解説

クラウド・セキュリティ・ガイダンス

日本クラウドセキュリティアライアンス

特定非営利活動法人

ASP・SaaS インダストリ・コンソーシアム

はじめに

本解説は、CSA クラウド・セキュリティ・ガイダンス　ver. 1.0.（以下、　クラウド・セキュリティ・ガイダンスという）を、主として日本のクラウドサービスの提供者・利用組織(以下、便宜上、利用者という)に分かりやすく理解してもらうことを念頭に作成された。　その全体構成は、Ⅰ　導入・実装ハンドブック編　と　Ⅱ　法律問題編　から成る。

「導入・実装ハンドブック編」は、クラウドコンピューティングの利用・導入に際してＩＴポリシーおよびマネジメントシステムのなかに如何にクラウドサービスを位置づけて構築するかという点に関する解説している。

クラウドサービスの利用者が、その利用にともなって、従来の IT マネジメントシステムやそれの中核をなす IT ポリシー（以下、IT ポリシーという）にどのような修正等を加え、どのような手順を踏んで、クラウドサービスを利用すべきかという点について、特に留意すべき事項について解説を加えている。

「法律問題編」は、クラウド・セキュリティ・ガイダンスが背景としている米国の法律知識について乏しい読者においても、理解に必要なかぎりで、米国の法律と日本の法律の関係する部分を並列的に論じるようにこころがけることによって、クラウド・セキュリティ・ガイダンスの要素を深く理解してもらうことをこころがけている。

目　　次

Ⅰ　導入・実装ハンドブック編

Ⅱ　法律問題編

解説

クラウド・セキュリティ・ガイダンス

Ⅰ　導入・実装ハンドブック編

日本クラウドセキュリティアライアンス

特定非営利活動法人

ASP・SaaS インダストリ・コンソーシアム

はじめに

本解説は、CSA クラウド・セキュリティ・ガイダンス　ver. 1.0.（以下、　クラウド・セキュリティ・ガイダンスという）[1]を、主として日本のクラウドサービスの提供者・利用組織(以下、便宜上、利用者という)に分かりやすく理解してもらうことを念頭に作成された「解説　クラウド・セキュリティ・ガイダンス」のうちのクラウドコンピューティングの利用・導入に際してＩＴポリシーおよびマネジメントシステムのなかに如何にクラウドサービスを位置づけて構築するかという点に関する解説書である（以下、便宜的に、「導入・実装ハンドブック編」と呼ぶことにする）。本解説は、クラウド・セキュリティ・ガイダンスが、背景としている米国のクラウドサービスに関する独自の状況についての知識について乏しい読者においても、クラウド・セキュリティ・ガイダンスの要素を深く理解してもらうことを最大の目的としている。クラウド・セキュリティ・ガイダンスは、クラウドサービスの利用者およびクラウド事業者に対するガイダンスをともにそのガイダンスの対象範囲にしており、また、発行時期の関係もあって、背景となる知識にクラウドコンピューティングについての相当の知識があることを前提としている。そのために、 クラウド・セキュリティ・ガイダンスは、クラウドサービスを利用したいと考える利用者が、どのような点を考慮して、クラウドコンピューティングの導入を検討したらいいかという手引きにするのには、ややハードルが高いのではないか、また、特に米国での議論がそのままでは日本の議論として考えるのには、十分ではないのではないかという懸念がある。本解説は、このような観点から、クラウドサ

---

[1] 正式には、“Security Guidance for Critical Areas of Focus in Cloud Computing”（ http://www.cloudsecurityalliance.org/csaguide.pdf）最新版は、バージョン 2.1 である。これの日本語訳「CSA クラウド・セキュリティ・ガイダンス　ver. 1.0.日本語版」が、株式会社インプレス R&D より発行されている。なお、本解説において、クラウド・セキュリティ・ガイダンスとして引用しているのは、この日本語訳にもとづいている。また、G〇頁としているのは、このガイダンス日本語訳の頁数によるものである。

ービスの利用者[2]が、その利用にともなって、従来のITマネジメントシステムやそれの中核をなすITポリシー[3]（以下、ITポリシーという）にどのような修正等を加え、どのような手順を踏んで、クラウドサービスを利用すべきかという点について、特に留意すべき事項[4]について解説を加えようとするものである。

なお、本解説は、特定非営利活動法人ASP･SaaSインダストリ･コンソーシアム（ASPIC）の支援をもとに、高橋郁夫が執筆しまとめられたものである。コメント等をいただいた佐藤慶浩（日本ヒューレット・パッカード）、梶本政利（日本ITガバナンス協会）の各氏、および、この企画に際して、いろいろとアイディアを提案いただいた久禮由敬、由見　浩一郎の各氏には、謝辞を申し述べる。

---

[2] ASP・SaaS 事業者が ASP・SaaS サービスを提供する際に実施すべき情報セキュリティ対策を対象とするものに ASP・SaaS の情報セキュリティ対策に関する研究会「ASP・SaaS における情報セキュリティ対策ガイドライン」がある（http://www.soumu.go.jp/menu_news/s-news/2008/pdf/080130_3_bt3.pdf）。

[3] 本解説においては、広義で使用しており、情報セキュリティを確保するための基本的な考え方の統一体（基本ポリシー、基準、実施手順を含むもの）をいう。

[4] したがって、本解説は、ITポリシもしくは情報セキュリティマネジメントシステムについての枠組を、クラウドサービスをふくめて全体的に体系的に構築するというものではない点については、留意いただきたい。

情報セキュリティマネジメントシステムの全体像については、中尾康二・中野初美・平野芳行・吉田健一郎　著「ISO/IEC 17799:2005（JIS Q 27002:2006）詳解　情報セキュリティマネジメントの実践のための規範」（日本企画協会、2007）などを参照のこと。

第１　クラウド・セキュリティ・ガイダンスのポイント

１　クラウド・セキュリティ・ガイダンスの構成

クラウド・セキュリティ・ガイダンスにおいて、ポリシー構築の問題に対応する部分は、ドメイン２「ガバナンスとエンタープライズリスクマネジメント」およびドメイン５「コンプライアンスと監査」の二つの部分を中心に成り立つものということができる。また、ドメイン６「情報ライフサイクル管理」およびドメイン７「移植性と相互運用性」も、プランニングやアカウンタビリティに関連する論点を多く含むものである。

もっとも、クラウド・セキュリティ・ガイダンスのドメインのうち、どのドメインがポリシー構築に関係するかは、各組織のポリシーがどのような内容を記載しているかによる。したがって、クラウド・セキュリティ・ガイダンスのドメインと、自分の組織のポリシーの対応表を作成して、ポリシーに関係するドメインを選択する必要がある。

以下、本解説（導入・実装ハンドブック編という）においては、これらのドメインの取り扱う問題を、日本において検討するものとする。そして、米国の制度を念頭に記載されたクラウド・セキュリティ・ガイダンスの記述をわかりやすく論じるもために、ポリシーの中でも技術面よりも、体制や管理面に対応付けられるであろうドメインを中心に取り上げて解説する。

２　問題提起について

はじめに、ドメイン２「ガバナンスとエンタープライズリスクマネジメント」およびドメイン５「コンプライアンスと監査」の二つの部分の問題提起をみてみよう。

ドメイン２において検討されている懸念は、利用者が、クラウドサービスプロバイダに対するガバナンスを喪失してしまうことや、その利用によって利用者自身のエンター

プライズリスクの測定が困難になってしまうことであり、それらの解決策が未成熟であるということである。これによって、なにか問題が起きてしまったときに、誰が責任をとるのか明確でないということである。

ドメイン５において検討されている懸念は、完全なシステムのアウトソースを行うことが、企業活動の維持を可能にして費用対効果が高いとしても、それは、コンプライアンスの観点からいって、また、そのコンプラアインスの説明責任を果たすという観点からいって、困難であるということである。しかも、そうした完全なシステムのアウトソースに関する保証業務のあり方や費用負担のあり方については大いに検討の余地があるということである。

3 ガイダンスの深い理解のために

上述のような分析に基づいたときに、どのような観点から、上述の懸念を解決してしいかなければならないのかということになる。この懸念に対する解決策を提供するためには、ガイダンスの種々の記載の、体系的かつ深い理解が必要であろうと思われる。ガイダンスの体系的かつ深い理解のためには、具体的にプランニングの問題として（１）クラウドサービスの導入（２）リスクアセスメント（３）リスク対応がポイントとなり、対応策実行後、（４）コントロールについての各観点から、問題を抽出し、その上で、実践的なセキュリティガイダンスを導くというのが、有効なものとなる。

第２　問題と考察

１　クラウドサービスの導入

「多くの企業組織では、ミッションクリティカルなサービスの提供をサポートするために、クラウドサービスにスピードと低コストを求めている。」（G41 頁）

いうまでもなく、「企業に求められているのは競争力の強化であって、コスト削減は目的ではなくて手段」[5]なわけであり、クラウドサービスのどのようなメリットによってどのようなビジネス目標を実現しようとするのかというのが最初のポイントとなる。

クラウドサービスのメリットについては、「スケール性」（セキュリティ手段がより安く実装される）、「差別化要因」（最関心課題であり、プロバイダとしては、差別化要因としうる）、「セキュリティ管理のための標準化されたインターフェース」、「資源の迅速かつ最適なスケール化」「監査および証拠収集」（仮想化マシーンの利用に応じたフォレンジック・イメージを提供しうる）、「初期値およびアップデートの適時の、効果的な適用」「資源の集中化による利益」などがあるとされている[6]。

ビジネス目標を実現するのにあたって、その目標を達成するのにあたって、どのようなプラスの影響を及ぼす事象があり、その可能性はどの程度なのか（事業機会）、ということは、基本的に考察すべき事柄である。「資源の迅速かつ最適なスケール化」（このひとつとして初期投資なしですぐに利用を開始できること）というメリットを利用す

---

[5] 佐藤慶浩「クラウドサービスで何をしたい？」（http://www.digitalforensic.jp/expanel/diarypro/diary.cgi?no=197&continue=on）

[6] ENISA　“Cloud Computing－Benefits, risks and recommendations for information security” http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment による。なお、以下、本書を ENISA 報告書という。

ることにより、ビジネス機会を活用する可能性がきわめて大きいという判断がなされれば、それによる目的達成の阻害する影響を及ぼす事象（リスク）が生じる可能性を判断して、その阻害結果に対して、どのようにマネジメントするかという点を考えなければならないということになる。

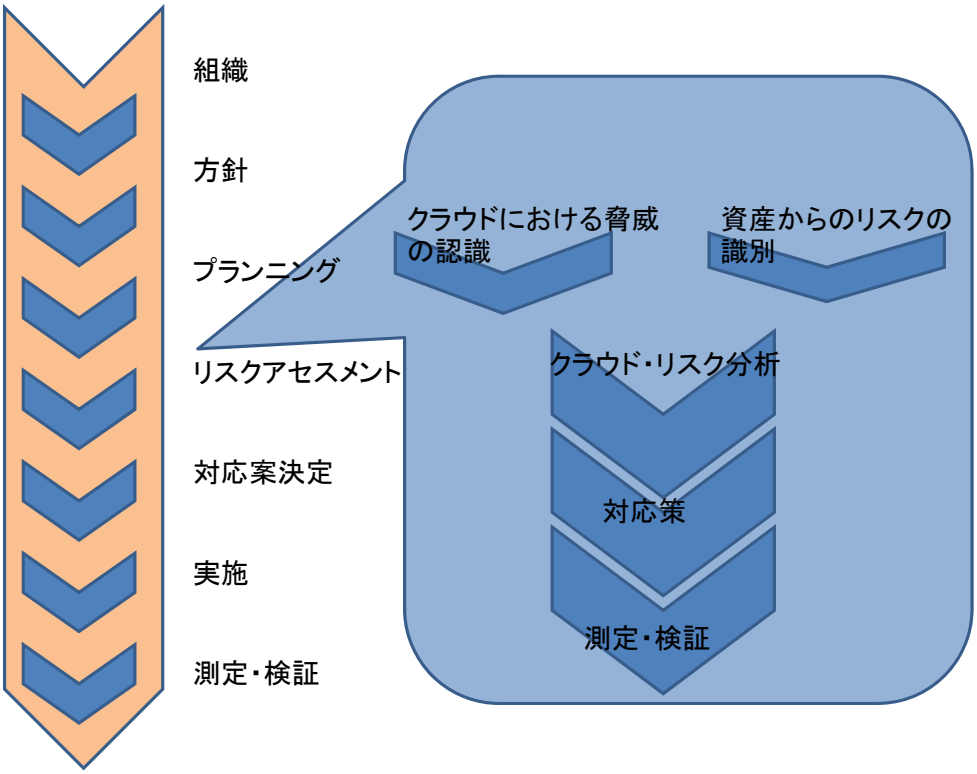
クラウドコンピューティングセキュリティ、ビジネス継続性、ディザスタリカバリーを、利用者自身のポリシーと手順に統合する（G85 頁）

前述したようにクラウドサービスを利用することが自己目的化するということはありえないのであるから、クラウドサービス利用の際に検討された事項は、最終的に利用者たる組織の情報セキュリティ一般・ＩＴポリシー一般に統合されなければならない。情報に関するリスクのマネジメントを考えたときに、利用者は、クラウドサービスの利用を考える前に、すでにマネジメントの体制を構築しているはず[7]である。　クラウドサービスの利用の際には、この存在しているマネジメント体制を前提にいくつかの点について、修正、追加、補充等をなしていくことになる[8]。この作業のうち、特に体制・管理面に関する局面を図示すると、以下のようになる。

---

[7] 羽生田和正・荒川誠実・池田秀司「ISMS 構築・認証ハンドブック　ISO／IEC　27001 対応　情報セキュリティマネジメントシステムの実例集」（日科技連、2008）29 頁は、ISMS 構築の概要として「準備・計画」「枠組み構築」「リスクマネジメント」「運用」「認証審査対応」の各段階があるとしている。

[8] JIS Q 27002:2006　6.1.4　は「情報処理設備の認可プロセスは、新しい情報処理設備に対する経営陣による認可プロセスを定め、実施することが望ましい」という。



左の矢羽は、通常のＩＴマネジメントの体制での検討手順のうち、注目すべきフェーズを示している。これに対して、右側の矢羽で記載されている分野は、クラウドサービスの採用にあたって特に留意すべきフェーズを示している。つまり、クラウドの導入・運用にあたってはリスクアセスメント・対応策の検討・対応策の採用の各論点を検討すべきであり、そしてその検討された点が統合されなければならないということである。

２　クラウドにおける脅威

2.1.ベスト・プラクティス

クラウドサービス利用へのシフトは、一方でクラウドによって実現された利用者側の IT コスト削減の一部をクラウドサービスにかかわるリスク、情報プライバシーやセキュリティの領域で強化された規制への対応に振り向ける必要がある（G41 頁）

ビジネス目標を実現するためには、その目標を実現するのにプラスの影響をおよぼす事象を最大限に活用し、マイナスの影響を及ぼす事象の影響を最小限にすることが必要になる。しかしながら、これらの事象には、明確なものから、不明確なものまであり、また、潜在的影響も重要なものから非常に重大なものまである。これらの事象を識別し、とくに、マイナスの影響をおよぼすものについては、そのマイナスの影響について、適切な対応をとらなければならない[9]。

ドメイン 1 のクラウドコンピューティングの定義はフレキシブルで事業者間の関係をダイナミックにするものであるが、同時に常にリスクマネージメントを必要とする（G15 頁）。

リスクマネージメントにおけるベストプラクティス（対策を実施するにあたっての、具体的な実施手法や注意すべき点をまとめた参考事例）は、クラウドサービスの導入・利用にとっても有効である。クラウドセキュリティアライアンスのミッションである「クラウドコンピューティングのセキュリティを確保するためのベストプラクティスの利用促進」というのは、まさに、このようなアプローチの策定と普及を目標にしているのである。

2.2. クラウドにおける脅威

では、一般のコンピューティングサービスの場合と比較して、クラウドサービスの利用に際して、どのようなリスクが、特徴のあるものとして認識されるのであろうか。CSA では、“Top Threats to Cloud Computing V1.0”を発表している。そこでは、具体的な利用に際して考慮すべきリスクというよりは、一般的なクラウドコンピューティングの問題点として「クラウドコンピューティングの不正および犯罪目的の利用（Abuse and Nefarious Use of Cloud Computing ）」、「安全ではないインターフェースおよびＡＰＩ」「悪意ある内部者」「共有技術（Shared Technology）問題」「データ消失または漏えい」「アカウントもしくはサービスのハイジャック」「未知のリス

---

9 リスク管理態勢と法律を説く資料として、濱野敏彦・浦野雄介「クラウド・コンピューティングが変える法律実務」(NBL 918 号ないし 930 号)がある（商事法務、2010）。

クのプロフィール」の７つを、クラウドコービス自体の脅威としている。また、ENISA 報告書においては、より、具体的な利用にさいしての脅威として「ガバナンスの消失」、「ロックイン」、「障害の分離」「コンプライアンス　リスク」「マネージメントのインターフェイスの毀損」「データ保護」「データ消去の不完全」「悪意ある内部者」「その他」などをあげれている。これらは、「ポリシーおよび組織的リスク」「技術的リスク」「法的リスク」「クラウドに限らないリスク」に分析されるとまとめられている[10]。

具体的なリスクを識別し、網羅的にその内容を詳論することは、この解説の目的から離れるものであるので、省略する。しかしながら、ガイダンスの種々の章において、触れられている脅威について、以下のように分類し、コメントしておくことは、後述のように情報資産ごとに脅威および脆弱性を分析するときにも有意義であろう。

（１）「第三者」の利用に伴うリスク

クラウドサービス事業者といういわば第三者からサービスを受けていることに伴って、とくに以下のリスクが発生する可能性があるということがいえる。

サービスのきめ細やかさの欠如

データの所有者は、誰が、いつ、どのような条件でデータにアクセスできるかを決定する責任を持つ（G73 頁）。

利用者は、クラウド事業者のサービスを利用するとしても、自己の情報セキュリティポリシを変更することは許されるものではない。その一方で、クラウド事業者にとっては、利用者ごとのセキュリティポリシに対応したサービス条件を提供するというのは、面倒なことになる。利用者にとって、このリスクに対する認識が低ければ、事業者を利用することで、セキュリティのレベルの低下がおきる可能性がある。「取引上の機密事項などの機密な情報に対するコントロールと公開に関して、サービス条件が適切に対応できていない」（G73 頁）というのが、情報ライフサイクル管理に関する大きなリスクとして指摘されているが、これは、このような趣旨で考えるべきであろう。

---

[10] 前出（注 6）　ENISA 報告書　25 頁以降による。

また、利用者と事業者とのコミュニケーションにおいても、きめ細やかなサービスの欠如というリスクがあるという点は、指摘される。ガイダンスにおいて、インシデントへの対応、サービスの復旧、サイト障害に対する弾力性についてのコミュニケーションが、きめ細やかでないために、ミッションクリティカルなサービスを利用することができないと指摘されている（G42 頁）。

サービス自体のレベルの問題について

第三者のサービスに依存することは、どの程度のサービスが、提供されているのかという点について、利用者が自己で管理している場合に比較して、より不確実な状況を生み出す。具体的には、「重要データの漏えいの際の責任の不明確さ」（G41 頁）という問題や「サービスの可用性以外についての不明確さ」（G42 頁）という問題が存在する。

また、これらのサービス事業者をサポートする第三者（外注業者など）について、言及もしくは定義がされることもなく、利用者において、ガバナンス上での課題やリスクをもたらしているといわれている（G42 頁）。

クラウドサービスプロバイダの事業継続性懸念について

クラウド事業者の財政的実行可能性を念頭に置かなければならない（G15 頁）。

また、第三者の事業が、契約時におけるのと同様のレベルで継続的に営まれてるとも限らない。この点については、「サービスプロバイダーの突然の倒産もしくは、サービスの中止（G55、75 頁）」「サービスプロバイダーのサービス品質がさまざまな理由により低下（同上）」「契約更新時において容認できないレベルのコストの増大（同上）」などの点が指摘されている。

データのライフサイクル管理における困難性

データに対するガバナンスは、（略）データの復元、バックアップ、オフサイト上でのストレージ、仮想化サービス提供による残余データ、契約終了に伴うデータの除去などに対する明確な基準が曖昧なためにリスクにさらされている（G42 頁）。

