。まず，裁判所は，インターネットは発展途上にあり，ある環境下で人々は自己の私的な目的のためにクラウドにいろいろなものを置いているという事実を認識しなければならない。第二に，バーチャル・コンテナ理論が一般的に考慮さるべきである。この理論の下では，隠蔽のためのバーチャルな方法，すなわち，暗号化，パスワードがプライバシーの主観的に合理的な期待を満たしていると認識さるべきである。最後に，第三当事者原理は，デジタル足跡についての社会の期待へと合理的に向けらるべきである。オンラインに格納されたファイルは，その内容は第三者に見られることを意図したものでも求められたものでもないし，バーチャルな内容の正統な保護を尊重するための URL やパスワードのような一種の準取引に対する実際的な期待を生ずるのであるから，取引データの意味はない［Couillard［2009］2231ff.］。

修正第 4 条の下で，クラウドコンピューティングにおけるプライバシーの利益が認められるためには，内容物に対する合理的な隠蔽の努力が必要である。そうすると，Web サイトを一つのコンテナに見立て，サイト内のコンテンツはパスワードロックにより隠蔽されていると類推することになる。また，修正第 4 条は，隠蔽の方法として，封筒の使用を認めるが，暗号化は除外されている。これに対して，Couillard は，「現在の暗号化は複雑でほとんど解読不可能である。封筒の封をする，バッグのジッパーを閉めるということが隠蔽のための合理的努力と認められているのに，暗号化は除外されている」という［Couillard［2009］2234］。

現在，企業も個人もクラウドへ移動している。そして，今までのハードドライブより便利で安価なものとして，クラウドに様々な情報を格納している。その姿は，まるで家のパソコンを使用する姿と全く同じである。可用性は高まり，パスワードや暗号化というようなバーチャルな隠蔽ツールの利用が，プライバシーの期待を主観的にも合理的なものにしている

［Couillard［2009］2238］。

6. クラウドコンピューティング社会

6.1 クラウド社会のコンセプト

クラウドコンピューティングの定義を模索する前に，日本の「クラウドコンピューティング社会」（Cloud Computing Society）の社会像を探って見ることにする。それは，「クラウドコンピューティングを導入・活用することによって実現される社会」である［経産省［2010］18］。

情報通信技術が牽引するイノベーションの主役は，2000年代以降，インターネットと Web を活用した新サービスへと移行してきており，ビジネスのイノベーションを支えたのは実験的精神であると言われる。クラウドコンピューティングはユーティリティコンピューティングという別名を持っており，それが実験者精神を一層喚起するプラットフォームとなる。ネットワークで接続された大規模な情報処理基盤を万人が活用できる社会が到来すると，ベンチャーの事業創出や既存企業の新事業進出から個人の創造活動に至るまで，イノベーション参加者の裾野が飛躍的に広がることが期待される。すなわち，クラウドコンピューティング社会は，「万人がイノベーションに参画する社会」である［経産省［2010］18］。

前述のイノベーションの創発は，センサ情報や行動履歴などの生活情報を解析して個々人のニーズを汲み取った広告・勧奨などを行うことによって消費財・サービスの需要を喚起するとともに，実空間の行動と密着した拡張現実や健康・疾病管理，防犯，介護・見守りサービスといった新たな消費者向け（B2C）サービスの創造に繋がる。

個人生活を支える社会システムについても，情報を双方向でやり取りできる高機能端末・機器をネットワークでつなぐことにより，仮想空間（クラウドコンピューティング）から実空間を制御して，エネルギー・水道・交通網といった社会インフラストラクチュアを効率化・高度化することが期待される。低炭素社会をはじめとする社会的課題の解決を図りつつ生産性向上や経済成長を図る，社会大のイノベーションの基礎として有望である。すなわち，クラウドコンピューティング社会は，「個人生活の便利さ，豊かさと社会の効率性が両立する社会」である［経産省［2010］18–19］。

インターネットが国民生活に広く普及することにより，組織から個人への情報提供手段が電子的になり，リアルタイムに行うことが可能となった。クラウドコンピューティングを活用することにより，1 対 n のサービスから n 対 n のコミュニケーション・コラボレーションの高度化を実現することが可能となる。すなわち，クラウウドコンピューティング社会は，「人と人とがつながり，全ての市民が社会参加する社会」である［経産省［2010］22］。