これらについては、「データ複数のコピーの存在（G67 頁）」「クラウドサービスプロバイダとの契約関係終了後についてのデータに関する権限の不明確さ」などが特徴的

なものとして存在する。後者については、ユーザ企業における適切な計画の必要性（G55 頁）、保存および破棄のスケジュール調整・確実性の確保の重要性などがガイダンスで説明されている（G73 頁）。また、ドメイン６「情報ライフサイクル管理」は、この点についての技術的な対応策も踏まえて記載されており、参考にされたい。

また、諸般の事情によりクラウド事業者を切り換える必要性が突然生じることもある。この場合、従前利用していたデータを移植するということになる。このような場合、移植が困難であるとか、コストがきわめて高くなるというリスクが存在する（ドメイン７「移植性と相互運用性」参照のこと）

クラウド事業者の監査に関する事項

第三者たるクラウド事業者を利用することによって問題となるリスクについて、これを監査することによって、特定し、対応策をとることが必要となる。しかしながら、これらのリスクについて、監査がきわめて困難であり高額なものになるという問題がある（G68 頁）。

（２）ネットワークを利用することによる問題

クラウドコンピューティングは、リソースから「場所」という特性を取り除くことで、私たちが考えるコンピューティングのあり方を大きく変えた。クラウドコンピューティングは、急激な境界線からの開放としてとらえることができる（G103 頁）。

クラウドコンピューティングは、「ネットワークを通じて」クラウド事業者のサービスを利用することになるので、「ネットワークセキュリティ」の問題が、そのままリスクとして認識されることになる。「クラウドコンピューティングのセキュリティは、それぞれ相互に利用されている保全状態のデータのメカニズムと同様に、移送中のデータのメカニズムに対して広範囲に適用されることを要求している」（G103 頁）というのは、ネットワークセキュリティの問題も、自社において処理している場合の（狭義の）コンピュータセキュリティのレベルと同様に考えなければならないということを示しているのである。

クラウド事業者のセキュリティレベルおよびネットワーク途上におけるセキュリティの問題がそのまま問われることになる。（１）機密性（データの漏えい、通信の傍受）（２）インテグリティ（無権限改ざん、通信途上での改変）（３）可用性（物理的利用

不可能、DoS 攻撃）などのリスクがあろう。これらの各点については、クラウド特有のリスクとはいいきれないことから、クラウド・セキュリティ・ガイダンスにおいて、特別に詳述されているわけではないが、クラウドサービスの利用にあたって、心がけておかなければならないことになる。

（３）インフラストラクチャの抽象化に起因する問題

インフラストラクチャの抽象化とはいうのは、「どこで、どのような物理リソースでデータが処理され、送られ、保存されるかは、それを提供するアプリケーションあるいはサービスの処理能力の観点から不透明」であるということをいう（G28 頁）。この要素から、データがどこのハードウエア上で処理されるかわからず、また、特定のプロセスで処理されたのが、すべてのデータであるかどうか不透明であるということを導き出す。この抽象化をもたらす技術は、社会的にデータ保存技術として求められるレベルという点からみるときには、いまだ未成熟であるといわざるをえず、この点が問題を引き起こすことになる。

データの越境保存によって引き起こされる問題点

特に、データの所在が、法律の適用において、一定の意味を持つ場合がある。そのような場合には、データが国境を越えて処理が委託された国の域外で保存され、処理されるという場合には、種々の問題点が引き起こされることになる。

データの物理的な場所は、データを統制する法律の選択に直接影響するため、企業にとっては、データが保管されている国がどこであるかを理解することは重要である（G52 頁）。

この観点から問題になる法律の側面としては、「データ保護・プライバシー法制」（G54 頁）、「証拠法に関する開示義務」（ドメイン４　電子情報開示）、「行政的規制により国内保存および処理が求められている情報（ヘルスケア情報など）」、「国家保安等の観点から輸出が規制されている情報」などについて検討しなければならない。このような観点から

データの転送や保存がどこでできてどこでできないかということの立法上のコンプライアンスに関して、クラウドコンピューティング事業者は、当該データが自分たちの言

っている場所に存在し、その場所のみに存在することを保証できる必要がある（G69 頁）。

ということがいえる。具体的な法律の適用の問題点については、本解説の「法律問題編」を参照されたい。

特にフォレンジックの観点から問題となる事項

特定の場合に、コンピュータで処理されたすべてのデータが、どのように保存・改変・消去されたかというのが、客観的な方法で明らかにされることが、社会的に重要な意味を持っている。このような社会的な要請に応えるために、「クラウド事業者自身が、顧客や顧客の利害関係者（従業員、外部顧客、経営者、投資家など）を代表して正当な証拠物件として彼らのもとにある記録が実際に重要な部分を提示しているということを保証する情報セキュリティサービスを採用することが重要になっている」（G64 頁）。また、インシデント対応における他のアプソリケーションからの分離などの処理もこのような意味に関連している。これらの点についても、本解説編の「法律問題編」を参照されたい。

（４）仮想化技術により発生する問題点

仮想化は、クラウドコンピューティングを可能にする基本的な技術であり、近代的なデータセンターの姿への移行である。新技術を導入するときは、いつでも、悪い方向に行くための新しい機会を作り出す（G114 頁）。

仮想化技術が、本来、インフラストラクチャを抽象化する性質をもっていること、そして、それによってリスクを発生しうることについては、上述したが、その一方で、仮想化技術は、新しい技術であり、率直に言って、いまだ発展途上であるという性質をもっていると評価することができる。これらの観点から、（１）仮想化自体が、サイドチャンネル攻撃の危険を引き起こす可能性がある（２）仮想マシンモニタを乗っ取られると被害が甚大である（３）仮想マシン自体の脆弱性をついた攻撃が可能である（４）物理的なエラーが攻撃のきっかけとなりうる（５）キャッシュ共有・メモリの覗き見等の攻撃が可能である、などの技術的な問題点が議論されている。これらの技術的なリスクの詳細について触れるのは、本解説の目的ではないが、これらのような技術的な問題点があることを認識しておくことは重要である。

３　リスクマネージメント

具体的な評価にもとづき、具体的なリスクごとの対応を検討することになる。対応策については、リスクの回避、低減、共有および受容がある。では、具体的にクラウドサービスを利用する利用者は、どのような手順で、これらの対応をなすのかということになる。

ガイダンスに記載されている手順を作業ごとに整理すると（１）情報の分類･評価（２）対応策評価（３）対応策の選択の手順を踏むことになる。以下、各作業ごとにガイダンスの記述をまとめていくものとする。

3.1.　情報の分類・評価

（1）分類・評価の必要性

データを適切に保護するために、企業はそれを分類しなければならない（G68 頁）。

識別・評価されたリスクを前提に、それに対する対応を考慮するのにあたって、前提として、処理されるべき情報を分類しなければならない。具体的に、クラウドサービスによって処理されるべき情報の評価以前の段階になすべきものである。特に、データとシステムの分類については、

データとシステムは、明確にラベル付けされ、データの取り扱いを取り巻くプロセスを形式化する必要がある（G68 頁）

というガイダンスがなされる。個別のデータについては、その性質によって、種々の規制が課されることは、2.1.(3)「インフラストラクチャの抽象化に起因する問題」で論じられているとおりである。処理される情報が、個別のデータであるのか、システムであるのかを峻別することによって、個別のデータに関する規制にフォーカスすることができるし、その一方で、システムに関する情報については、規制要求についての考慮をそれほど求められないで済むということがある。

（2）情報の分類・評価

クラウドにどのようなデータが置かれているか、そのデータのセキュリティ要件は何かを明確に理解する（G84 頁）

情報資産たるデータについては、識別、評価、分類がなされるべきことは、基本といっていい。この評価は、データの性質（機密性・インテグリティ・可用性の観点からの位置づけ）からくる取扱の重要度の観点から評価・分類される。クラウドサービスによって処理される可能性があるデータについては、特に、その性質を認識し、その性質にもとづいて、セキュリティ要件は何か、を理解する必要がある。 これは、本章　2･1で述べたようなクラウド特有のリスクが存在するので、それを特に考慮する必要があるからである。

このための具体的な作業としては、（１）法規制等の要請についての理解（２）データの機密性・完全性・可用性の観点からの評価が求められることになる。（２）については、一般的な分析が妥当するとしても、（１）については、データの場所のおよぼす意味を検討した上で適用の可能性のある法規制を網羅し検討し、その法規制の適用の可能性、適用された場合の法的効果について検討しなければならない。

最も重要なことは、組織が必要な法的要件を理解しなければならないということである（G68 頁）。

というガイダンスの記載およびそれに続く論述は、この作業の重要性および大変さを物語っている。これらの詳細については、本解説の「法律問題編」を参照されたい。

事業者がデータの性質を意識していることを確認する（G84 頁）。

そして、その評価・分類については、クラウドサービスを提供するクラウド事業者も認識を同一にしていなければならないのである。

3.2.　情報資産ごとのリスクの評価

クラウドのリソースのために考えられているシステムとデータに関して、すべてのリスクが特定され、説明されるのを保証するために、第三者機関によるリスク査定を行うべきである（G69 頁）

事業体にとって、その事業目的の達成に不利益をおよぼしかねない事象を識別したら、次にその事象を、発生の可能性と影響度から、評価しなければならない。ガイダンスに

おいては、リスクの十全な評価をなすために、第三者機関によるリスク査定が推奨されている点は、注目されるものということができるであろう。

なお、このクラウドサービスにおけるリスクごとの可能性と影響度の分析については、注 6 でも紹介している ENISA 報告書の 24 頁に、35 のリスクを分析している分布図があるので参考にされたい。

3.3. 対応手法

セキュリティ要件が認識されたデータに対して、どのような手法で、リスクマネージメントを行うかどうか、まさにセキュリティの対応策の評価の問題になる。利用者にとって、クラウドサービスの利用がリスクをもたらすのであれば、そのリスクをどのような形で低減しうるのかということになる。利用者からみた場合に、どのような手法で、その提供されるクラウドサービスの信頼性を確保するかということになる。この信頼性の確保の手法としては、大きくわけると（1）サービス提供主体および内容の評価（2）技術的手法（3）法的手法による三つの手法を考えることができる[11]。これらの手法についてポイントを拾いだすと以下のようになる。

(1)サービスの提供主体および内容

クラウドサービス事業者として、誰が(主体)、利用者の IT ポリシーのなかで、どのようなサービスを(種類)、どの程度の「質・価格」でもって提供しうるのか。それを「客観的に評価」することが、リスクを管理するためにきわめて重要なことである。

なお、CSA では、クラウド事業者およびクラウド利用者に対して、セキュリティ対応の原則を提供し、利用者において、事業者のリスク対応の評価の一助となる枠組とし

---

[11] ISMS によれば、管理策は、「セキュリティ基本方針」「情報セキュリティのための組織」「人的資源のセキュリティ」「物理的および環境的セキュリティ」「通信よび運用管理」「アクセス制御」「情報システムの取得、開発および保守」「情報セキュリティインシデントの管理」「事業継続管理」「遵守」にわけられている。

本稿においては、特にクラウド特有の管理策という観点から、三つの観点を特に取り上げた。

て、”CSA Cloud Controls Matrix V1”を提案している[12]。このマトリックスは、「コンプライアンス」「データガバナンス」「物理的セキュリティ」「人的資源管理」「情報セキュリティ」「法的」「運営マネジメント」「リスクマネージメント」「レジリエンシー（弾力性）」「セキュリティアーキテクチュア」などの統制エリアをあげており、それらについて個々の SPI モデル（SPI モデルについては G29 頁）ごとにどのようなコントロールが問題になるかを分析している。本解説においては、このマトリックスをもとに検討する時間的余裕はなかったので、これとの関係については、またの機会としたい。

サービスの主体

だれが、クラウドサービスを提供する業者として望ましいのか、これをどのような基準で選定するのかという点が問題となる。この点については、一般的な外部委託の場合の委託業者の選定基準が参考となる。そのうちのいくつかをガイダンスから拾うことにしよう。

サービス主体(サービス事業者)については、その財政的健全性の問題があることは、前述しているが、マーケットでの評価、管理状況、主要役員構成、過去の受託等の業績の評価が基本となる。その上、関与するサードパーティーベンダのリストと各事業者に対する役割、責任事項および、それらのインターフェース情報の提供を求め、それぞれの確認が必要となる(G44 頁)。

次は、それらの主体が、どのようにリスク管理をしているかという点についての考慮が、必要になる。その事業者自体のリスクレベルの評価、ポリシーの評価、手続およびプロセスに対するレビューが必要になる(同)。これは、事業継続性計画の有無等なども評価されることになる。また、例えば、コンプライアンスに関する態度、データのライフサイクル管理の可能性、損失に対する保険加入状況なども考慮される。

サービスの種類

クラウドサービスの種類については、一般的に SPI モデルにもとづいての説明がなされる。SPI モデルについては、そのモデルごとに

---

[12] http://www.cloudsecurityalliance.org/cm.html

それぞれ、統合された特徴、オープン性（拡張性）、およびセキュリティの分野で重要なトレードオフをもたらす(G30 頁)。

のであり、このモデルごとに、リスクと便益のバランスを考慮して、後に触れるように対応手法を選択していかなければならないことになる。

また、展開の方法については、「プライベートクラウド」「パブリッククラウド」「マネージドクラウド」「ハイブリッドクラウド」の 4 つの方法がある(G31 頁)。これらの分類は、管理されるアプリケーション/情報/サービスのタイプ、誰がどのように管理するか、コントロールはどう統合しているか、規制の問題などのポイントについて、相違を示しているのである。

これらのサービスの種類が適切なリスク評価のもとで選択されることになる。

サービスの質・価格

サービスの質としては、種々の事項を考慮することができるであろう。いうまでもなく、どの程度の稼働が保障されているかというのが中心的な事項であるが、それ以外にも、サービスの供給開始は、いつからなのか、また、サービスを停止することを決定した場合に、迅速に停止がなされるかもサービスの質として考えることはできるであろう。

いうまでもなく、価格の問題も重要である。客観的な価格以外にも、帯域幅、CPU 使用率との関係での課金の実際の検討も必要であることが指摘されている。

客観的な評価

契約は唯一のガバナンスのためのツールではなく、クラウド事業者に必須となる幅広い適正評価を含めていくべきである(G15 頁)。

上記サービスの種類および質について客観的な評価をおこなうことが必要になる。そのためには、デューデリジェンスが求められる。デューデリジェンスは、サービス種類、サービス主体、サービス条件、SLA の実効性を対象とするものということができる。

具体的にデューデリジェンスの対象事項については、クラウド・セキュリティンガイダンスのドメイン 2 が詳しく触れている。

ガイダンスにおいては、まず、もし、パブリッククラウドを利用するというのであれば、注意深い、包括的なデューデリジェンスが必要となることが強調されている。そもそも、利用者の IT ポリシーにおいて、SPI モデルについてどのタイプの事業者を必要としているのかレビューすることが必要になるし、また、プライベートクラウド、ハイブリッドクラウドにおいて展開した場合の評価も必要になる(G43 頁)。

主体の評価のポイントについては、上述している。これらについての客観的なデューデリジェンスがポイントになってくるのである。

（2）技術的手法

ここで、技術的な手法については、暗号化、鍵管理、アイデンティティ管理、アプリケーションセキュリティなどの従来からコンピュータセキュリティでも重要なものとして認識されているポイントがあり、それぞれ、IaaS、PaaS、SaaS などのサービス提供モデルごとに異なって対応されることになる。そして、これらのモデルごとの違いが、後述の対応策の選択において重要な意味を持ってくることになる。

従来からの技術的手法については、むしろ、クラウド事業者自体におけるデータセキュリティの確保の問題と位置づけられるが、サービス利用者としても、それらの概要について理解しておくことは重要であろう。

暗号

強固な暗号化は、鍵管理と並んで、クラウドコンピューティングにおいてデータを保護するために利用するコアのメカニズムである（G103 頁）。

第三者のもとで保管されるデータについては、暗号化がきわめて重要である。暗号化されたデータについては、これを解読する鍵がなければ、そのデータを読むことはできない。我が国において、個人情報保護法に関するガイドラインにおいて暗号化された情報については、解釈上は、暗号化されていたとしても個人情報であると解するものの、漏えい時においては、監督官庁への届出等の必要がないものと示されているなど、暗号化が、データの保護に強力な役割を果たしていることに対応している。

鍵管理

クラウドサービスにおいては、利用者ごとの独立性（isolation）が確保されることが必要であり、それが十分でない場合には、技術的なリスクとして認識されることは前述した。また、独立性が不十分な場合のリスクについて、「法律問題編」では、具体例からの紹介がなされている。まさに、

事業者は、それぞれの顧客のデータを分離する鍵管理スキームの構築を望んでいる（G103 頁）。

ということになる。

データ自体が暗号化されている場合、第三者が、法律上の根拠に基づいて（米国においては訴訟法上の証拠開示（ディスカバリ）や規制法上の提出命令（サピーナ）があり、日本においては、規制当局の行政調査の場合、文書提出命令がありうる）、データにアクセスしようとしても、鍵管理が適切になされている場合、法的にアクセスが許容されているデータに対してのみアクセスが可能になるにすぎない。その一方で、この管理が不十分な場合、利用者は、その保有するデータに対するプライバシの合理的な期待があるにもかかわらす、第三者が、無権限でアクセスしうるというリスクを発生させることになる。この場合、事業者自身としても、重大な契約違反などの責任を問われることになるであろう。

事業者は、データの保持と利用との間における役割を分離することで、事業者自身を保護することが可能である。顧客の側でも同じメカニズムで自身を保護することができる（104 頁）。

というのは、上述のような意味で考えることができる。

そして、暗号や鍵管理については、利用組織としては、契約によってクラウド事業者において適用する暗号を特定する場合には、業界もしくは政府の基準を満たすように特定することができる。

アイデンティティ管理

本ガイダンスにおいては、各利用者企業を便宜上、利用者と呼称しているが、実際のクラウドサービス利用においては、各利用者（企業）において、データに対するアクセ

ス権限を有する各ユーザが、実際にデータに対してアクセス・処理をすることなる。この場合、各ユーザのアイデンティティ管理は、重要な問題になる。

アイデンティティ管理およびアクセス管理については、CSA より「CSA Domain12:Guidance for Identity & Access Management V2.1 」(以下、ドメイン 12 ガイダンスという)が公開されている。これらの問題点について、ドメイン 12 ガイダンスは、「アイデンティティ・プロビジョニング」「認証」「連合(Federation)」「アクセス管理およびユーザ・プロファイル管理」「IDaaS(サービスとしてのクラウド・アイデンティティ)」について論じている。これらの観点のポイントは、

アイデンティティ・プロビジョニング

クラウドを利用するに際しては、利用しうる状態(プロビジョニングーユーザに対する権限の割付け)であるか利用し得ない状態(デ プロビジョニングーユーザに割付けた権限の解除)であるかを安全に、かつ時宜に、管理するという問題に対処しなければならない。しかも、この問題は、さらに、利用組織において、いままでのアクセス管理をクラウドサービスの利用にまでに拡張しなければならないという問題をもっているのである。

認証

利用者が、クラウドサービスを利用する際には、ユーザの認証を、信頼できる方法で管理することが重要なことになる。そのような認証のためには、クレデンシャル情報の管理や、認証処理の委譲、クラウド全般のトラスト管理などの問題を検討する必要がある。

フェデレーション

アイデンティティの管理に際しては、その管理をする事業者が、お互いに安全に、認証手続を統一してすることができるように、フェデレーション[13]を組むのが、利用者の便宜という観点からも求められるのではないかということから、種々の動きがある。

---

[13] フェデレーションとは「アイデンティティやさまざまな資格・権限情報を、個々のドメイン間で流通させるための合意、標準、技術を意味する」(「アイデンティティ・

クラウド環境においては、このフェデレーションが、重要な役割をはたすものと考えられる(ドメイン 12 ガイダンス 16 頁)。

アクセス管理およびユーザ・プロファイル管理

そのユーザが、どのような立場でアクセスするのかということに応じて、ユーザのプロファイルおよびアクセス管理に求められるものが異なってくる。ユーザのプロファイルの正確な情報にもとづいて、そのユーザが、どの資源にアクセスしうるのかというアクセス管理がなされる。クラウドサービスの環境では、それらの情報が種々の組織から提供されることになるために、きわめて、困難な作業ということになる(ドメイン 12 ガイダンス 20 頁)。しかも、その管理手法が監査可能な手法でなされる必要があるのである。

IDaaS(サービスとしてのクラウド・アイデンティティ)

IDaaS とは、アイデンティティの管理をサービスで行おうとするものである。そして、そのサービスをクラウドを用いて行うという考え方が提案されている。

アプリケーションセキュリティ

クラウドコンピューティングプラットフォームの上で稼動中あるいは開発中のアプリケーションソフトウェアは、その特定のプラットフォームの配信モデルに依存したセキュリティ上の挑戦が必要である(G93 頁)。

企業における既存のセキュリティ ポリシー、基準およびツールの機能をクラウドプラットフォームに応じて拡張する必要があることは、アプリケーションにおける問題についても同様である。クラウト・セキュリティ・ガイダンスにおいては、ドメイン 11(バージョン 1 において)がこれについてふれている。さらに CSA は、このウエブアプリケーションセキュリティについて、”Domain 10: Guidance for Application Security V2.1” (以下、ドメイン 10 ガイドラインともいう)を 2010 年 7 月に公表している。

フェデレーション:企業の境界を超えた、セキュアなコラボレーションの実現」より)(http://jp.sun.com/practice/software/identity/jp/federation_mgr/J_wp_id_federation_secure_collab.pdf)

この点についてドメイン 10 ガイドラインは、アーキテクチュアの全体像を論じた後に、SPI モデルごとに、コスト便益、ツール、尺度などの観点から論じている。これらの観点について論じるのは、本解説の範囲を越えるので、詳細については、ドメイン 10 ガイドラインを参照されたい。

(3)法的手法による対応

クラウドサービスというイノベーションの採用にあたって、そのイノベーションに伴う問題点(リスク)については、法的手法によって、対応するということもひとつの重要な方法になる。この場合、契約条件が公平であるかが、情報の共有・解消の容易さの観点から、検討されることになる。

サービス条件については、一定の事項についてサービスレベルアグリーメント(SLA)を締結することが行われる[14]。また、それ以外にも、契約書でもって定めておかなければならない事項が多く存在する。契約書において定めるかどうか検討しておくべき事項のうち、ガイダンスで触れられているものを中心として、簡単に触れるものとする。これらの事項について、契約の締結・履行に際して、利用者としても留意すべきであるし、以下の点に関するサービス事業者における情報提供をきちんとうけなければならないだろう。

データの独立性についての規定

クラウドサービスにおいて各利用者ごとのデータは、それぞれ独立して保存されるべきことが求められる。これを独立性（isolation）という。「データが混在された場合、それだけ脆弱性が増すからである」（G52 頁）。この独立性を、契約によって確認・保障させることが必要となる（G56 頁）。

データのアクセスに対する規定

クラウドサービスの過程において、クラウド事業者の従業員が、利用者のデータにアクセスしうることになるが、そのような場合に関してのアクセス制限、閲覧制限、アク

---

[14] ＳＬＡについては、経済産業省「SaaS 向け SLA ガイドライン」（http://www.meti.go.jp/press/20080121004/03_guide_line_set.pdf）を参照のこと。

セスログなどのアクセスに関する規定および保護措置についても契約において定め保証を受けることが求められるということがいえよう。

技術的な手段の利用についての規定

また、クラウド事業者において、一定のセキュリティ措置がとられるのは、当然のことであり、これについての契約の定め、保証なども有効である。「パスワードの強化、暗号化、あるいはファイアウォールの利用などの技術的な手段が求められる。」(G56 頁)

データの所有権限に関する定め

クラウドサービスの利用者は、サービス事業者に対して「データの保有者」(データを最新の状態に維持する責任のある個人または組織)であることを確保したいと考えている。セキュリティ上の問題やプライバシ上の懸念がある場合に、利用者が、その保有権限でもって、みずからの問題・懸念に対処しなければならないのは、当然のことである。

この理は、いわゆるメタデータ(データが付随して持つそのデータ自身についての抽象度の高い付加的なデータ)に対しても適用される。「取り扱いが機密な個人情報、会社の取引上での機密事項、あるいはその他の価値のある情報を保有している企業は、クラウドサービス事業者による情報へのアクセス、あるいは、情報データに関係する取引情報の利用に対して制限をかけたいと考える」ということになる(G55 頁)。

セキュリティ手段に対する定期的なモニタリング権限の定め

クラウドサービス契約では、企業がこうしたモニタリングやテストを実施する権限を盛り込んでおく必要がある。さらに、企業経営者は、モニタリングやテスト実施のためのプラン策定や組織体制の構築を行わなければならない(G59 頁)。

クラウド事業者としては、このようなモニタリングやテストを回避したいということになり、独立した第三者による証明書を提供することで代替しようとする。しかしながら、そのような証明書が保証する事項については、利用者の IT ポリシーからみるとき、不十分なのではないかという問題がある。

法的遵守事項についての定め

法律、規制、国際規格、および、関連するベストプラクティスは、企業がデューデリジェンス（契約締結前）やセキュリティ監査（契約期間中）を実施することでこうした義務を満たしていることを明らかにすることを要求している(G56 頁)。

法的遵守事項としては、きわめて多様な事項を考えることができる。そのなかで、注目すべき事項としては、個人情報保護(もしくはデータ保護)対応、e-ディスカバリ対応、刑事・行政手続上の提出命令対応、情報漏えい時の対応などがある。これらについて、どの国の法律が適用されうるか、また、留意すべき事項はなにかなどの問題があることは、本解説の「法律問題編」を参照されたい。これらの法律の遵守自体をクラウド事業者に求めることや、また、想定外の法律の適用を免れるために、データの保存場所を限定するよう要求することなどが、クラウド事業者と利用者との間の契約事項として検討されうることになる。

円滑な契約終了のための定め

企業はクラウドサービス事業者に委託した情報データに対する責任を有し、情報データを回収するか、あるいは、もはや不要な場合その内容を消去する必要がある。こうした要求は、数多くの法律や規制事項、あるいは慣習法などに基づく義務に起因している。さらに、企業はその顧客に対して、顧客に関する情報データが常に利用可能であることを保証する責務を課されている(G59 頁)。

どのようなサービスでも新規のイノベーションは、実際に利用してみないと、その実際はわからないということがいえる。その意味で最後には、円滑な契約終了が可能であって始めて契約の公正性を保持することができるということがいえるかもしれない。また、そのような場合以外にも、倒産や事業再生などによって、クラウドサービスの永続的な提供が困難になるという場合もありうる。しかしながら、そのような場合に、データの回収や消去がスムーズにいくとは限らない。クラウド事業者がホスティングを継続することもあれば、独立性の維持が図られない場合もある。「当事者は、サービス契約においてこうした問題が生じることを想定して、契約終了の場合の適切な手続きを定義し、争議に備えて回避策を特定しておく必要がある。」ということになる(G60 頁)。

3.4. 対応策の選択

(1)対応策の選択の基礎

リスクへの対応としては、回避、低減、共有、受容[15]がある。具体的に、クラウドサービスにおけるリスク対応としては、

回避

リスクを引き起こすような可能性あるサービスを利用しない、すなわち、クラウドによるサービスを利用しないということである。結局、クラウドサービスに対する対応策を採用したとしても、許容レベルまで低減させる対応策が認識されない場合ということになる。

低減

リスクの発生可能性または影響度、あるいはその両方を低減させることであり、3.2. 対応手法で論じた技術的手法、サービスの評価、法的手法などにより、これを図ることができよう。

共有

リスクの一部を転嫁することまたは共有することをいい、クラウドサービスの利用者からみた場合、損害が発生した場合に保険契約を締結する場合などが代表となる。

受容

リスクについては、これが発生した場合、その影響をそのまま甘受することであり、発生可能性および影響度に影響をおよぼすような行動をとらないことである。これは、評価されているもともとのリスクが、それ自体で、許容しうる範囲内の場合である。

---

[15] これらの一般的な定義については、八田進二［監訳］／中央青山監査法人［訳］「全社的リスクマネジメント　フレームワーク編」（東洋経済新報社、2006）75 頁を参照されたい。

なお、JIS　Q 27001:2006 などにおいては、低減、受容、回避、移転とされている(JIS Q 27001:2006 においては、4.2.1 f)、JIS　Q 27002:2007 については、4.2 セキュリティリスク対応)。

これらの対応策のために、上記で検討した対応手法を選択していくというのが、実際の対応策の選択の手順ということになる。

(2)対応策の選択の要素

観点

では、リスク対応策を決定する場合に、どのような観点から決定していくべきかということになる。いうまでもなく、一定のサービスを利用することによるメリットを正確に認識することが必要であろう。その一方で、上記対応手法が、どれだけリスクの発生可能性や影響度に影響を与えるかということの比較による経営判断ということになる。そして、その対応手法の採用については、費用対効果の選択が影響することになる。

プロセス

適正水準でリスクに対するコントロールが可能なプライベート（バーチャル）クラウド、あるいはハイブリッドクラウドを構築するかどうかの検討を行う(G43 頁)。

すでに、本解説で前述した手順によれば、情報の分類がなされ、それらの情報処理についてクラウドサービスを利用する場合のリスクが認識されていることになる。そして、本解説においては、その際にデューデリジェスを行うことを推奨している。それらのリスク分析にもとづいて、クラウドサービスを利用することによるメリットが大きいと判断した場合、プライベートクラウド・ハイブリッドクラウドの選択の検討を行うことになる。この場合、パブリッククラウドの選択については

顧客の期待値を管理し、適切な契約のドラフトを描くことができないならば、自社ビジネスのミッションクリティカルな領域でパブリッククラウドサービスを利用するという決定を下す前に、注意深く、かつ包括的なデューデリジェンスを行う必要がある(G43 頁)

という指摘が重要性をもってくることになる[16]。また、SPI モデルにおいて、どのモデルを採用すべきかという点についても検討しなければならないことになる。サービ

---

[16] 同様の指摘は、ガイダンスの 70 頁にもある(「保証が提供されない場合には、データと処理のいくつかは例外なしにドメイン 1 で定義されているパブリッククラウドの資源を使用することができないということを記憶にとどめておくべきである。」)。

ス利用の種別によっては、一定の認証を経ている業者を選択するということも判断のひとつになる。

情報資産ごとに、これらのサービスの種類・質を選択し、技術的手法や法的手法によって、リスクを低減させていく。具体的には、クラウドサービスに関する情報資産についてのリスクとそれに対する対応策の対応表が作成されることになる。この表において、資産ごとに許容される程度までリスクを範囲内に抑えることができているかどうかがポイントということになる。

押さえ込まれたリスクに対しては、それを承認[17]して、リスクマネージメントシステムを実施することになる。その一方で、もし、抑えることができなければ、別途、リスク対応策を考慮することになるだろうし、場合によっては、想定されたリスク許容度自体を見直すべきなのかもしれないということになる。

---

[17] JIS　Q 27001:2006 の 4.2.1 h)は、「残留リスクについて経営陣の承認を得る」という。

4　測定・検証と開示[18]

4.1　測定と検証のプロセス

クラウドサービスに伴うリスクを評価し、対応策を選択し、リスクを許容範囲内にまで管理したのであれば、その対応策が、正しく実施されるべきであり、また、正しく実施されていることを測定し、検証することが必要になる。

クラウドコンピューティング環境におけるセキュリティは、組織の内部ポリシー、手順、標準、ガイドライン、プロセスをお互いに締め出してしまうものではないということを忘れてはならない（G70 頁）。

本解説の基本的なスタンスは、クラウドサービスの利用に関するポリシーは、最終的には、

クラウドコンピューティングセキュリティ、ビジネス継続性、ディザスタリカバリーを、利用者自身のポリシーと手順に統合する（G85 頁）

ことによって、利用者組織のＩＴポリシと統合されることが目標であるということである。

この目標のために最初になされることは、データがどのように保存され、処理され、アクセスされ、制御されるかという点についての定義と文書化ということになろう。セ

---

[18]伊藤　哲也「IT 環境の変化とクラウドコンピューティング」企業リスク 2010 年 1 月号（第 26 号）
http://www.tohmatsu.com/print/ja_JP/jp/knowledge/gr/2722416b97e0a210VgnVCM200000bb42f00aRCRD.htm

日下部　公「2 年目の内部統制（IT 全般統制）の改善ポイント［最終回］システム環境に合わせた継続的な改善 」http://www.nec-nexs.com/sl/sol/cons_column05_09.html

なお、視点が本解説と異なるが、戸村 智憲「なぜクラウドコンピューティングが内部統制を楽にするのか 」（技術評論社、2010）がある。

キュリティ・サービス・レベル目標（SLO：：Service Level Objectives）と SLA（SLA：：Service Level Agreement）を定義するプロセスは、クラウドサービスに期待されるものの概要を記述したドキュメンテーションの集まりということになる。これが、その他の業績の指標とセキュリティ要件の基盤ということになる。測定・検証といっても、リスク管理がきちんとなされているかを何を基準に測定するのかがはっきりしないと意味がない。

クラウドサービス事業者によって行われる第三者監査を仮定すると、監査の範囲はあなたの会社や規制の要件を満たさないかもしれない。その場合、レポートの正当性自体が意味のないものとなってしまう（G68 頁）。

利用者の会社においてみずから、業績の指標とセキュリティ要件の基盤を定めないと意味はないのであり、ガイダンスのこの記述は、基本的な作業の重要性を物語っている。

組織内部における情報処理であれば、リスク管理の目的や対応策について、リスクの管理が有効になされていかは、内部監査等によって、その有効性の測定がなされることになる。クラウドサービスの利用についてのこのような考え方を延長するとき、上記のような定義と文書化がなされたあとは、クラウド事業者が、それらの点についてこのレベルのとおりに行うのかというのを利用者が確認するという手順になる。

クラウドコンピューティングのリソースをホスティングしている組織のセキュリティ状況を理解し、どのような対策を取ろうとしているかを理解する必要がある(G69 頁)。

しかしながら、このクラウドリスク管理の測定・検証というのは、非常に難しい問題である。サービス事業者に、実際の SLA や SLO の実施状況を確認したいので、詳細に立ち入り検査等をさせてほしいといったとしても、容易に立ち入り検査が認められるわけではないだろう。クラウドリスク管理の測定・検証が、クラウドサービス利用のきわめて重要な問題であるのは、このようなことにも原因がある。

この点に関して、実際には、米国公認会計士協会による監査基準書（SAS70）の報告書によって、統制の保証とすることも良く行われている。我が国では、監査委員会報告 18 号がこれにあたるであろう。これらが入手できない場合には、予めサービス事業者から入手可能なドキュメント等を確認した上で代替の管理方法を検討することになる。もっとも、第三者の報告書等が存在したとしても、クラウドサービスについて、利用者

の IT ポリシーから、全く別個のものがつくられるわけではなく、むしろ、ＩＴ管理プロセスにおいて、認識されていた具体的な統制が、クラウドサービスにおける統制に応じて変更するということになるものと考えられる。

4.2. 測定・検証の対象事項

業績の指標とセキュリティ要件の基盤がクラウドサービスのリスク管理の基本となるといっても、具体的にどのような観点がその基本となるかということになる。ここで、「財務報告に係る内部統制の評価及び監査に関する実施基準」は、財務報告にかかわらず、むしろ一般的なリスク管理についての基本的な枠組の作成に関しても参考になる。

実施基準は、まず、内部統制の基本的枠組みの検討において、内部統制の基本的要素のひとつとして「ＩＴへの対応」を掲げている。これは、組織の業務内容がＩＴに大きく依存しているとか、組織の情報システムがＩＴを高度に取り入れている等、多くの組織がＩＴ抜きでは業務を遂行することができなくなっており、業務を実施する過程において組織内外のＩＴに対して適切に対応することが内部統制の目的を達成するために不可欠となっていることにあらためて注意喚起したものであり、この点をまず留意すべきである。また、ＩＴを取り入れた情報システムに関する統制は、ＩＴに係る全般統制とＩＴに係る業務処理統制とにわけて考察される。ＩＴに係る全般統制の具体例としては、アプリケーション開発・変更管理、IT インフラ変更管理、システム運用管理（障害管理を含む）、アクセス管理、委託管理などがあり、これらが、クラウドサービス利用においては、それぞれ具体的に変容すると考えられる。また、ＩＴに係る業務処理統制としては、 入力情報の完全性、正確性、正当性等を確保する統制、 例外処理（エラー）の修正と再処理、マスタ・データの維持管理、 システムの利用に関する認証、操作範囲の限定などアクセスの管理などがあるとされている。

業績の指標とセキュリティ要件の基盤が、SLO や SLA によって定義される場合には、上記実施基準で指摘されている事項が、クラウドサービスの特性におうじて変容し、適切に考察されることによって、具体的に記述されることになる。クラウドサービス事業者に実施されるべき情報セキュリティ対策ついて詳述したものとして、（注２）でふれた「ASP・SaaS における情報セキュリティ対策ガイドライン」があり、このガイドラインに記載されている事項について、それぞれ、SLO や SLA によって定義がなされる

場合には、それらが、具体的な測定・検証の対象事項となる。したがって、そこで記載されている

（１）組織運用に関する事項

基本方針、組織、連携 ASP・SaaS 事業者に関する管理、情報資産の管理、従業員にかかる情報セキュリティ、情報セキュリティインシデントの管理、コンプライアンス、ユーザサポートの責任

（２）物理的・技術的対応策に関する事項

アプリケーション・プラットフォーム・ハードウエアの物理的・技術的対応策、ネットワークの対応策、建物・電源（空調等）、共通する情報セキュリティ対策、その他

などの観点には、十分な留意をはらう必要がある。

4.3. 利用者における開示の問題について

内部統制のシステムは、資本と経営の分離する現代においては、経営者にとって当然の要請であり、内部統制の構築義務というのは、わが国の判例において取締役の善管注意義務の一つの形態として認識されてきている[19]こと、会社法において「取締役の職務の執行が法令及び定款に適合することを確保するための体制その他株式会社の業務の適正を確保するために必要なものとして法務省令で定める体制の整備」が取締役会としての決議事項（会社法 362 条４項６号）であることなどについては、「法律問題編」で説明している。

これらの体制を整備し、それを運営する具体的な活動について利害関係人に開示する制度としては、以下のものがあり、それらについて、クラウドサービスの利用との関係での具体的な開示の程度等については、以下のことがいえる。

事業報告

上記事業報告について、会社法施行規則 100 条１項２号は、「損失の危険の管理に関する規定その他の体制」を、事業報告に記載するように求めている。一般のＩＴセ

---

[19]大阪地判・平成 12 年 9 月 20 日（大和銀行事件第１審判決）や神戸製鋼所総会屋利益供与株主代表訴訟(平成 14 年 4 月 5 日)和解文言

キュリティの枠組を定めていることがこの記載事項になるものと考えられるが、クラウドサービスの利用に際して、本解説で述べた点を考慮したことを取り立てて報告すべきかどうかという点が問題になる。この点については、導入および利用に伴う社内体制を整備した旨を記載した上で、更なる詳細な開示をなすべきかどうかは、クラウドサービスの利用対象業務や範囲、その利用内容や頻度等を総合的に勘案して判断すべきものと考えられる。

内部統制報告書

米国においては、米国の資本市場に対する投資家の信頼を取り戻すために企業の経営者に対して厳しい責任を負わせ[20]、また、従来は、自主的な監督のみでなされていた監査の質の保障という点について、会計監査や内部統制の監査の基準を制定し、さらにその監督を行うために、公開企業会計監視委員会（PCAOB）を設置するということを基本的な枠組みとした Sarbanes　Oxley 法（正確には、U.S. Public Company Accounting Reform and Investor Protection Act of 2002）[21]が制定されていること、そして、我が国においても、金融商品取引法が制定され（証券取引法の一部改正）、経営者確認書（同法 24 条の 4 の 2）、内部統制報告書（24 条の 4 の 4）、監査報告書（同法 193 条の 2）の３つの報告書の制度を中核とする内部統制のための制度が組み込まれることになり、導入されるにいたっていることは、「法律問題編」で論じている。