6.2 クラウド社会の提供サービス

購買行動や交通手段利用の履歴情報をはじめ，個人に関わる情報が大量に作り出されサイバー空間に蓄積されるようになっている。こうした大量の個人情報の大部分は限られた利活用に限定されている現状から，膨大な計算処理能力とストレージを経済的に利用可能なクラウドコンピューティングを活用することによって，分野横断的な情報分析が可能となり，新たなイノベーションを想像することが期待できる［経産省［2010］19］。

その例として，クレジットカードの使用履歴情報の活用が見込まれている。携帯端末の位置情報や動線情報などとあわせて解析することにより，利用者の居場所や行動に応じて，お勧めの店舗情報などをリアルタイムに配信するサービスが実現可能になる。また，医療分野においては，加速度センサなどの情報や，フィットネスジムの履歴，投薬情報などを踏まえて，個人ごとに最適かつリアルタイムなヘルスケアアドバイスを提供することにより，国民の疾病予防効果の向上を図ることが期待できる［同上］。

センサ情報など情報量が膨大で解析する方法がないために，利活用が行われて来なかった分野で，クラウドコンピューティングを活用することで，潜在的なサービスを現実化することが期待できる分野がある［経産省［2010］20］。交通分野においては，プローブ情報と呼ばれる，自動車から取得可能なブレーキ・ワイパ・速度などの情報をセンサで取得し解析することにより，より安全に走行するための情報を運転手にリアルタイムに伝達することが可能になる。その結果，交通事故の削減や最適走行による CO_2 排出量の削減が期待できる。農業分野においては，センサを搭載した無線発信装置のネットワークを農場に張り巡らせ，気温，土壌温度，相対湿度，土壌分量，光，風速，葉の湿り具合や気圧などを直接測定し解析することにより，作物の生長などに合わせて葉の除去や肥料の追加，必要最低限の農薬散布などが可能となり，生産性が大きく向上することが期待できる。

6.3 全市民参加型社会の実現

企業では，組織と在宅勤務者を結ぶテレワークが普及しつつある。今後，多地点同時接続 TV 会議システムや企業内 SNS を活用し，様々な場所で働く勤務者同士のコミュニケーションを円滑に実現することで，在宅勤務者の生産性の向上を図ることが期待できる。

教育現場では，児童同士が宿題や試験に関する内容に関して安全・安心に議論したり，教え合ったりすることが可能なネットワークが実現されれば，学習意欲向上を図ることが期待できる。さらに，児童同士の議論の内容を教材作成に活用することができれば，より学習効果の高い教材の開発が可能となる［経産省［2010］22–23］。

クラウドコンピューティングの普及を支える要素として，利用者側端末の高度化・スマート化も欠くことはできない。近年，急速に普及しつつある電子書籍やスマートフォンなどは，

端末側で行う処理とクラウドコンピューティング側で行う処理を巧みに融合することで，利用者に高い利便性を提供可能とした。今後も様々な分野で，クラウドコンピューティングと融合し，ユーザビリティの高さと高速処理を両立した高機能・高性能端末が発展していくであろう［経産省［2010］23］。

7. お わ り に

クラウドコンピューティングも，その立場の違いによって，さまざまに定義されている。ただ，定義それ自体はたいして重要ではないだろう。また，バズワードかどうかという議論も実り多いものではない。筆者としては，Reese のクライテリアに加担したい。すなわち，「1）初期費用はゼロ。2）ウェブブラウザ上で利用できること。3）オン・デマンド方式であること。4）利用部分に対する支払方式であること。5）最少限の技術的知識で利用可能であること。」という五要件を満足するものであれば，それを，「クラウドコンピューティング」と呼ぶことにする。加えて，ユーザあるいはクライアント側の端末はいわゆる「シンコンピュータ」を用意するだけで十分でなければならない。すべては雲の上にあるのだから。「クラウド」と聞いて，「ノンちゃん雲にのる」という幼稚園児の本のことを思い出したり，「幸せは雲の上に」と口笛を吹くぐらいのことをやっても許されよう。