この内部統制報告書が前提としている報告事項は、まず、適正な財務報告を実現するための内部統制に関する事項である。金融庁の「財務報告にかかる内部統制の評価および監査に関する実施基準」によれば、「財務報告の信頼性を確保するために整備するものであり、財務報告の信頼性以外の他の目的を達成するためのＩＴの統制の整備及び運

---

[20] 302 条および 404 条である。ここで、302 条について触れると、SEC 登録企業の経営最高責任者（CEO）と財務最高責任者（CFO）に対して、所定の文言による宣誓書に個人名で署名し、それぞれの宣誓書を別々に年次報告書に綴じ込むことを求めている。また、404 条は、経営者に対して、会計年度末における財務報告にかかる内部統制の有効性評価と評価結果の年次報告書での開示をすることを求め、そして、それについて、公認会計士による監査を受けることを要求している。

[21] この法律の解説については、種々の本がでている。詳細については、「COSO フレームワークによる内部統制の構築」中央青山監査法人編・（東洋経済新報社、2004）などを参照のこと。

用を直接的に求めるものではない。」とされている。このことから、クラウドサービスを利用していること自体が、内部統制報告書において報告すべき事項となるわけではないと解されている[22]。

有価証券報告書等

金融商品取引法 第 24 条は、「有価証券の発行者である会社は、その会社が発行者である有価証券（特定有価証券を除く。次の各号を除き、以下この条において同じ。）が次に掲げる有価証券のいずれかに該当する場合には、内閣府令で定めるところにより、事業年度ごとに、当該会社の商号、当該会社の属する企業集団及び当該会社の経理の状況その他事業の内容に関する重要な事項その他の公益又は投資者保護のため必要かつ適当なものとして内閣府令で定める事項を記載した報告書（以下「有価証券報告書」という。）を、（略）内閣総理大臣に提出しなければならない。」と定めている。この提出内容等については、企業内容の開示に関する内閣府令が定めており、それによれば、「投資者の判断に重要な影響を及ぼす可能性のある事項」について記載することが求められている。「企業内容等の開示に関する留意事項について　（企業内容等開示ガイドライン）」[23]の「C 個別ガイドライン　I 「事業等のリスク」に関する取扱いガイドライン」においては、具体的なＩＴ技術の導入それ自体が、リスクになるという観点からの指摘はない点から考えて、一般的に記載対象となるとはいえないであろう[24]。

---

[22]浦野（前出　注９）NBL930 号 46 頁

[23] http://www.fsa.go.jp/common/law/kaiji/01.pdf

[24] 浦野（前出　注９）NBL930 号 47 頁は、「クラウド・コンピューティング導入に伴い生じるリスクについても、有価証券報告書等の記載対象となりうる」とする。

第３　セキュリティ・ガイダンス

以上のような問題点とその考察を減るとき、クラウドサービスの利用者が、その利用にともなって、どのように考え従来の IT ポリシーにどのような修正等を加え、どのような手順を踏んで、クラウドサービスを利用すべきかという点について、個別の問題について詳細な解説を加えてみた。その解説の要点をセキュリティ・ガイダンスとして以下のように指摘することができるであろう。これらの点は、クラウド・セキュリティ・ガイダンスの「ガイダンスの概要」の部分に記載されているが（14 頁以下）、それらのガイダンスを、本解説の観点から、体系的に整理することによって理解が深まるといえるであろう。以下、「ガイダンスの概要」のうち、各体系においてポイントとなるものを並べることで、本解説のまとめに代えよう。

IT 枠組の統合とリスクマネージメント

ドメイン 1 のクラウドコンピューティングの定義はフレキシブルで事業者間の関係をダイナミックにするものであるが、同時に常にリスクマネージメントを必要とする（2－2）。

クラウドサービスの利用に際して、そのダイナミックさから生じる機会は、リスクを伴う可能性があり、そのリスクを識別・対応していかなければならないことになる。

クラウドコンピューティングの利用により削減されたコストの一部は、事業者のセキュリティ能力の監視の強化、および、継続中の詳細な監査のために支払われるべきである（2-1）。

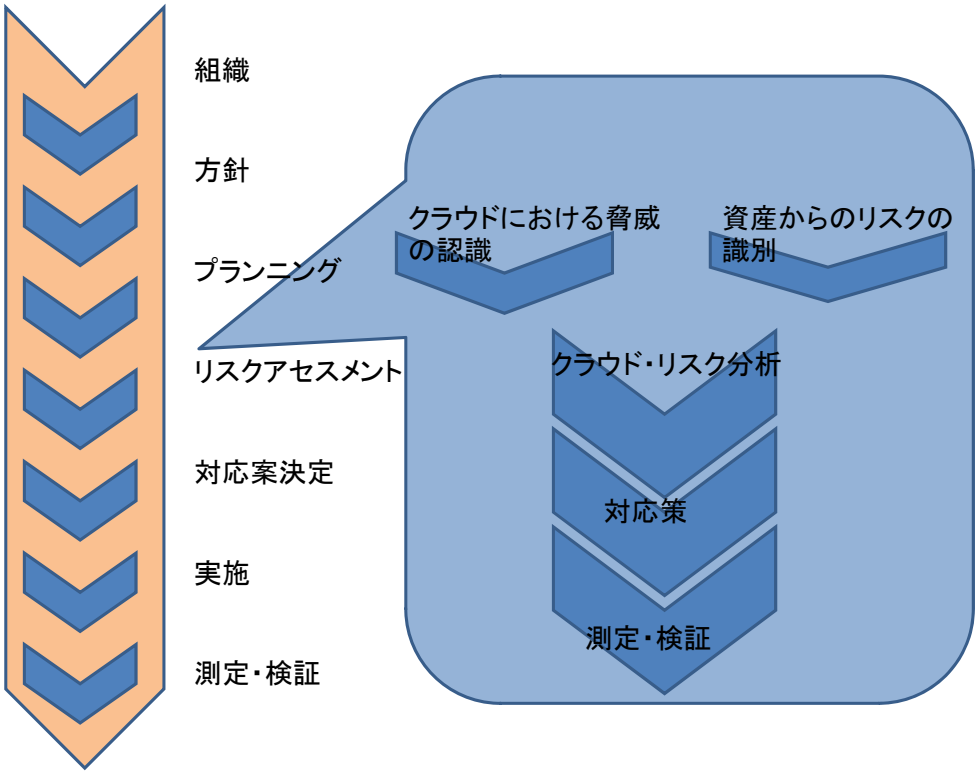
そして、そのリスクマネージメントは、最終的には、利用者の有している IT セキュリティポリシと統合されなければならない。クラウド事業者が主体なのではなくて、利用者が主体となるのである。

ミッションクリティカルなビジネスや個人情報のホスティングを行う際に、適正評価を

行うのは利用者側の責任である（2-8）。

データに対するリスクの評価

実際の作業の手順の内、代表的なものを時系列的にまとめると以下のようになる。



コンプライアンスの要求を理解するために、データとシステムを分類しなければならない（5-1）。

データの所在、とりわけデータのコピーがどのように作られ、どのようにコントロールされているかを理解しなければならない（5-2）。

情報の論理的な分類と、実装されている保護管理を理解しなければならない（6-1）。

情報が識別されることが最初のステップとなる。

プライバシーインパクトアセスメントを含む外部リスク評価を実施すべきである（5-4）。

あなたの会社に預けられたデータに固有の守秘義務を理解しなければならない（6-2）。

情報の分類・評価がなされることが続くステップとなる。情報に対して要求される要件を理解し、評価することになる。そしてその評価が客観性をもったものであることが大切になる。そして、実際に準備されるべき情報の保護手段は、組織内部のポリシーと一致しなければならないことになる。

クラウド事業者の選択

クラウド事業者の財政的実行可能性を念頭に置かなければならない（2-6）。

事業者は第三者によるリスク評価を定期的に行い、その結果を利用者が利用できるようにしなければならない（2-4）。

クラウド事業者とそれにかかわる第三者の関係は明示されなければならない（2-5）。

クラウド事業者の主なリスクとパフォーマンスの指標を理解し、利用者の観点からそれらをモニターおよび測定できなければならない（2-7）。

利用者は、クラウド事業者の事業継続およびディザスタリカバリープランを調査すべきである（8-5）。

利用者は、クラウド事業者のインフラストラクチャーの物理的依存関係を調査すべきである（8-6）。

もし実行可能であるならば、クラウド事業者によるビジネスの変化が顧客経験に影響を与えるかどうかを評価するために、そのクラウド事業者の別の利用者を見つけるべきである（9-3）。

クラウド事業者の顧客サービス機能を定期的にテストし、彼らのサポートレベルを判断

すべきである（9-7）。

クラウド事業者が、どのようなレベルのサービスを実際に提供するのか、これは、利用者からすると、ある意味で不確実性のきわみであるということになる。そこで、上述のようなガイダンス（なお、上記のガイダンスは、関連性のある一部のものということになる）に従った客観的な評価がなされるべきことになる。

技術的対応策

ドメイン 1 のアーキテクチャーフレームワーク、とりわけ SaaS、PaaS、IaaS の区別は、移植性、相互運用性のリスクを理解するために不可欠である（7-1）。

リスクマネージメントの観点からいえば、クラウド中に存在する非暗号化データは、利用者にとっては「失われたもの」と考えるべきである（12-1）。

クラウド事業者にとって ID 管理を成功させる秘訣は、堅牢なフェデレイティッド ID 管理アーキテクチャーを持つことと組織の内部に対する戦略を持つことである（13-1）。

仮想化された OS は、サードパーティーのセキュリティテクノロジーで補強し、クラウド事業者単独のプラットフォームへの依存を減少させるべきである（15-1）。

本解説の範囲を越えることになるが、暗号技術、ID 管理、仮想化技術などは、クラウドサービスの利用を考えるときに、基礎的な技術的な対応策ということになる。利用者としては、これらについての十分な知識をもとに、対応策を採用することが望ましいということがいえるであろう。

法的対応策

契約はすべての基準となるものであり、組織独自の要求とクラウドコンピューティングのダイナミックな性質に基づいて交渉できるものでなければならない（3-1）。

契約にはサービスレベルアグリーメント（SLA）を盛り込む（3-7）。

クラウド事業者の遵守すべき法令と利用者の遵守すべき法令の間にギャップがある可

能性があることを理解すべきである。そのギャップを明確にするために適正評価が必要である（3-3）。

クラウド事業者は、その情報セキュリティシステムが、利用者のデータを正確で信頼できる状態で保管されているという利用者からの要求に対して、それを保証するように求められる（4-4）。

クラウド事業者によるデータの二次的な利用の可能性を理解し、必要に応じてこれを禁止するための契約の文言を盛り込む（3-5）。

ストレージの地理的な場所を確かめる（14-2）。

国境を越えたデータの移動がある可能性を洗い出し、必要に応じて契約の文言にそれを禁止する条項を盛り込む（3-6）。

クラウド事業者との関係で一定のセキュリティレベルを維持するために、SLAは、有効な手段である。そして、その際には、種々の法的な要請に対しても、リスクをコントロールしうるような条項について情報を求め、契約のなかで議論することが重要になる。

実施・測定・検証と開示

規制の権限やビジネスの必要性がすぐに変化するように、オンデマンドの監査の正当性を維持しておくことが重要である（5-3）。

利用者は、クラウド事業者のオンサイト査察をいつでもできるようにすべきである（8-4）。

SAS70 TypeII 監査や ISO27001 認証は、広くセキュリティの能力を評価でき、両方を活用することで他のいかなる認証よりも信頼がおける（5-4）。

利用者が、クラウド事業者から提供を受けるサービスについて、どのようにコントロールを確保するかというのは、重要な問題であり、また、議論もなされているところである。この点については、今後、さらなる議論の進展が図られるものと考えられ、それらのなりゆきに注目しなければならないだろう。

解説　クラウド・セキュリティ・ガイダンス

II　法律問題編

日本クラウドセキュリティアライアンス

特定非営利活動法人

ASP・SaaS インダストリ・コンソーシアム

はじめに

本解説は、CSA クラウド・セキュリティ・ガイダンス　ver．1.0.（以下、　クラウド・セキュリティ・ガイダンスという）[25]を、主として日本のクラウドサービスの提供者・利用者（サービスの顧客であり、通常は、利用企業のことをいう。）に分かりやすく理解してもらうことを念頭に作成された「解説　クラウド・セキュリティ・ガイダンス」のうちの法律編である。本解説は、クラウド・セキュリティ・ガイダンスが、背景としている米国のクラウドサービスに関する独自の状況についての知識について乏しい読者においても、クラウド・セキュリティ・ガイダンスの要素を深く理解してもらうことを最大の目的としている。そして、クラウド・セキュリティ・ガイダンスを深く理解することによって、利用者が、クラウドコンピューティングの導入・利用に際して、よりスムーズにコンプライアンスのリスクに対応することができるであろう。

クラウド・セキュリティ・ガイダンスが背景としている米国の法律知識について乏しい読者においても、理解に必要なかぎりで、米国の法律と日本の法律の関係する部分を並列的に論じるようにこころがけることによって、クラウド・セキュリティ・ガイダンスの要素を深く理解してもらうことをこころがけている。

なお、本解説は、特定非営利活動法人 ASP･SaaS インダストリ･コンソーシアムの支援をもとに弁護士高橋郁夫、弁護士吉井和明が執筆を担当して、まとめたものである。

---

[25] 正式には、“Security Guidance for Critical Areas of Focus in Cloud Computing”（http://www.cloudsecurityalliance.org/csaguide.pdf）最新版は、バージョン 2.1 である。これの日本語訳「CSA クラウド・セキュリティ・ガイダンス　ver．1.0.日本語版」が、株式会社インプレス R&D より発行されている。なお、本解説において、クラウド・セキュリティ・ガイダンスとして引用しているのは、この日本語訳にもとづいている。また、G〇頁としているのは、このガイダンス日本語訳の頁数によるものである。

第１　クラウド・セキュリティ・ガイダンスのポイント

１　クラウド・セキュリティ・ガイダンスの構成

クラウド・セキュリティ・ガイダンスは、法律の問題に対応する部分としてドメイン３「法律」およびドメイン４「ｅ－ディスカバリ」の二つの部分からなりたりっている。全般的な構成として、リーガルリスクの適切な理解と把握を前提に「契約を中心としたリスクのマネジメント」「データの場所に対する留意の重要性」「説明責任の重要性」を強調するものであるということができよう。ドメイン３の「法律」についてみれば、これらの視点が「問題提起」を前提に、「継続的なコンプライアンス義務」「選択された法的課題」「データの保管場所に対する理解」「プライバシー保護の確保」「海外の法律への対処」「データの二次利用」「情報セキュリティ法の遵守」「セキュリティ違反への対応」「事業継続性の確保」「訴訟要求への対応」の各論点から論じられている。また、ドメイン４の「ｅ－ディスカバリ」についても、「問題提起」をもとに、法的ルールなどが検討されている。

本解説においては、日本におけるクラウドサービスの運用・利用の観点から、ドメイン３の「法律」の問題に加えて、ドメイン４の「ｅ－ディスカバリ」の提起する問題点を、「法律」に関する問題点として取り扱う。

２　問題提起について

ドメイン３の「問題提起」をきっかけに法律問題について検討してみることにしよう。クラウド・セキュリティ・ガイダンスは、「公的機関および民間企業に対して、保有する情報とコンピューターシテムのセキュリティに関して保護を行うことを要求している」としており、米国における種々の法律の適用があることを論じている。そして、この法律を遵守する義務は、経営者の義務であるということが強調されている。この経営

者の義務は、クラウドコンピューティングを利用する場合にも同様である。しかも、クラウドコンピューティングにおいては、重要なデータ、ファイル、記録などが第三者に委ねられているのであるから、当該企業組織は、その下請け契約業者、サービスプロバイダー、あるいは外注業者に対して適切なセキュリティ手段を講じることが課せられているのである。

この問題提起においては、法律の適用関係を熟知し、それを遵守する義務は、経営者の義務である、そして、その義務は、クラウドコンピューティングを利用する場合も同様である、ということが述べられており、ある意味で、これが、クラウドコンピューティングにおけるコンプライアンス対応を考えるキーポイントになることが語られている。

3　クラウドコンピューティングの法律問題の分析

3.1.各論点の位置づけ

では、クラウド・セキュリティ・ガイダンスがあげている具体的な論点をどのように位置づけ、問題として把握し、問題に対して応用しうるセキュリティガイダンスを導くかという点について考察してみよう。

まず、すべての問題について、問題提起でふれられているように「法律等を遵守する等の義務は、経営者の責務である」という認識が、根本的な要請になる。そして、この認識は、現代社会においては、客観的に遵守しているということのみではなく、適切な方法で社会に対して遵守していることに対する説明義務をはたさなければならないという形で認識されているのである。

そして、クラウドコンピューティングについては、仮想化という技術的側面とリモートにデータが所在するという側面（厳密にいうとき、分散コンピューティングであること）[26]から、「第三者の利用に伴うリスク」「ネットワークを通じることによるリスク」

---

[26] ドメイン４「RIM におけるクラウドコンピューティングのインパクト」の項では、「・少なくともビジネス上関係のある期間、顧客に関係する情報資産の維持管理についての主な責任がサービスプロバイダーに移行。」としている。

「インフラストラクチャの抽象化に伴うリスク」「仮想化技術による発生するリスク」があることが指摘される。この各点から生じるリスクの一般的な分析については、「導入・実装ハンドブック編編」　Ⅰ－５頁から分析されており、そこでの記述を参照されたい。

ガイダンスの「選択された法的課題」の項においては、適用される法律等が種々であることが論じられている。そして、この遵守を要求される法律については、「プライバシー保護の確保」「情報セキュリティ法の遵守（セキュリティ違反への対応を含む）」をはじめとして種々の法律がある。しかも、その法律等の適用関係は、「データの保管場所に対する理解」で明らかにされるように、データの保管場所によって左右されることがある。その結果、「海外の法律への対処」が課題として発生してくる。

これらの法適用の遵守は、仮想化技術とリモート処理の側面から、具体的な困難をともなっている。現実の社会では、利用者が、すべてのデータをもれなくコントロールしうることが要求されている。上記の説明義務の理論は、このような立場を前提としている。しかしながら、クラウドコンピューティングの環境のもとでは、このような前提がみたされないこともあることに留意しなければならない。「事業継続性の確保」「訴訟要求への対応」という論点は、特にこの前提の不完全さから導かれる問題であるということができる。また、リモート処理という観点から、「データの二次利用」に対する困難性も議論されることになる。

これらの問題点を認識したあとには、その問題点とデータの重要性に応じて具体的なセキュリティ対応策がとられなければならないことになる。この対応策として法的に重要なものは、「継続的なコンプライアンス義務」で論じられているような契約によるリスクへの対応である。その一方で、技術的・政策的な対応についても検討してければならないことになる。

3.2.　ガイダンスの深い理解のために

上述のような分析に基づいたときに、ガイダンスの深い理解のためには、具体的に（１）コンプライアンス義務の位置づけ（２）適用されるべき具体的な法と規則（３）国際的な法律の適用関係（４）セキュリティ対応策の法律問題の視点の各観点から、問題を抽出し、その上で、実践的なセキュリティガイダンスを導くというのが、有効なものとなる。

第２　問題

１　コンプライアンス義務の位置づけ

1.1.　コンプライアンス義務の位置づけ

多くの場合、これらの義務（注ー、保有する情報とコンピューターシステムのセキュリティに関して保護を行うことを要求しているーことをさす）は会社の経営者の責務である（G48 頁）。

経営陣もしくは従業員が、企業活動を行う際に、その企業活動が、かかる資本の効率的な運営目的をよりよく実現しているか、それを、利害関係者がチェックできるようにしておき、それによって、非効率的な資本運営を予防しようという内部統制のシステムは、資本と経営の分離する現代においては、経営者にとって当然の要請であるということになる。これは、米国においても日本においても当然のことである。そして、内部統制の構築義務は、わが国の判例や法律の条文のもと取締役の善管注意義務の一つの形態として認識されてきている[27]。そして、内部統制体制については、リスク管理システムやコンプライアンス確保の体制が、定義として含まれることになる[28]。また、米国にお