クラウドにおけるプライバシー問題といいながら，その解決手法として，個人情報保護措置に言及している。やはり，プライバシー保護と個人情報保護とは区別して議論されなければならないように思われる。個人情報のライフサイクルの把握は，個人情報保護の分野では「データ監査」という手法である［北原［2006］200ff.］。クラウドに格納された個人情報が，どのようにデータ処理（利用・提供・消去）されているのか，データ主体にはそれを知る権利がある。つまり，自己の個人情報のライフサイクルを把握しておかねばならないのである。特に，アメリカのプライバシー論議には，情報（データ）主体の権利・利益に関する議論が欠落している。

イギリスでは，「データ保護法」という法律を持っていることから，前述の同じ問題を，やはり，「データ保護」という観点・手法を用いて議論していることが伺われる［Machini［2010］43ff.］。クラウドサービスプロバイダも個人データを取り扱うことになるので，同法が CSP にも適用されるのである。当然のことである。

もう何年も前から，「プライバシー影響評価（PIA）」が，カナダ，オーストラリア，米国等で導入されている。PIA は，個人情報の収集を伴う情報システム導入・改修にあたり，プライバシーへの影響を事前に評価し，問題回避・緩和のための運用・技術の変更を促す一連のプロセスである。IT システム稼働後のプライバシーリスクを最小限に抑える管理手法のひ

とつといえる。それらば，クラウドの導入は，PIA の対象にはならないのだろうか［瀬戸［2010］］。

クラウドあるいはクラウドコンピューティングは決して新しい技術ではないと強調されてきた。クラウドを支える技術一つひとつはここ10年以上も情報社会において使い古されてきたものである。しかし，クラウドにまつわるいろいろな問題が提起されるや，それらの解決の入り口に到達することすら，如何に困難であるかを肌身で感じ取った次第である。

クラウドを支える一つひとつ技術は，使い古されたものであるが，それらが融合することで，全く新規の利用方法が，全く新しい情報サービスが生まれたと考えるしか方法はない。そして，歴史は継続している。それならば，常套手段として，法的先例の類推的探究方法，先行技術の類推的探究方法によって，解答を模索することが残されている。

参　考　文　献

［1］ Solove［2004］: Daniel J. Solove, *The Digital Person: Technology and Privacy in the Information Age*, New York Univ. Press 2004.

［2］ 北原［2006］：北原宗律「イギリス・データ保護法におけるデータ監査とコンプライアンス」経済科学研究第９巻第２号2006年，199–223頁。

［3］ Zittrain［2008］: Jonathan Zittrain, *The Future of the Internet-And How to Stop It*, Yale Univ. Press 2008.

［4］ Solove［2008］: Daniel J. Solve, *Understanding Privacy*, Harvard Univ. Press 2008.

［5］ Fina［2008］: Siegfried Fina（ed.）, *European Union E-Commerce Law*, Stanford Univ. Press 2008.

［6］ Reese［2009］: George Reese, *Cloud Application Architectures: Building Applications and Infrastructure in the Cloud*, O'REILLY 2009.

［7］ Mather［2009］: Tim Mather/Subra Kumaraswamy/Shahed Latif, *Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance*, O'REILLY 2009.

［8］ Matwyshyn［2009］: Andrea M. Matrwyshyn, *Harboring Data: Information Security, Law and the Corporation*, Stanford Univ. Press 2009.

［9］ Coiillard［2009］: David A. Couillard, Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing, Minnesota Law Review 2009, 93: 2205, pp. 2205–2239.

［10］ 城田［2009］：城田真琴『クラウドの衝撃』東洋経済新報社2009年。

［11］ Buffington［2010］: Jason Buffington, *Data Protection for Virtual Data Centers*, WILEY 2010.

［12］ Murray［2010］: Andrew Murray, *Information Technology Law: The Law and Society*, Oxford Univ. Press 2010.

［13］ Machini［2010］: Renzo Marchini, *Cloud Computing: A Practical Introduction to the Legal Issues*, BSI 2010.

［14］ NRI［2010］：NRI セキュアテクノロジーズ編『クラウド時代の情報セキュリティ』日経 BP 社2010年。

［15］ ティム・マザー［2010］：ティム・マザー／サブラ・クマラスワミ／シャヘド・ラティフ『クラウドセキュリティ＆プライバシー－リスクとコンプライアンスに対する企業の視点』オライリー・ジャパン2010年。

［16］ 経産省［2010］：経済産業省『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』2010年。

［17］ 瀬戸［2010］：瀬戸洋一他『プライバシー影響評価 PIA と個人情報保護』中央経済社2010年。