---

[27]大阪地判・平成 12 年 9 月 20 日（大和銀行事件第 1 審判決）や神戸製鋼所総会屋利益供与株主代表訴訟(平成 14 年 4 月 5 日)和解文言

また、取締役会としての決議事項（会社法 362 条 4 項 6 号）に「取締役の職務の執行が法令及び定款に適合することを確保するための体制その他株式会社の業務の適正を確保するために必要なものとして法務省令で定める体制の整備」が含まれている。

[28]会社法施行規則 100 条 1 項（なお、委員会設置会社については、同施行規則 112 条 2 項）は、内部統制システムを「取締役の職務の執行に係る情報の保存及び管理等に関する体制、損失の危険の管理に関する規程その他の体制、取締役の職務の執行が効率的に行われることを確保するための体制に関する事項、使用人の職務の執行が法令及び定款

いても、取締役は、会社の受託者（fiduciary）として、同様な地位にある通常の慎重な人間が同様な状況のもとにおいて用いると同様な注意をもってその職務を遂行しなければならない（受託者としての注意義務）し、また、もっぱら会社の最大の利益のためにその職務を遂行すべき（受託者としての忠実義務）とされている。この注意義務のひとつとして、取締役は、相当な注意を払って、役員の職務の執行が適法かどうかを監視しなければならないとされており、リスク管理・コンプライアンス確保についても同様であるということがいえる。

リスク管理・コンプライアンス対応が、当然の要請だといっても、実践は困難である。米国においては、エンロン、ワールドコム事件などをきっかけとして、無責任な抗弁[29]をなしうる土壌を改善しなければならないという共通認識が形成され、投資家の米国資本市場に対する信頼を取り戻すために制定されたのが、Sarbanes　Oxley 法（正確には、U.S. Public Company Accounting Reform and Investor Protection Act of 2002）[30]（以下、SOX 法という）であり、日本では、企業改革法などとも呼ばれている。この米国 SOX 法は、米国の資本市場に対する投資家の信頼を取り戻すために企業の経営者に対して厳しい責任を負わせ[31]、また、従来は、自主的な監督のみでなされていた監査

に適合することを確保するための体制、当該株式会社ならびにその親会社および子会社からなる企業集団における業務の適正を確保するための体制」と定義する。

[29]米国においても日本においても、なにか問題がおきると、それは、担当者がなしたことで、責任者としては「知らなかった」という抗弁がなされることが多かった(これらの抗弁は、Chutzpah defense（フッパ抗弁）－厚かましいという意味－といわれる)。

[30] この法律の解説については、種々の本がでている。「COSO フレームワークによる内部統制の構築」中央青山監査法人編（東洋経済新報社、2004）、ガイ　P．ランダー著　メディア総合研究所　訳　「SOX 法とは何か？米国企業改革法からＣＳＲ、内部統制を読み解く」（メディア総合研究所、2006）、スコット・グリーン著　三宅弘子・田沢元章・久保田隆・小澤有紀子・生田美弥子　訳　「SOX 法による内部統制構築の実践」（レクシスネクシス・ジャパン、2006）などを参照のこと

[31] 302 条および 404 条である。ここで、302 条について触れると、SEC 登録企業の経営最高責任者（CEO）と財務最高責任者（CFO）に対して、所定の文言による宣誓書に個人名で署名し、それぞれの宣誓書を別々に年次報告書に綴じ込むことを求めている。また、404 条は、経営者に対して、会計年度末における財務報告にかかる内部統制の有

の質の保障という点について、会計監査や内部統制の監査の基準を制定し、さらにその監督を行うために、公開企業会計監視委員会（PCAOB）を設置するということを基本的な枠組みとしようとするものである[32]。

このような枠組の基本的なところ[33]は、我が国においても、金融商品取引法が制定され（証券取引法の一部改正）、経営者確認書（同法 24 条の 4 の 2）、内部統制報告書（24 条の 4 の 4）、監査報告書（同法 193 条の 2）の 3 つの報告書の制度を中核とする内部統制のための制度が組み込まれることになり、導入されるにいたっている。

これらの内部統制制度において、リスク対応・コンプライアンス対応は、きわめて重要な役割をしめることになる。したがって、クラウドコンピューティングにおけるリスクおよびコンプライアンス対応は、経営者にとって当然の要請ということになる。

1.2.責任と説明義務について

クラウドサービス事業者が一方での当事者として民事訴訟に関与する場合、あるいは、政府当局によって、内部に対する調査が執行される場合、クラウドサービス事業者は、ホスティング事業体として保管する情報データへのアクセスを要請される（G58 頁）。

効性評価と評価結果の年次報告書での開示をすることを求め、そして、それについて、公認会計士による監査を受けることを要求している。

[32] SANS Institute“The Impact of the Sarbanes-Oxley Act on IT Security”(http://www.sans.org/rr/whitepapers/casestudies/1344.php)” rights.

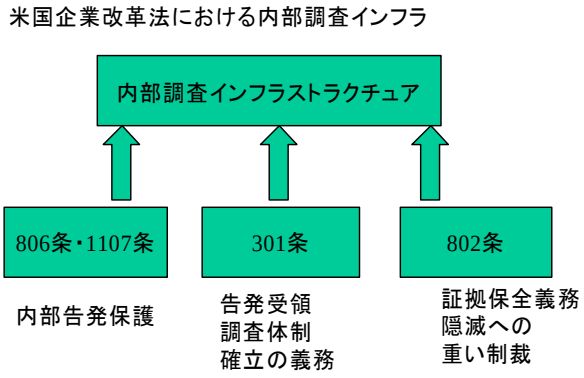
同、The Role of IT Security in Sarbanes-Oxley Compliance”
(http://www.sans.org/rr/whitepapers/legal/1376.php)

[33] もっとも、詳細に見たときには、米国 SOX 法において特筆すべきは、特に、経営者の宣誓書に虚偽があった場合の刑罰の重さという点から日本法とは　実際のインパクトが違うのではないか、また、損害賠償という点からも適時開示違反を請求原因として訴訟が提起されうる点、訴訟制度としてディスカバリ、クラスアクション制度がある点などで重要な違いがあるとかんがえることもできる。

不祥事があったさいに、しばしば、いわれるのが、企業ぐるみの犯罪であるとか、また、企業ぐるみで証拠を隠蔽しようとしたということである。このような行為がなされれば、企業は、致命的なダメージを受けてしまうことはいうこともないであろう。現代社会においては、コンプライアンスの要請は、法令等についての遵守のみを意図するものではなく、むしろ、その遵守について、相当の根拠をもって、社会に対して説明責任を果たさなくてはならないというところまで包含するものとなっていることに留意しなければならない。この点は、米国[34]においても日本においても、全く共通である。我が国において、2010 年 7 月に、日本振興銀行が、電子メールを組織的に消去したという検査妨害罪で、消去時の役員が逮捕されたという事件があった。この事件は、不正行為については、すべての証拠でもって、その不正行為が存在しないことを明らかにしなければならないという義務を経営者が負っていることのひとつの展開とみることができるであろう。

---

[34]説明責任の観点からみるとき、米国 SOX 法は興味深い。そもそも、同法第 8 章は、「企業および刑事不正行為説明責任法 2002」とも称されており、また、第１１章は、「企業不正説明責任法 2002」とも称されている。SOX 法 802 条は、（あ）合衆国の然るべき機関の捜査・執行権限から免れ、妨害し、影響を与えようとする行為（い）会計人が企業の会計もしくは報告記録の維持の義務を定め、それに違反する行為について、刑事罰を定める。また、同法 805 条は、司法妨害や刑事不正行為に対する連邦量刑ガイドラインについての見直し、806 条は、内部告発者保護、807 条は、公開会社の株主による詐欺に対する刑事処罰を定めている。また、1102 条においては、公的な手続について、記録、文書その他の物を改竄、破棄、隠匿することを処罰している。



このような現代的な説明責任の思想は、すべての証拠について企業が管理しうるものであるということを前提としている。その一方で、クラウドコンピューティングにおいては、このような前提を満たすことができないことも起こりうる。これをどのように考えるかというのが、現代社会において重要な役割を果たすようになってきていることに留意する必要がある。

２　適用法令等をめぐる議論について

2.1.　法令等の適用の問題の複雑性について

クラウドコンピューティングに関しては、どこの国の法律が適用されるのですかと聞かれることがある。しかしながら、これに対する簡単な答えは実は、存在しない。これは、まず、各国における法の適用に対する考え方がそれぞれであり、どこの国の考え方を基準にするかをまず設定しなければならないということがあるからである。日本の考え方で、アメリカでの処理を語ることはできない。その上に、適用が問題になっている法律自体の性格の問題が存在する。政府の執行力に関する法律規定であれば、その執行力の限界に関して、各国の主権のおよぶ範囲に限られるということがある。また、法律自体も、適用の問題なのか、執行の問題なのかで、それぞれ限界が異なってくる。その上に、クラウドコンピューティングにおいては、「インフラストラクチュアの抽象化に伴うリスク」「仮想化技術による発生するリスク」があると述べたが、それにより「データの所在が把握しにくいこと」と「データが国の領土を越えて保存されること」になる。まさに、これらの要素が交錯するところに、クラウドコンピューティングの法律の適用の問題が発生してくる。これらの観点から、限界的な事例では、きわめて複雑な問題を惹起しうるということを認識しておく必要があり、これらから生じる問題については、本章の３「国際的な法律の適用関係」で論じることになる。

議論を簡単にするために、以下においては原則としてデータを処理する主体が日本において、活動しており、収集されるデータも主として日本に存在するという場合から議論を進めることにする。

2.2. 具体的な適用法令等について

（１）個人情報保護法・プライバシー保護法制について

企業は、その顧客や従業員に関するプライバシー情報の保護や、このようなデータが二次利用されないこと、また、第三者に対して開示を行わないという法的義務を有する（５３頁）。

現代社会で、もっとも、議論されている権利のひとつが、プライバシーに関する権利ということができるであろう。法的な立場から、プライバシーの最大公約的な定義を探すと、一般的に「ひとりでいさせてもらいたいという権利（the　right to be let alone)」であり、不当な公開から自由である人間の権利であると理解される。しかしながら、法的にプライバシーをどのように認識すべきかという点については、その後、特に現代の情報化社会と関連して種々のバリエーションが存在している。また、世界的には、「プライベートと家族生活の尊重の権利（Right to respect for private and family life）」を中心に論じられており、どちらかといえば、自律（autonomy)に関する概念として議論されている。

プライバシーとデータ保護の制度

個人に関する情報に関するプライバシの問題を考え、それを法的な制度から考えるときには、「プライバシーの制度」および「データ保護（我が国では、個人情報保護）」の二つの制度について検討することになる。両者は多くの点で重なり合うが、同一の概念ではなく、その他プライバシーを保護するための一般法は存在しないものと解される[35]。

個人情報保護法

個人情報保護法における個人情報とは、「生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの」であり、個人情報を含む情報の集合物である個人情報データベース等を事業の用に供している者で、個人情報保護法（以下、単に「法」という。）２条３項各号に掲

---

35 この点については、見解の対立が存在する。堀部政男編著「プライバシー・個人情報保護の新課題」（商事法務、2010 年 4 月）61 頁以下。

げる者を除いた者が個人情報取扱業者とされ、個人情報保護法[36]の遵守を要求される[37]。

クラウドサービスの利用と個人情報保護法との関係について考えると、個人情報保護法の遵守という観点からは、（１）クラウド事業者と個人情報取扱事業者（２）同法における第三者性･外部委託にかかわる問題点（３）管理上の必要性から生じる問題点（４）その他の問題などがある。

（１）については、クラウド事業者自体が個人情報取扱事業者となるか否かが問題となる。個人情報を形式上保有しているように見える事業者でも、個人データの内容に関知しないため、そもそも「個人情報データベース等を事業の用に供して」いることにならない場合（倉庫業者、運送業者、書店など）もありうるが[38]、これはクラウドコンピューティングでも同じで、特に IaaS のようなリソースの提供を主目的とする形態の場合、個人情報データベース等を積極的に事業の用に供することは行わず、クラウド・ベンダーが個人情報取扱事業者とされない可能性もある（これはクラウドの形態のほか、契約内容によっても異なると思われる）。

---

[36]我が国における個人情報保護法制は、基本法部分と個人情報取扱事業者の保有する個人情報について規定する①「個人情報保護法」と、行政機関の保有する個人情報について規定する②「行政機関の保有する個人情報保護に関する法律（以下「行政機関個人情報保護法」という。）、③独立行政法人等の保有する個人情報の保護に関する法律、地方自治体の保有する個人情報について規定する④個人情報保護条例」により構成されており、その規制態様や個人情報取扱事業者が負う義務についても自ずと異なる[36]。本解説は、一般ユーザのクラウドサービスの利用に際しての手引きを旨としており、個人情報保護法の適用の関係について論じる。

[37] 保有個人情報の特定の個人の数の合計が過去６月以内のいずれの日においても 5000 件を超えない者を除く（ただし、保有する個人情報データベース等の全部又は一部が他人の作成に係るもので、個人情報保護法施行令 2 条各号のいずれかに該当するものを編集し、又は加工することなくその事業の用に供するときは、上記 5000 件の中からその分が控除されることになる）（個人情報保護法 2 条 3 項 5 号、個人情報保護法施行令 2 条）。

[38]消費者庁作成の「わかりやすい個人情報保護のしくみ」２１頁参照のこと

（２）について、個人情報保護法は、第 23 条１項において、個人情報取扱事業者は、本人に同意をえないで個人データを第三者に提供してはならないとしている。したがって、クラウドサービスの利用において、そもそも、データが「提供」されることになっているかという点について検討する必要がある。「提供」とは、「さし出して相手の用に供すること。」（広辞苑第六版）をいう。したがって、データについて提供が議論される場合には、その第三者がデータに対して、一般的な処理（複製、閲覧、変更、消去など）の権限を有しているか否かを議論すべきことになる（第三者が利用可能かどうかということである）。データが、クラウド事業者において、処理されるか否かという点について考えると、いわゆる SPI モデルごとに、議論のポイントが異なってくることになる。PaaS および IaaS のモデルにおいては、データは、利用者みずから、処理権限を有しており、そもそも「提供」されているとはいえない。その一方で、SaaS のモデルにおいては、一般的に、クラウド事業者は、データに対して、処理権限を有しうるが、このような行為は、契約によって禁止されている。わが国において、この点が「提供」に該当するかどうかについて詳細な議論はいまだなされていない。しかしながら、同法においては、「利用目的の達成に必要な範囲内において（略）委託」する場合については、第三者ではないとされており（法２３条４項）、また、委託の趣旨・目的が明確であり、また、終了時におけるデータの返却・消去などが限定される場合に、同法は、２２条で「委託」として委託先の監督を定めている趣旨からして、SaaS のモデルにおいても、第三者に提供ということにはならないと考えられる。この場合においては、利用者は、法２２条に従い、「委託を受けた者に対する必要かつ適切な監督を行わなければならない」ことになる。この場合の「安全管理」「委託を受けた者」「必要かつ適切な監督」が如何なるものであるかについては、個人情報保護に関する基本指針が定められているほか、各分野毎に主務大臣等の定めた指針、ガイドラインにより定義されている（２４分野について４０のガイドラインが策定されている）。 基本指針においては、「漏えい、滅失又はき損等をした場合に漏えい、滅失又はき損等をした場合に本人が被る権利利益の侵害の大きさを考慮し、事業の性質及び個人データの取扱状況等に起因するリスクに応じ、必要かつ適切な措置を講じる」べきこととし、「その際には、個人データを記録した媒体の性質に応じた安全管理措置を講じることが重要」とする[39]。また、

---

[39] 個人情報保護に関する基本方針 10 頁（http://www.caa.go.jp/seikatsu/kojin/）。

「委託を受けた者」について、委託元は、委託先の監督義務の一環として、委託先が再委託先を適切に監督しているか否かも含めて監督する義務を負う[40]。以上のような観点から、クラウド事業者に対する選択・監督等について深い注意が求められることになるが、この点の詳細については、本解説の「導入・実装ガイドブック編」を参照されたい。

（3）管理等の必要性から生じる問題点については、

データベースの機密性、セキュリティ、あるいはそのプライバシー確保に懸念が生じる場合、あるいは、こうした情報データへアクセスできる対象者に対してコントロールをかけたい場合、情報データの管理者としてクラウドサービス事業者には何ができるのかという点をサービス利用者として把握・理解しておきたい（G55 頁）。

という記述が注目される。クラウド事業者は、自社ビジネスのコントロールの保持、運用管理上の柔軟性の確保、費用の削減などの観点から、データに対するアクセス権付与やセキュリティ対応選択について自ら講じる自由度を確保しておきたいと考えている（G56 頁）。しかしながら、個人情報保護法のもとでは、もし、通常の場合のサービス事業者に対するアクセス権の制限、サービス終了時のデータの消去、返還が適切になされない場合には、そもそも、委託という評価を受け得ないのではないか、むしろ、原則として禁止されている第三者提供になってしまうのではないかということになる。また、クラウド事業者は、誰が何の情報を閲覧したか、いつ、あるいは、何のクエリーや検索を実行したかという非常に価値のある情報を取得したがるかもしれないのである。これらの行為は、利用者自身の個人情報保護ポリシーやプライバシー・ポリシーに反してしまうことが起きてしまうことになりかねない。

---

[40]個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン 2-2-3-4（http://www.meti.go.jp/policy/it_policy/privacy/）では、「また、委託者が受託者について『必要かつ適切な監督』を行っていない場合で、受託者が再委託をした際に、再委託先が適切といえない取扱いを行ったことにより、何らかの問題が生じた場合は、元の委託者がその責めを負うことがあり得るので、再委託する場合は注意を要する。」とする。

（4）その他の問題として、個人情報保護体制の構築に際して検討すべき事項、国際的な法の適用関係からおきる問題が存在する。前者については、解説の「導入・実装ガイドブック編」を参照されたい。また、後者については、本解説において後述する。

プライバシーを根拠とする損害賠償

プライバシーの利益に対する認識は、「ひとりでいさせてもらいたいという権利（the right to be let alone)」から、次第に拡張されるにいたっている。とくに米国においては、「不法侵入」「私的事実の公開」「公衆の誤認」「盗用」の類型にわけて、不法行為が議論されるようなっている。

日本においては、プライバシー権は、いわゆる「ひとりで放っておいてもらう権利」[41]としてアメリカで判例上発展したものについて、「宴のあと」事件第１審判決(東京地判昭和３９年９月２８日、下民集１５巻２３１７頁)において、「いわゆるプライバシー権は私生活をみだりに公開されないという法的保障ないし権利として理解されるから、その侵害に対しては侵害行為の差し止めや精神的苦痛に因る損害賠償請求権が認められるべき」とされ、その後最高裁においても、多くの事件において、プライバシー侵害による不法行為責任が認められてきた。法的な効果としては、プライバシー権侵害がなされた場合の法的回復手段として、私法上の人格権たるプライバシー権が侵害されたものとして、不法行為に基づく損害賠償請求権、差止請求権などを行使することができる。情報セキュリティ関係では、情報漏えいに関する情報主体から、漏えいさせたものに対する損害賠償請求が、プライバシーが法的に保護されるべき利益であるとしてなされることになる。

このような事案において、米国においては、漏えいがあった場合に，情報を管理していた者に対して情報主体からの損害賠償を認めるかどうかという議論については、むしろ、現実の損害が存在しないという判断をする判決が多数である[42]。また、法律、規制、

---

41 芦部信喜　高橋和之補訂「憲法 第四版」（平成 19 年、岩波書店）

42 Ruiz v. Gap, Inc. (9th Cir. May 28, 2010)において、判事は、データ流出事件において抽象的なプライバシーの侵害があったという主張のみでは、具体的な請求として認容されないとしている、Erick Goldman“9th Circuit Affirms Rejection of Data Breach Claims Against Gap -- Ruiz v. Gap”（Technology & Marketing Law Blog）（http://blog.ericgoldman.org/archives/2010/06/9th_circuit_aff.htm）。また、同ブログによれば、米国においては圧倒的多数が、この判決の立場と同様であるとのことである。

国際規格、ベストプラクティスなどに対する違反が、不法行為を構成するのかどうかという論点も存在する。

これに対して、我が国においては、ヤフーBB 事件[43]、TBC 事件[44]などにおいて、事業内容等に応じて、個人情報保護のために安全対策を講ずる法的義務があるものとして捉えて、損害賠償義務を認めるのが一般になっている。

なお、利用者が、クラウド事業者にデータを委ねていて、そのクラウド事業者から、データが漏えいしてしまった場合における利用者と事業者との間の損害賠償の責任の範囲というのが問題になろう。具体的には、情報主体が（１）利用者およびクラウド事業者に対して損害賠償を求める場合の請求原因の構成（２）利用者とクラウド事業者間の契約が、上記損害賠償もしくは求償関係に与える法律上の意味などが問題になる。ここで、情報漏えい事件において下請と元請との責任分配が問題となったケースとして、山口地判平成 21 年 6 月 4 日（公刊物未登載）がある[45]。

---

[43] 大阪地判平成 18 年 5 月 19 日（判タ 1230 号 227 頁）、大阪高判平成 19 年 6 月 21 日（運営会社である BB テクノロジーが電気通信事業者としての安全管理義務を負うところ、ユーザー名、パスワードの管理が不十分であり、リモートアクセスにおける注意義務違反があったものとして、大阪地裁では原告１人当たり５０００円、大阪高裁では原告１人当たり４５００円と原告１人あたり１０００円の弁護士費用の支払いを命じた）

[44] 東京地裁平成 19 年 2 月 8 日（判タ 1262 号 270 頁）は、個人情報を取り扱う企業に対しては、その事業内容等に応じて、個人情報保護のために安全対策を講ずる法的義務が課せられていたものとし、受託会社の不法行為責任を認めたほか、本件ウェブサイトの管理を主体的に行い、受託会社 に委託したコンテンツの内容の更新、修正作業等についても実質的に指揮、監督しており、受託会社には、独立した判断や広い裁量がなかったものとして使用者責任を認めている。この事件では、漏えいした情報が秘匿されるべき必要性が高い情報であること、広く流出し、回収困難となっている情報流出の態様等に照らし、顧客１人当たり各２万２０００円から３万５０００円の慰藉料の支払を命じた。

[45]原告が個人情報取扱業者として個人情報の安全管理義務を負っていたにもかかわらず、個人情報の管理について、業務に先立ち、個人情報は作業完了後は直ちに消去するよう被告従業員らに注意をしたのみで、貸与パソコンによって持ち出す個人情報の管理については、専ら被告に任せていたことについて、原告に安全管理義務を怠った過失 が

行動履歴等の集積・分析と利用についての主体の利益

なお、プライバシーに関する法的規制という観点からは、個人情報の定義に該当しない情報であったとしても、利用者の行動履歴等を分析することによって得られた情報をその分析者のため利用することが、プライバシーの観点から法的な問題点を惹起するのではないかということが議論されている。いわゆるライフログの法律問題である。「パーソナル情報研究会」「次世代パーソナルサービス推進コンソーシアムについて」[46]の議論や「利用者視点を踏まえた ICT サービスに係る諸問題に関する研究会」[47]などにおいて、これらの問題は議論されている。その分析者の立場、分析および利用目的などにおいて、できるだけ、公正であると評価される状況のもとでの行動履歴等の取得・処理が問題になるというのがこれらの検討の結果であるということができよう。この理は、クラウド事業者においても同様である。ガイダンスにおいても

クラウドサービス事業者は、マーケティングや市場調査目的で、二次利用者の立場で会社の情報データやメタデータの情報マイニング能力を持ちたいと考える（G55 頁）。

と指摘されている。我が国においては、このような行動履歴等の取得・分析等については、議論となりうる余地がありうることは留意しておく必要がある。

連邦プライバシー法の議論について

米国の下院において、一般的なプライバシー法を導入すべきではないかという点について、Bobby Rush 議員の提案などを契機に議論が開始されている[48]。そこでは、個別の

あったとして原告から被告への情報漏えいによる損害賠償額について４割の過失相殺をおこなった事案。

[46] http://www.igvpj.jp/index/cat12/post-60.html

および 「次世代パーソナルサービス推進コンソーシアムについて」（http://www.igvpj.jp/index/pdf/consortium.pdf）

[47] http://www.soumu.go.jp/menu_sosiki/kenkyu/11454.html

[48] 提案については、
http://www.boucher.house.gov/images/stories/Privacy_Draft_5-10.pdf

なお、佐藤よしひろ「我輩は連邦プライバシー法である。まだ名は無い・・・」（砂糖の甘い付箋、http://yoshihiro.cocolog-nifty.com/postit/2010/05/post-cfa3.html）は、この提案を紹介しており、また、「米国連邦プライバシー法-第２案」

情報ごとに、プライバシーとして、センシティブなものか、そうでないものかというクラスわけがなされており、米国の現時点でのプライバシーに対するアプローチとの乖離も目につくところである。この法律については、実際に導入されるとなると経済に悪影響を及ぼすのではないかと強い批判がなされている。今後の動向に注意をしておく必要はあろう。

HIPAA 法

米国において、従来は、個人のプライバシーを保護すべき各州の規定がきわめて不十分な状況にあり、十分な対応がなされていなかった。1996 年に、Health Insurance Portability and Accountability Act（「医療保険の移転とそれに伴う責任に関する法律」、以下、HIPAA 法という）が、定められており、その後、その法律に基づく、プライバシルールおよび情報セキュリティルールが定められた。米国において、それらのルールがきわめて注目されるようになっている。HIPAA 法は、そもそも、ある企業の被傭者が、別の州の企業に転職した場合、前の企業でかけていた医療保険を一緒に持っていくことを可能にする法律であった。しかしながら、アメリカ全土における医療情報の標準化が必要であり、そのためにコンピュータ情報に変更、統一することにより、合理化、医療費削減の目的を果たそうという目的を有していたため、それを実装するためにプライバシー対応や IT セキュリティ対応の必要が出て、結局、HIPAA 法に基づくプライバシルール[49][50]とＩＴセキュリティルール[51]が定められ、施行されることになった。

（http://yoshihiro.cocolog-nifty.com/postit/2010/07/--c84e.html）で他の議員による提案を紹介されている。

議論の状況については、“Tech firms warn privacy bill will harm economy“（http://news.cnet.com/8301-31921_3-20011435-281.html）

[49] HIPAA 法の授権の下、連邦政府厚生省が制定した行政命令の形をとるプライバシルールが定められている。この具体的なルールは、（ア）規制機関－Office of Civil Rights（OCR）（人権保護局）、（イ）対象機関（CE-Covered Entitiy）（ウ）個人識別医療情報の定義（エ）匿名化情報の利用（オ）（キ）公益目的として許可がなくても利用および提供が認められる場合などの内容が定められている。

[50] HIPAA 法の定めるプライバシー部分については、米国経済再生法（American Recovery and Reinvestment Act of 2009：ARRA）のタイトル 8「経済的および臨床的

GLB 法など

米国において 1999 年に制定された金融サービス近代化法（グラムリーチブライリー法）は、金融機関における個人情報の取扱についても一定の指針を与えている。これは、金融の分野で規制緩和が進んでいることや、多重債務防止のために金融機関相互で貸付記録などの相互利用が行われるようになっていたことが背景にあった。この法律は、金融機関（投資アドバイザー会社を含む）にプライバシー保護方針を明示することを義務づけ、消費者が自らの個人情報の利用に関する選択を行う際に指針となる情報を提供することを求めている。また、個人情報の第三者提供についても定めており、関連会社においては、特に法律の規定がないが、関連しない第三者企業に対しての提供については、オプトイン・オプトアウト権の行使が可能になっている。もっとも、この場合でも外部への業務委託、共同マーケッティング、本人が求める取引の遂行上必要な場合は、オプトアウトの対象外になるとされている。また、金融機関プライバシー保護法（Financial Institution Privacy Protection Act ）はグラムリーチブライリー法を強化し、プライバシー侵害 1 件ごとに、企業役員および取締役に 10、000 ドル以下の罰金を科すことを定めている。

健全性のための医療情報技術に関する法律（Health Information Technology for Economic and ClinicalHealth Act：HITECH）」によって、さらに、執行が強化、適用対象の拡大、情報流出時の通知が定められている。デジタルガバント「米国 HIPAA 法による医療情報化への影響」米国マンスリーニュース 2009 年 9 月（http://e-public.nttdata.co.jp/f/repo/648_u0909/u0909.aspx）参照のこと。

51　ＩＴセキュリティルールは、外部と内部の脅威、セキュリティの脅威と脆弱性にフォーカスするものである。そこでは、患者の医療情報、関連情報を見て、送信して、保存するコンピュータ・ワークステーションの保護を含むものであるし、また、ポリシーの制定、文書化、監査ルートの作成についても触れている。そこでは(ア)対象機関（イ）管理的手続き（ウ）物理的安全対策（エ）技術的セキュリティサービス（オ）技術的セキュリティメカニズムなどが論じられている

（２）その他の情報セキュリティに関する法律について

情報セキュリティポリシの構築とその執行

企業は、自社の知的財産、その他の資産、および従業員や顧客、契約にかかわる個人情報を保護するため、常に妥当なセキュリティレベルを確保しておかなければならない。こうした義務は、数多くの法律、規制、国際規格、ケース、およびベストプラクティスに起因している（G55 頁）。

各利用者は、リスク管理態勢の一つとして、情報セキュリティポリシを構築しており、それを運営しているのが一般的である。この場合、日本においては、具体的な状況に応じて、個人情報保護のために安全対策を講ずる法的義務があるとして、損害賠償を認めるという法理が発展しているが、むしろ、米国においては、連邦取引委員会（FTC）が、連邦取引委員会法（FTC Act）にもとづいて、セキュリティ管理態勢の整備を求めうるという形になっている。この仕組みが活用されたのが、Twitter 事件である。これは、Twitter のセキュリティ対策が十分でなかったことから生じた複数のセキュリティ侵犯事件に対して、調査をおこない、同社に対して、セキュリティ・ポリシーやプライバシー・ポリシーをきちんと遵守することなどを命じ、同社がこれに同意した[52]という事件[53]である。FTC の調査した事実[54]によれば、同社は、2006 年より 2009 年 7 月にかけて、ほとんどすべての従業員にシステムの管理権限を与えており、パスワードのリセット、非公開のつぶやきの閲覧、ユーザー名でのメッセージ送信ができるようになっていた。また、管理用パスワードの強度を確保すること、失敗したログインが続いた場合、そのアカウントを停止すること、管理用ログインウエブページを別個に作成すること、などを怠っていた。これらの懈怠が原因で、2009 年 1 月には、侵入者は、ブルートフォース攻撃によって管理者パスワードを取得し、非公開の情報やつぶやきにアクセスした。また、侵入者は、パスワードをリセットし、無権限で、他人のアカウントから、つぶやきを送ったりした。オバマ大統領が、調査に応じると、500 ドル分のガソリンが当たる

---

52 同意命令は、http://ftc.gov/os/caselist/0923093/100624twitteragree.pdf

53 Tech Crunch 「FTC、Twitter に対して「今後 20 年間ユーザーを惑わせる」行為を禁止」(http://jp.techcrunch.com/archives/20100624ftc-twitter-privacy-settlement/)

54 訴状については、http://ftc.gov/os/caselist/0923093/100624twittercmpt.pdf

という懸賞を薦めるつぶやきをしたというのもこの方法で送られた。また、同年４月27日にも、また、侵入がなされ、ユーザーの非公開情報や非公開のつぶやきにアクセスしうる状態になった。

これらの事実関係をもとに、Twitterは、非公開のユーザー情報に対して無権限でのアクセスを防止する対応策等やユーザーのプライバシーを尊重するための対応策をとることなどで　FTCと合意をした(上記の同意命令参照)のである。

情報漏えいについての主体への通知

米国においては、情報漏えい時における情報主体に対する通知が、情報セキュリティに関する法律の問題として議論されている。この代表的な法は、カリフォルニアデータセキュリティ法（California Data　Security Act　、The Security Breach Information Act (S.B. 1386)ともいう）であるが、これは、州政府機関およびカリフォルニアで営業している民間企業に対し、暗号化されていない個人情報の漏洩があった場合、あるいは漏洩が疑われる場合に、原則としてカリフォルニア州の住民に通知することを義務づけている。もっとも、この法律では、データが暗号化されていた場合には、通知する必要性はないと解されている。この法律は、２００３年７月に実現されたものであるが、現在（２０１０年４月現在）では、４６の州で、このようなセキュリティ侵犯通知法（State Security Breach Notification Laws）が採用[55]されており、米国においては、連邦も含めて、一般的に採用すべきではないかと議論[56]されている。もっとも、この仕組み自体、むしろ、情報漏えいの報告件数を減らすような力が働いているのではないかという批判もある。

このような情報漏えい時の情報主体に対する通知という制度がクラウドコンピューティングに適用される場合には、情報漏えいがあった場合に、各利用者ごとに独立性がなされている場合であっても、クラウド事業者を利用している者すべてに通知しなければいけないのかという論点が発生することになる。

---

[55] http://www.ncsl.org/Default.aspx?TabId=13489

[56] Shannon Kellogg　“Data security and breach legislation -- will a new year and a new Congress = a national law?”
（http://www.rsa.com/blog/blog_entry.aspx?id=1173）

この点は、我が国においても、「個人情報の保護に関する基本方針」（平成１６年４月２日閣議決定）[57]をはじめとして、各分野のガイドラインにおいても、情報漏えい事件の発生時に情報主体に対する通知が必要であると記載されている点で同様である。クラウド事業者において、情報漏えい事件が発生した場合に、これらの通知が、どの範囲までになされなければならないかという問題が発生することになるであろう。

（３）情報セキュリティに関する国際規格等について

利用者における法令・基準等の遵守という観点からするとき、情報セキュリティに関する国際規格等は、利用者自身においても、遵守すべき対象となりうる。例えば、CSA クラウド・コントロール・マトリックス（以下，「CSA CM」という）においては、１１分野９８項目にわたるコントロールエリアが設定されており、それぞれ、従来から存在する規格、法令（COBIT、HIPAA、ISO/IEC 27002-2005、NIST SP800-53、PCI DSS）によりマッピングされている。ここでは、このうち、国際規格である COBIT、ISO、PCIDSS について簡単にふれることにする。

COBIT

COBIT（Control Objectives for Information and related Technology）は、企業に採用され、企業経営者、IT 専門家、保証専門家が日常的に利用する国際的に受け入れられた最新の IT ガバナンスのコントロールフレームワークの研究、開発、普及、および促進を行うことを目的とし、IT を４つのドメイン と３４のプロセスに分解して分析をおこなっている 。対象となる情報については特に限定がない。COBIT の特徴は、ビジネス重視、プロセス指向、コントロールベース、成果測定主導であり、特にビジネス重視の志向と成果測定主導が際だった特徴を有しているといえる。

成果測定については、各０（不在）から５（最適化）までの５段階に分け、当該フレームワークの達成状況を可視化するものである。３４のプロセスそれぞれに詳細なレベル設定がなされており、企業の成果レベルの把握、改善、コストの正当性の分析に資する。なお、CSA CM はコントロールエリアの存在を示すものであって、具体的な適用方法、評価方法については定められていない。

---

[57] http://www.caa.go.jp/seikatsu/kojin/kakugi2009.pdf

CSA CM がクラウド環境におけるセキュリティを第一に考えるフレームワークであるのに対し、COBIT がビジネス重視の志向を有している点で、完全には重ならならず、COBIT がマッピングするマトリックスのコントロールエリアは、29 のドメインである。

ISO27001、ISO27002

ISO27001、ISO27002 は、国際標準化機構（International Organization for Standardization）により定められた国際標準規格であるが、それぞれ日本工業標準調査会（JISC、Japanese Industrial Standards Committee）より、JISQ27001、27002 として日本語版がリリースされている。

ISO27001 は、情報セキュリティマネジメントシステム（ISMS）を確立、導入、運用、監視、レビュー、維持及び改善するためのモデルを提供することを目的とする要求事項を規定したものであり、ISO27002 は、組織における情報セキュリティマネジメントの導入、実施、維持及び改善のための指針及び一般的原則について規定するものであって、情報セキュリティマネジメントの共通に受容できる目標に関する一般的手引きを提供するものとされ、両者は、前者が要求条項、後者がこれに対する実践規範という関係にある。

ISO27001、ISO27002 により保護される対象となる情報は、保有情報資産全般であり、特に制限はない。ISO 27001 の付属書 A は、ISO 27002 の管理目的と管理策をそのまま表の形式にしたものであり、ISO 27001 の要求条項に対する実施規範を一覧できる形になっている。 ISO27001、27002 による要求条項とこれに対応する実施規範は、かなり網羅的であり、CSA CM との関係でもそのほとんどをマッピングしているが、管理策の具体性はそれほど高くはない。

PCIDSS

JCB-Global のサイトによれば、PCIDSS（Payment Card Industry Data Security Standard）は、「加盟店様・決済代行事業者様が取り扱うカード会員様のクレジットカード情報・お取り引き情報を安全に守るために、CB・American Express・Discover・MasterCard・VISA の国際ペイメントブランド 5 社が共同で策定した、クレジット業界におけるグローバルセキュリティ基準」とされている 。

PCIDSS は、安全なネットワーク構築と維持、カード会員データの保護、脆弱性管理プログラムの整備、強固なアクセス制御手法の導入、ネットワークの定期的な監視およびテスト、情報セキュリティにポリシーの整備という目的に合わせた 6 つのグループの中に、12 の要件を設定しているが、その要件は、「カード会員データを保護するために、ファイアウォールをインストールして構成を維持すること」（要件 1）などの、かなり実践的なものとなっている 。

また、クラウド環境において重視される情報の隔離についても、要件とはされていないものの、PCIDSS のメインドキュメントにより推奨されている。

さらに、第三者・アウトソーシングに関しても言及されており、サービス事業者による PCIDSS 準拠確認、準拠に関するレポートへのサービス事業者の各役割の記述を要求する、保存と廃棄のポリシー作成、暗号化キー、ID 管理、監査、時刻同期など、クラウド・セキュリティに関連する事項について規定されているほか、付録 A として、共有ホスティングプロバイダ向けの PCIDSS 追加要件が定められている。

PCIDSS 自体は、前述のとおり、ペイメント・カード業界における情報セキュリティ基準を定めたものであるが、業界を超え、情報セキュリティ基準の参考とされている。

2.3. 一般的なセキュリティリスクについて

（1）位置づけ

ここまで、個々の法律等の適用に関するコンプライアンスリスクについて検討してきた。しかしながら、そのような個別の法令等の提要から生じるコンプライアンス問題以外にも、一般的なネットワークセキュリティから生じるリスクに対するリスク管理についても検討しなければならない。

（2）ネットワークセキュリティの問題

クラウドサービスについては、そのサービスが、ネットワークを通じて提供されることから、通常のネットワークセキュリティで問題になるのと同様に、機密性、インテグリティ、可用性、否認不可性（Nonrepudiation rule）、通信の機密性の保護の要素が、それぞれ検討されなければならない。脆弱性が発見されて、それの対応の遅れから、保

存していたデータが漏洩するということもあるだろうし、また、悪意ある内部者から情報が漏洩することもありうるのは、一般のネットワークセキュリティの問題と同様である。

現実には、犯罪組織が、サービス妨害攻撃を行うと脅迫を行い、金銭的な利益を要求する（恐喝）という例が増えてきている。DDoS 攻撃については「現在、一般の企業のサーバに対する DDoS 攻撃が、日常的に発生するようになっています」と評価されている[58]。このようなネットワークセキュリティの現状に対するリスクも検討しなければならないことになるだろう。

また、「導入・実装ガイドブック編」で詳述しているが、クラウド事業者の健全性は、重要な問題になる。クラウド事業者が、経営破綻をしたり、また、法的に問題のある行為で、捜索・差押を受けたりした場合には、そこからサービスを受けている業者は、重大な損害を被ることなる。アメリカにおいて、２００９年３月および４月に FBI がテキサスのデータセンター(Crydon Technology と Core IP Networks)に対して捜索・押収をなした際に、そのサーバー・ルーターなどの機材を押収し、そのデータセンターを利用していた利用者にも損害が発生したという事件があった[59]。この事件は、 クラウド事業者の健全性の観点から捉えるほうが望ましい事例のようにおもわれる。ある報道[60]によると、FBI の捜査官は、データセンターのオーナーの関係者が書類を偽造して、大手の通信業者から、接続サービスを購入していたという証拠を把握しており、共謀があったことを信じるに付いての相当な理由があったとしていたとのことである。これに対して、データセンターのオーナーは、偽造等の刑事事件が存在していたことを否定している。米国においては、ハードウエア自体が禁制品、犯罪の証拠、手段または果実で

---

[58]株式会社インターネットイニシアティブ「Internet Infrastructure Review」（Vol.8 August 2010）6 頁 http://www.iij.ad.jp/development/iir/pdf/iir_vol01_infra.pdf

[59] なお、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 31 頁

[60] “FBI Defends Disruptive Raids on Texas Data Centers” (http://www.wired.com/threatlevel/2009/04/data-centers-ra/)

あるとき、そのハードウエア自体を押収することは法的に可能である[61]。また、犯罪者に対して証拠湮滅をする余裕を与えないようにノックなしの令状を裁判官が発行することができる仕組みが発達している(Richards v. Wisconsin, 520 U.S.385 (1997))[62]。司法省マニュアルにおいては、「技術的には、捜査官は、ネットワーク全体の押収のための令状の発付を受けることも可能であろう。しかしながら、ネットワーク全体を運び去ることにより、PPA（42U.S.C.§2000aa）およびECPA（18U.S.C.§§ 2701-11）に基づく民事訴訟が国に対して提起される可能性があるのみならず、合法かつ営業中の事業を停止させ、非常に多くの人々の生活に支障をきたす可能性もある。」と記載されており、このような場合に対する慎重な配慮をなした捜索の計画を推奨しているが、この事件に関しては、捜査側において、配慮不足であったという可能性があろう。

（３）仮想化技術から発生する問題点

一般的なネットワークセキュリティの問題以外に、クラウド独自のものとして仮想化技術を採用することによって発生する技術的な問題点がある。これについては、（１）仮想化自体が、サイドチャネル攻撃の危険を引き起こす可能性がある（２）仮想マシンモニタを乗っ取られると被害が甚大である（３）仮想マシン自体の脆弱性をついた攻撃が可能である（４）物理的なエラーが攻撃のきっかけとなりうる（５）キャッシュ共有・メモリの覗き見等の攻撃が可能である、などの技術的な問題点が議論されている。これらの技術的な問題点の深刻さ・評価・対応について検討するのは、本解説の範囲を越えることになる。

また、前述のテキサスの例のような法執行機関による押収の場合において、各利用者のみが犯罪に関連していた場合に、その利用者毎の独立性が技術的に確立していない場合には、他の利用者のデータについて、機密性が損なわれる可能性があるということが

---

[61]米国司法省「Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations」(翻訳は、「犯罪捜査におけるコンピュータ捜索・差押および電子的証拠の獲得」(平成15年度社会安全研究財団委託調査研究報告書))(以下、司法省マニュアルという)の「II　令状によるコンピュータの捜索・押収」「C　令状と宣誓供述書を作成すること」ステップ1参照。

[62] 詳しくは、司法省マニュアル「II　令状によるコンピュータの捜索・押収」の「B 捜索を計画すること 5 ノー・ノック令状」を参照のこと。

いえる。仮想化されている記録とそれに対する法執行の方法などについては、今後も議論が必要となるものと思われる。

（４）フォレンジック的な観点からの問題点

本章の 1.2.「責任と説明義務について」でふれたように、企業において、すべてのデータが適切に保全、記録されており、問題となった行為についての真実がこのようなものであったということを明確にして、政府関係機関等からの被傭者の証拠隠滅が、経営層によって指示されていたとか、見過ごされていたという主張に反論することができるようでなければならない。しかしながら、現在の仮想化技術のレベルにおいては、データの記録について、そのような要求をみたすことができるかは、不明であるといわれる。そうだとすると、むしろ、実際のシステムを構築するのにあたり、上述のような要請を満たしうるように留意することが必要となる。

2.4. その他の法律問題について

（１）利用規約および濫用について

クラウドサービスを利用するのにあたっては、その利用規約を遵守しなければならない。例えば、Amazon であれば、Amazon Web Services Customer Agreement[63] があり、これを遵守しなければならないことになる。そこでは、利用者が、クラウドサービスを使って Spam をなすことやネットワークセキュリティを脅かすような行為をなすこと禁止している。また、ポートスキャン行為、過剰な Web クロール行為、オープンプロキシーなどの禁止があげられている。これらの行為の疑いがある場合には、即時に利用が停止される場合がある（同 3.4. Termination or Suspension by Us for Cause 参照）。全般的に提供している事業者側の権限が広く認められており、これらの行為があると認められた場合には、サービスの利用を停止されることになる。

また、これと関連してクラウドサービスのいわば同居テナントが、スパム送信などの不正行為をなしていた場合には、そのサービスを利用している者すべてがフィルタリング等される可能性があるということも留意しておく必要がある。

---

[63] http://aws.amazon.com/agreement/

（２）不正競争防止法の問題

また、クラウドサービスのセキュリティリスクの観点から、不正競争防止法２条６項に定める「営業秘密」が、クラウドサービスによって記録されている場合には、もはや「秘密性」を失うのではないかという議論[64]がある。

３　国際的な法律の適用関係によって発生する問題について

3.1.　国際的な法律関係の適用に関する一般理論

（１）基本的なアプローチ

これまで、一国のなかで、利用者・クラウド事業者がデータの処理を完結させる場合を念頭に議論してきた。しかしながら、むしろ、データが各国に記録される可能性があり、また、鍵管理についても種々のアプーチがある以上、きわめて法律関係の適用が複雑になる可能性がある。

この問題については（１）どこの誰が（どの国の裁判所か、行政機関か）（２）どのような法律問題を、検討しているのかということによって、左右されることになる[65]。この法律の適用を考える際によくいわれる言葉が「ジュリスディクション－裁判管轄」という用語である。法律家は、この言葉を聞くときに、一国の裁判所が裁判権を行使しうるかという国際裁判管轄を意識するが、実際は、それ以外にも一定の問題がジュリスディクションの概念の下で論じられている。

---

64 夏井高人「クラウドコンピューティングサービスと営業秘密の保護」（情報ネットワーク・ローレビュー第９巻１号　93 頁）

65　この点について「電子商取引及び情報財取引等に関する準則　改訂案」（平成 22 年８月）は、我が国での考え方を述べたあとに、これは「当該紛争について我が国の裁判所に訴えが提起された場合についての我が国の立場からの判断であることに注意する必要がある。すなわち、当該紛争について外国の裁判所に訴えが提起された場合には、当該外国の法に従って、国際裁判管轄が認められるかどうかや、どの国の民法や商法が適用されるかについて判断されるのであり、その結論が我が国のそれとは異なる可能性もあるのである。」と論じている（同 10 頁）。

一国の機関が、法的な力を及ぼしうるかどうかという管轄[66]の問題に関して、一般原則のもと権限を及ぼしうると認められる場合（国際私法により外国の法律を適用する場合もある）でも、種々の制約により外国法の適用をなしえない場合[67]がある。これは、利用者からすると、自国の法律が適用されないことになるので、実際に適用する国における法適用の考え方と関連しあって複雑な問題を惹起する。

（２）主体による問題

前述のようにどこの誰が、という点が法律の適用について大きな意味をもつというのは、法律の適用についての原則が国によって異なっているということ[68]、また、執行権限を行使する場合においては、その行使は、領域の範囲内でしか行えないということによる。

---

66 「原告は、裁判所の助けを借りることができるか」「裁判所の権限が被告に及ぶか」「裁判所は、事案を決定する力があるのか（裁判所は、権限を行使しなければならないのか、拒絶することができるのか）」という点が管轄の概念のもとに議論される。これらの点について John　O'Brien"Smith's Conflict of Laws"(Cavendish,1999)175 頁。

67 制約としてあげられるものは、以下の四つの観点からに整理されるであろう（John O'Brien　前出152頁以下、P.M.NorthJ.J.Fawcett"　Cheshire and North's Private International Law"(Butterworths,1992) 252頁以下）。
その1つは、その法律の性質上、内国において外国法の適用がなされないものである。これは、詳細にわけると、具体的には、歳入法(revenue laws)、刑事法(penal laws)その他のパブリックロー(other public laws－輸出入規制、敵国への貿易規制、価格規制法制、反トラスト規制など)、公共収用法(foreign expropriation laws)、公序に反する規定(contrary to public policy)がある。
2つめは、救済手段の種類からする制約である。この点については、婚姻関係に影響を与える救済を与える権限の制限があるとされている。
3つめは、当事者に対するジュリスディクションの制限である。具体的には、主権および主権国家、大使その他の外交官などが例にあげられている。
4つめは、適用しようという法律自体が、外国における行為に対して、適用を拒否している場合である。この具体例としては、特に国際条約などにおいて、特定の場合において裁判所の管轄を否定する場合などの例が挙げられている。

68「国境を越える電子商取引の法的問題に関する検討会　報告書」（平成２２年９月）http://www.meti.go.jp/policy/it_policy/ec/crossborderec_houkokusho.pdf は、通常の電子商取引の法律問題についてであるが、「日本の裁判所に訴えを提起した場合の裁判管轄権と準拠法」と「外国の裁判所に訴えを提起した場合の裁判管轄権と準拠法」とにわけて考察したきわめて参考になる資料である。

特に米国においては、いわゆる低触法革命[69]の後に、適用結果において、適切な結論を正当化しうるかという観点のもとに、自国法の適用の傾向が強まっていること、効果が、米国における法益に影響を及ぼす場合については、法律の一般的な適用か肯定されやすいことなどの特徴がある。

（３）法律問題の性質

法律問題の性質といっているのは、適用される法律が、刑事法であるのか、民事法であるのか、行政に関する法律なのか、また、適用されるべき効果が執行的な性質、もしくは、上述のパブリックロー的な性質をもつものかという点に左右されるということである。また、それぞれの手続法においては、それぞれの手続法の仕組みが適用されることになる。

刑事法であれば、一般的な規制は、属地主義である。しかしながら、その一方で、各法律は、保護主義などの根拠に基づいて、その適用範囲をさだめることができる。行為者の行為地、データの所在地などが、どれだけの意味をもっているのか、それらは、その刑事法の解釈の問題ということになる。

民事法であれば、契約当事者間の関係は、契約における準拠法の定めによってきまってくる。しかしながら、そうであったとしても、公序に関する部分については、各国の公序に関する法律が関与してくる。例えば、消費者保護に関する規定が属地的な観点から、適用されることは、世界的にみて一般的である。

行政に関する法律については、それ自体が、国家のもつ執行力に密接に関連するものが多いので、厳格に属地的なものとなることが多いだろう。逆に、その見地から、行政調査などによる事実発見、法執行の要請から、むしろ、データ自体が領域のなかに記録されていなければならない（輸出禁止）ということを要請することもある。

そして、それぞれにおいて手続的な要素がからんでくる。刑事手続の観点からは、法執行機関が、その国の法律に基づいて、データにアクセスしうる場合は、そのデータの所在地が重要な意味をもつ。また、この理は、民事訴訟においても同様である。

（４）留意すべき事項

これらの分析を前提に、クラウドコンピューティングを前提に、国際的な事柄が関与し、法律の適用関係が問題となる場合について、留意すべき事項としてまとめると以下のようにもまとめることができるであろう。

69　1960 年代中旬以降のアメリカにおける抵触法に関する考え方で、従来の実質法的価値と抵触法的価値とを峻別していたアプローチ（「くらやみへの跳躍」）を否定し、よりよい法を適用するという考え方をもとに適用する法律を決める考え方をいう。詳細については、石黒一憲「国際私法」（新世社、1993）62 頁。

（１）民事上の問題についても、適用される法律を決定するのは、きわめて種々の問題が存在する。

（２）データの所在がきわめて重要な意味をもち、データが外国でアクセスしうる場合に、そのアクセスしうる国の法律の適用をうける場合がある。

（３）主権国家は、その主権の行使として、パブリックローにもとづいてデータを域外に移転することを禁止することができる。

（4）データを管理する主体が国外に存在するとき、法的な要求を執行するのは、きわめて困難になる。

これらの項目について、現実に問題となりうる事項を解説するものとする。

3.2. 民事問題における複雑性

（１）契約法の準拠法と属地性

例えば、我が国において、契約の成立や効力が議論されている場合においては、当事者が契約締結時において、適用地を選択した場合には、当該土地の法律が準拠法とされる（法の適用に関する通則法－以下、法適用通則法という－７条）。これに対し、準拠法の選択がない場合には、法律行為の当時において、法律行為の成立および効力は、法律行為に最も密接な関係がある地の法によることとなる（同法８条１項）。この密接関連性に関しては、同法同条２項において、法律行為において特徴的な給付を当事者の一方のみが行うものであるときは、給付を行う当事者の常居所地法を最も密接な関係がある地の法と推定するとの定めがあり、クラウドコンピューティングにおける特徴的な給付は、主にベンダーが行うものであるから、これによれば、外国のベンダーとユーザーとの間での契約においては、ベンダーの常居所地法が適用される可能性が高いこととなる。しかしながら、更に、ユーザーが消費者であった場合、同法１１条２項から５項の規定により、消費者の常居所地法が適用されることが多いであろう。

このような説明は、我が国において、契約の成立や効力が議論されている場合の処理ということになる。しかしながら、契約をめぐって紛争が起きた場合に、我が国のような国際私法に関するアプローチがすべての国で同一であるという保障はない。実際には、ベンダーの常居所地法が適用され、また、執行等の関連から、ベンダーの常居所を管轄する裁判所において裁判がおこなわれるものと考えられるが、理論的には、紛争の解決が図られる裁判所と、適用される法は、全く別の問題ということになる。

（２）不法行為の準拠法

議論を具体的にするために、情報主体（日本在住）のデータを処理していた利用者（日本企業）から、委託をうけていたクラウド事業者が、その脆弱性対応を怠り、流出させたという場合を例としてみよう。このクラウド事業者が、外国に存在していたとする。情報主体が、クラウド事業者[70]に対して、プライバシー侵害を根拠に損害賠償を求めうるかということである。

我が国における議論されている場合においては、例えば、不法行為に基づく損害賠償請求を行う場合、加害行為の結果が発生した地の法によることが原則であり（同法１７条）、ユーザーがベンダーに対して請求する場合、通常結果が生ずるのは、ユーザーの居住地であることが多いであろうから、同所の法律が適用されることが原則となる。もっとも、法適用通則法は、生産物責任の特例（同法１８条）や名誉または信用の毀損の特例（同法１９条）を定めており、そのような特例の適用があるかも問題になる。上記の具体例については、プライバシーが問題となっているので、その不法行為の問題であるとの法的性質をもとに考え、プライバシーについては、同法１７条の適用により[71]、結果発生地ということになる。この場合、「直接に侵害された権利が侵害発生時に所在した地」の解釈ということになる。情報主体の居住地になるのか、情報の所在地なのかということになる。もし、情報の所在地が結果発生地であったとすると、例えば、米国において、そのような情報漏えいは、「違法」と考えられるのか、損害賠償義務を発生させるほどの違法とはいえないのではないかという議論が発生してくることになる。

我が国における議論をとっただけでも、上述のような論点を検討しなければならないことになるが、もし、執行の観点から、クラウド事業者の常居所の裁判所で判断を求めた場合はどうか。例えば、米国の裁判所で、クラウド事業者に対して損害賠償をもとめたらどうなるのか。情報漏えいに関する米国の法理の適用がなされる可能性も強いように思える。法律関係の適用に関する一般論で、どこの誰が判断するかという主体が影響を与えるといっているのは、そのようなことである。

また、プライバシーの問題を考えたか、もし、その漏洩したのが、営業秘密であったとすればどうか。知的財産権については、保護国法を準拠法として考えるべ

---

70 事業者に対する損害賠償請求の問題もあるが、ここでは、上記問題に限ることにしよう。

71同法１９条の適用により、被害者の常居所地法とも考えられるが、一般的な立場とはいえない。小出邦夫「逐条解説　法の適用に関する通則法」（商事法務、2009）224 頁参照。

きではないかという議論が一般的であるが、その保護国法の解釈じたいが我が国では明確とまでは評価しがたい状況である[72]。また、国境をまたいだ不法行為による損害の範囲についての海外における議論[73]も非常に難しい問題がある。

このように民事一般の範囲内で考えたとしても、法律問題の性質が、適用法に強く影響を与えるのである。

3.3. アクセス権限と属地性

クラウドサービスの利用者とクラウド事業者が、意図すると意図しないとにかかわらず、保存データに対して、アクセスが法的に認められることがあり、そのような適法なアクセス（Lawful Access）は、場合によっては、利用者にとっては、想定外のリスクとなりうる。特定の法域において保護されるべきデータといえども、別の法域においては、その法域の法に従うことからする問題がおこりうる。

この観点から、問題として論じられるのは、法執行の要請からする適法なアクセスと民事訴訟におけるｅーディスカバリである。

（１）法の執行の要請からする適法なアクセスについて

我が国においては、クラウド事業者などの第三者が、データについての事実上の管理権限を有している場合に、その第三者が任意で法執行機関にそのデータを開示することは原則としてなく、法執行機関としては、捜索・差押令状による場合でないと、そのデータを取得することができないと一般的にいわれている。これは、クラウド事業者にデータが保存されている場合、当該データは、通信の秘密に該当するからである。電気通信事業法４条は、「電気通信事業者の取扱中に係る通信の秘密は、侵してはならない。」と定めている。また、電気通信事業に関与する会社も、内規でもって、個別の通信に関

---

72 この点について前出　小出、230 頁。

73 この点については、Shevill v. Presse Alliance 事件（英国やその他のヨーロッパの国においては、限定された講読部数しかない France-soir 誌による名誉棄損について英国で訴訟が提起された事件）が、出版社の所在地で請求する場合と、被害者の住所地で請求する場合で損害額の違いを認めている。（鈴木淳司・高橋郁夫「法と規則の国際的側面」(インターネット弁護士協議会編＋村井純『インターネット法学案内--電脳フロンティア の道しるべ』所収)）（日本評論社、1998）135 頁

する内容、通信データ、および外延データは、裁判所の令状がない限り開示しないこととしている。しかしながら、通信に関するプライバシーを重視するこのようなアプローチは、他の国においても当然に採用されているわけではなく、日本的な感覚が当然と考えていると、法執行の見地からする適法なアクセス自体が、きわめて、データセキュリティに対する重大なリスクであると認識される。

一方、例えば、米国においては、「通信の秘密」という概念は、特に定められておらず、むしろ、「プライバシーの合理的な期待」という表現のもとに「通信の秘密」に対応する法的利益の擁護が図られている。そして、この「プライバシーの合理的な期待」という概念をメルクマールにして、「自発的開示」か「強制的開示」かといういわば法執行機関と情報とのかかわりという観点と「通信に関する情報の格付け」という観点から、プライバシーと法執行の利益のバランスの議論[74]がなされている。これらの具体的な状況については、前出の司法省マニュアルおよび「アメリカにおけるハイテク犯罪に対する捜査手段の法的側面」報告書[75]を参照されたい。

---

[74] アメリカにおけるプライバシーと法執行のバランスの議論については、高橋郁夫「通信の秘密」対「プライバシーの合理的期待」-米国司法省捜索差押マニュアルの示唆-（サイバー犯罪刑事手続調査委員会「アメリカにおけるハイテク犯罪に対する捜査手段の法的側面」報告書　52 頁　所収）
http://www.syaanken.or.jp/02_goannai/08_cyber/cyber1603_01/pdf/1603_01all.pdf
我が国に於ける通信のプライバシーの絶対化が弊害を生んでいるのではないか、米国の捜査方法や法律の規定が、サイバー犯罪に対するきめ細かな対応を可能にしているのではないかというのが筆者（高橋）の見解である。

[75]なお、我が国では、愛国者法（(“Uniting and　Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct　Terrorism (USA PATRIOT ACT) Act of 2001”）によって、あたかも、通信のデータ内容に対する無令状のアクセスが可能になったかのように報告されることがある。たしかに、大統領命令に基づいて、令状なしに通信の傍受がなされたことが米国で社会問題化したことはあるが、これは、電気通信プライバシー法（愛国者法による改正部分）の問題ではない。なお、愛国者法における改正部分については、「アメリカにおけるハイテク犯罪に対する捜査手段の法的側面」報告書　13 頁を参照のこと。

もし法執行機関に対する信頼がおけない場合には、法執行機関が、このようにデータに対してなす適法なアクセス[76]が、リスクとなりうるということになる。

（２）　ｅーディスカバリ

データが国境を越え、例えば、米国で保管されている場合に、米国のｅーディスカバリ[77]の適用があるとなされる場合には、我が国の利用者は、米国における民事訴訟法上のディスカバリ[78]に関する制裁規定の適用をうける可能性があるというリスクを検討しておかなければならないことになる。

米国においては、民事訴訟の当事者間において、原則として相手方の証拠の提出を受けることができ、しかも、訴訟状態になった段階から、当事者は、証拠を変更してはいけない義務を負うものと考えられている[79]。現在では、（１）e-discovery を通常の開示手続のなかに位置づけ、特にプレトリアル会議での実務を定める（同規則 34 条(a)、34 条(b) 、26 条(a) 、同（f）など)（２）e-discovery に関する特別の争点について一定の方向性をしめそうとする（26 条(ｂ)(2)、同条(ｂ)(5) 、37 条(f)など）などの観点か

---

[76]本文では、米国の例を挙げたが、英国においては、　2000 年捜査権限規制法（Regulation of Investigatory Powers Act 2000 ）(RIPA という）の２章（Chapter ２）となる。この２章は、このような「通信の内容」と「通信データ（communications data）」にわけて、通信データについては、法執行機関の判断のみで、電気通信事業者に対して開示を求めうるとしている。

[77] また、Electronic Evidence Discovery とか、Electronic Data Discovery などといわれることがある。

[78]　藤村 明子 (著), 金子 宏直 (著), 橋本 豪 (著), 西山 俊彦 (著), 松前 恵輪 (著), 須川 賢洋 (著), デジタル・フォレンジック研究会 (監修), 町村 泰貴 (編集), 小向 太郎 (編集) 「実践的ｅディスカバリ―米国民事訴訟に備える」 （エヌティティ出版, 2010）など

[79]電子証拠についての適用については争いがあったが、現在では、書類は、電子証拠の形態で存在するのであり、電子証拠の開示は、標準で、ルーチンなものと認識されると裁判所が述べるようになっている

ら連邦民事訴訟規則が改正されている[80]。実際に紛争が発生した段階で、紛争当事者は、（１）「訴訟ホールド」（開示に関する文書の保全義務の発生[81]）（２） 「会議」（開示を求める範囲や検索するためのキーワードについての合意(e-Discovery プロトコルともよばれる)(３)「概要的質問書の送付」(４)「供述書取得」(同規則 30 条(B)(6))。(５)「適正な開示」(同規則 34 条)などの手順を経ることになる。もし、適正な開示がなされていない場合には、当事者は、かかる開示の強制の申立や制裁の申立（簡易判決やコスト負担命令）をすることができる。

この場合、日本における利用者が、このｅーディスカバリの適用を受ける可能性は、データの所在地および鍵管理の主体の所在地によることになる。外国企業が、広汎なディスカバリの適用を受けた場合に問題点が発生するのではないか、という点についてアメリカの文書持参召還令状と守秘義務との相剋が問題となったマーク・リッチ事件は示唆に富むということができるであろう[82]。

3.4.主権からするデータ域外移転禁止

（１）EU データ保護規定との関係で

EU のデータ保護指令 25 条は、個人データは、データ主体の権利および自由についての「適切な」保護のレベルを確保していない限りは、そのような国家または領域に対する個人データの移転を許容しないとしている。この指令を実装している各国法におい

80　詳細については、橋本豪「アメリカ連邦民事訴訟規則のもとでのｅディスカバリ」（前出・注 54　「実践的ｅディスカバリ―米国民事訴訟に備える」所収）58 頁参照のこと

81 コンピュータ文書については、現状を維持することじたい（上書き保存の場合など）でも文書の破壊が発生するのである。そして、たいていの企業は、バックアップ手続を採用しており、そのテープに対しても保全義務の対象となるのである。

82 この事件は、スイスに本拠を置きスイス法を設立準拠法とするマーク・リッチ社に対して米国から文書持参召還令状が提出されたのを契機に、スイスの行政当局が、当該文書を、事業上の秘密保持義務に違反するおそれがあるとして没収した事件。詳しくは、石黒一憲「現代国際私法(上)」（東京大学出版会、1986）205 頁を参照のこと。

て、この規定を前提とする定めがある[83]。ここにおいて「移転」は、域外にデータを開示すること、もしくは、域外においてデータに含まれる情報を利用可能にすることをいうものと考えられる。この原則のポイントは、移転先に対して、個人データの「適切なレベル」の保護を要求するものである。この「適切なレベル」かどうかについては、「共同体の認識」に従って決定されることがあることが述べられており、また、個人データの性質、データに含まれる情報の原産国、その情報の目的国、処理の目的、その機関、問題の国ないし地域の実効性を持つ法、その国ないし地域の国際的な義務、関連する強制力を有する行動規範、ルール、データに関するセキュリティ手段などから、判断される。　そして、日本の個人情報保護法制では、EU 保護指令 25 条によるデータ保護水準が十分であるとは認められておらず[84]、EU から日本へのデータ移転は、EU 保護指令上未だ認められていない状況にある。そこで、日本から EU にデータを移転することはできても、EU から日本にデータを移転することが出来ない状況となっている[85]。

日本において生成されたデータについて考えるとき、日本から、データの国外移転に関する規定が存在しない。だからといって、個人データ取扱に関する法整備が進んでいない国にデータが移転することを軽視してよいことにはならない。個人データの漏洩、不正利用、抹消、改ざんなどの問題が生じても対策の執りようのない状況に置かれ、あ

---

[83]例えば、英国データ保護法　第１表、第１部、８文において、第８原則として「国ないし地域において個人データの処理に関連してデータ主体の権利および自由についての適切なレベルの保護が確保されないかぎり、個人データは、ヨーロッパ経済圏外に、移転されない」と定められている。「クロスボーダー」という用語の問題としては、特に、クロスボーダーでデータ収集を行っている会社が問題になる。ＥＥＡ域内において、本店を有している会社においては、その本店を有している国の法に服するのみであるが、域外に本店を有し、英国内において設備を用いてデータ処理を行っている場合は、英国法に従うと解されている。

[84] EU により、十分であると認められているのは、アルゼンチン、オーストラリア、カナダ、スイス、フェロー諸島、ガンジー島、マン島、ジャージー島である。また、米国については、セーフハーバー・旅客名称記録についても、同様の取扱がなされる。
http://ec.europa.eu/justice/policies/privacy/thridcountries/index_en.htm

[85] この点については、総務省　「スマート・クラウド研究会（第６回）議事要旨」４頁（http://www.soumu.go.jp/main_content/000077709.pdf）に詳しい。

るいは否応もなく他国の法制度に服さなければならなくなる危険にさらされるのである。

（２）行政権の行使の要請からする域外移転禁止

上述のデータ保護規定の関係とも関連するが、一定の行政庁の監督が望ましい分野については、データ自体の域外移転禁止を求めるということも合理的なものと思慮される。この代表的な例として、医療情報が、ASP・SaaS 事業者に委託されて保存される場合[86]については、データ自体が国内に保存されていることが求められることをあげることができる。

総務省「ASP・SaaS 事業者が医療情報を取り扱う際の安全管理に関するガイドライン」[87]においては、「所管官庁に対して法令に基づく資料を円滑に提出できるよう、ASP・SaaS サービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ等は国内法の適用が及ぶ場所に設置すること。」とされている（同　表 3-８ 災害等の非常時の対応における ASP・SaaS 事業者への要求事項　参照）[88]。

---

[86] 厚生労働省医政局長通知「医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン」が定めている点に関して、情報システムによる処理との関係では、「医療情報システムの安全管理に関するガイドライン　第 4.1 版（平成２２年２月）」が定めている。医療情報ネットワーク基盤検討会において、診療録等の保存を行う場所について、各ガイドラインの要求事項の遵守を前提として「「民間事業者等との契約に基づいて確保した安全な場所」へと改定すべき」とする提言が取りまとめられ、なお、その後、厚生労働省通知「診療録等の保存を行う場所について」 によって、外部保存が拡大されていたことを受けて、関連する部分が改定されている。
http://www.mhlw.go.jp/shingi/2010/02/dl/s0202-4a.pdf

[87] http://www.soumu.go.jp/main_content/000030806.pdf

[88] 「医療情報システムの安全管理に関するガイドライン　第 4.1 版（平成２２年２月）」においても、上記ガイドラインが前提条件であるとされているので、データが国内に存在することはなおも要求されていることになる。

（３）国家安全保障による輸出禁止

また、それ自体がセンシティブなものでないとしても、国家安全に関わる重要な価値を有する情報を域外において保存することはそれ自体、微妙な問題を惹起するのではないかと考えられる。

このような観点から検討が必要なのは、外国為替及び外国貿易法（外為法）による役務取引についての規制の存在である（同法第２５条）。「国際的な平和及び安全の維持を妨げることとなると認められる」貨物や技術[89]については、大臣の許可を受けなければならない（同法２５条１項）など役務取引等が規制されている[90]（輸出貿易管理令別表第一・九（七）（八））。同法２５条は、さらに、「第一項の規定の確実な実施を図るため必要があると認めるとき」について、「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（略）による特定技術を内容とする情報の送信」についても大臣の許可を受ける義務を課される場合があるとさだめている（同３項）。その限りで、いわゆる規制を課せられる可能性があるということになる。

また、ネットワークについて、現在、サイバーエスピオナージ(ネットワーク上でなされる経済スパイ活動である)が大きな問題として注目を浴びている。このような観点から、外国において、どの程度、重要なデータを保存しうるのかという点については、慎重な対応が望ましいということがいえる。

3.5.国外に対する法執行等の困難性

また、法律の適用がなされうる、といってみても、現実に、どのような法執行がなされるのかということが重要なポイントであり、国境をまたぐことで、法執行がきわめて困難になってくるのである。この国際的な事件における法執行の困難さを考える具体例として、Wiki Leaks 事件を取り上げてみよう。

WikiLeaks というのは、政府や、企業、宗教に関わる機密情報を公開するウェブサイトで、投稿者の匿名を維持する仕組みを採用している。このウエブサイトの管理人であ

---

[89]輸出貿易管理令により「暗号装置又はその部分品」「情報を伝達する信号の漏えいを防止するように設計した装置又はその部分品」とされている。

[90] 罰則については、同法６９条の６参照。

るジュリアン・アサンジ(Julian Paul Assange)は、アイスランドに家を借りているものの、実際の住所としては、不定に近いようである。この WikiLeaks というサイトに、2010 年 7 月 25 日、アフガニスタン紛争に関するアメリカ軍や情報機関の機密資料約 75000 点以上が公表された。これは 2004 年から 2009 年にかけての記録で、「秘密」格付けのなされている記録であった。具体的には、パキスタンの情報機関「ISI」とアフガン武装勢力との関係や、未公表の民間人死傷案件、アフガン側のアメリカへの情報提供者の身元情報が含まれていた。WikiLeaks は、スウェーデンを根拠とする PRQ といホスティング会社のサービスを利用しているが、中央サーバは、スウェーデンにあるものの、サーバ自体は世界に広がっている。また、スウェーデンにおいては、法的な保護も強いとのことである。アメリカ法においては、上記の情報を公開することは、合衆国法典 37 章 798 条に違反することになる。この刑事罰との関係で考えると、まず、WikiLeaks （もしくは、管理者のアサンジ)が、この法律に違反しているということができるのか、もし、その法律が、WikiLeaks に適用しうるとしても、どこの国に対して、具体的な犯罪人引き渡し等を求めうるのか、また、協力をもとめられた国の法律で違法とならない場合は、協力に応じるわけにはいかないのではないか、などの問題が山積である。また、民事的に情報の公開を差し止めようとすると、具体的な請求原因として何を保護すべきものとして差止を求めうるのか、どこの裁判所にもとめればいいのか、国家機密を根拠とする請求に対して、他の国の裁判所は、協力することがで きるのか[91]、実際に、具体的な執行をおこなえるのか[92]、などの問題を解決しないといけないことになる。

この WikiLeaks 事件は、漏えいした情報が、国家機密であることからする複雑な問題点をかかえているが、ここで示された問題点の多くは、企業秘密が漏えいした場合に、

91　この点で興味深いのは、イギリスの MI6 のメンバであった Peter　Wright の回想録である“Spycatcher”事件である。イギリスの法務総裁（AG）は、オーストラリアとニュージーランドで、“Spycatcher”の出版禁止をもとめる差止命令をコンフィデンス違反を根拠に求めたところ、両国ともに、その出版禁止の申立を認めなかった。その理由としては、オーストラリアでは、パブリックローの適用を求めるものであるからとしている。この点については、John　O'Brien　前出 159 頁以下。

92 例えば、ISP などに、上記の情報へのアクセス遮断を要請するということになるのかどうかということになる。

どのような対応をすべきかという場合にも当てはまるものであるということができよう。

４リスク対応策についての法的視点

4.1.　契約による対応について

クラウドサービスというイノベーションの採用にあたって、そのイノベーションに伴う問題点(リスク)については、法的手法によって、対応するということもひとつの重要な方法になる。この場合、契約条件が公平であるかが、特に情報の共有・解消の容易さの観点から、検討さることになる。特に、サービス条件については、一定の事項についてサービスレベルアグリーメント(SLA)を締結することが行われる。また、それ以外にも、契約書でもって定めておかなければならない事項が多く存在する[93]。それらの事項のそれぞれについては、「導入・実装ガイドブック編」でふれている。

4.2.　契約対応の法的限界について

クラウドコンピューティングのリスクとして、データ消失のリスクがある。オンプレミスでのデータ処理においても、この点については、SLAをもって、保証されることがある。もっとも、SLAについては、それによってデータの価値自体が保証されるというわけではない。

この点について参考になる判決例としては、東京地判平成２１年５月２０日がある。この事件は、被告（Ｙ）の共用サーバホスティングサービスを利用してサーバ事業を営む会社（Ａ）と契約してＷＥＢ上のサイトに係るプラグラムを運営していた原告ら（Ｘら）が、被告の管理するサーバの障害事故により、原告らのプログラム及びデータが消失したことにつき、被告は原告らのプログラム及びデータの消失を防止する義務を負うのに、これに違反し、また、損害拡大防止義務及び残存記録確認・回収義務を負うのに、これを怠ったもので不法行為に当たると主張して、不法行為に基づく損害賠償を求めた事案である。裁判所は、（１）Ｘらは、Ａと強要

---

[93] SLA についての一般的な検討事項として、経済産業省「SaaS 向け SLA ガイドライン」（http://www.meti.go.jp/press/20080121004/20080121004.html）がある。

サーバホスティングサービスの利用契約を締結しているだけで、Xとの間に契約関係や寄託契約的性質はない（2）Yが契約者との間で締結している責任制限規定や免責規定があり、これらの規定を越えて、Xに対して、原告らのプログラム等に対する消失防止義務というものは、考えられないなどの判断をしている。

この判決が示すように、契約当事者は誰かという点についても意識して、契約を締結することが重要であるし、また、データそれ自体については、クラウド事業者のもとで記録されていたデータが消失してしまったとしても、そのデータ自体の有していた価値についてクラウド事業者が責任を負うものではないことは、十分に認識しておく必要があるということがいえる。

4.3.法制度の違いから生じる限界について

本解説　3　「国際的な法律の適用関係によって発生する問題について」においてふれた事項については、各国の法制度が異なることが大きな影響を与えている。

しかしながら、各国の安全保障に対する考え方にもとづく相違から発生する問題は別として、より技術的な問題については、各国で標準的な手続をさだめ、それを相互認証することによって、国境を越えたデータの保存を実現可能にしようということが考えられてしかるべきことになる。この点で注目されるべきは、日本とアメリカにおいて、クラウドコンピューティング技術の普及を含む「インターネットエコノミーに関する幅広い政策課題について、日米両国政府間で意見交換を行い、両国のICT分野の発展に向けた認識の共有化と地球的規模での課題における具体的連携を推進する観点から、インターネットエコノミーに関する日米政策協力を行」うという動きがある[94]ことである。プライバシ・セキュリティ・行政調査の標準手順などにおいて、具体的な連携をなすことができれば、国境を越えての利用に一層のはずみがつくことに可能になるであろう。

94

日本においては、総務省が、「インターネットエコノミーに関する日米政策協力」（http://www.soumu.go.jp/menu_news/s-news/02tsushin06_02000027.html）と題して、また、米国においては、商務省がプレスリリース（http://www.state.gov/r/pa/prs/ps/2010/06/143357.htm）を出している。

第３　セキュリティガイダンス

上述の検討から、以下のセキュリティガイダンスをまとめとして、提示することができるであろう。

（１）「法律等を遵守する等の義務は、経営者の責務である」という認識が、クラウドの提供・利用において、根本的な認識である。

（２）「リスクについて十分な対応体制を整えるのみならず、経営者は、十分な配慮をなしたことを客観的に説明できるようにしなければ、ならない。」

（３）「クラウドサービスを利用している場合でも、法令等を遵守していることのみならず、客観的に、遵守していることを説明できるように準備していなければならない」

（４）「適用されるべき法律等を認識・理解することが重要であり、それらの法律については、個人情報保護、プライバシー、情報セキュリティに関する法律をはじめとして、もれなく、それらを遵守しなければならない」

（５）「クラウドの国際性から生じる国際的な法律の適用問題について十分に理解しなければならない。データ保護、e-ディスカバリ、法執行対応について十分な検討が必要である。 」

上記のセキュリティガイダンスは、本書の章ごとのタイトルをならべたときに一番重要となることをまとめてものとなる。これをもとに、クラウド・セキュリティ・ガイダンスの記述をみていくことで、本解説のまとめとしよう。適用される法律が異なるとしても、基本的な考え方は、全く同一なのである。

1　コンプライアンス義務の位置づけ

「法律等を遵守する等の義務は、経営者の責務である」という認識が、クラウドの提供・利用において、根本的な認識である。

組織は、また、クラウドの内であろうと外であろうと、こうした情報の正当性、セキュリティおよび機密性を保護する義務を等しく負っている。クラウドサービス事業者が保全するデータについても、それがオリジナルの所有者、あるいは管理者の手にあるときと同じような保護手段を受けなければならない(G49頁)。

法律等を遵守する等の義務は、経営者の当然の責務であること、クラウドの提供・利用においても、その義務が当然に適用されること、クラウドの提供・利用によって、もともと定めていた情報セキュリティ・プライバシーの保護レベルが下がっていいということにはならないことが重要である。

2 リスク管理体制の採用と説明責任

「リスクについて十分な対応体制を整えるのみならず、経営者は、十分な配慮をなしたことを客観的に説明できるようにしなければ、ならない。」

クラウドコンピューティングの手続きを行う前に、企業は、法的な障害やコンプライアンス要求事項を特定するために、提案されたクラウドコンピューティングサービスを利用した取引に関係する自社の行動規範、要求および制限事項について評価を行うべきである(G50頁)。

リスク管理体制を採用し、その上で、クラウドコンピューティングを導入すること、また、その体制のもとに適切にリスクの識別・評価がなされ、それに応じたリスクの対応策がとられるべきことは、重要である。この点については、本解説の「導入・実装ガイドブック編」において詳述されており、そちらも参照されたい。

3 業務執行における説明責任とクラウドサービス

「クラウドサービスを利用している場合でも、法令等を遵守していることのみならず、客観的に、遵守していることを説明できるように準備していなければならない」

クラウドサービス事業者が一方での当事者として民事訴訟に関与する場合、あるいは、政府当局によって、内部に対する調査が執行される場合、クラウドサービス事業者は、ホスティング事業体として保管する情報データへのアクセスを要請される(G58頁)。

現代社会において、説明責任がきわめて重要な役割を果たすときに、コンピュータで処理されているデータが、もれなく、改ざん等なくもれなく提供しうるというのは、ひとつの重要な要求ということになる点については意識が必要である。

4 適用法令等をめぐる議論について

「適用されるべき法律等を認識・理解することが重要であり、それらの法律については、個人情報保護、プライバシー、情報セキュリティに関する法律をはじめとして、もれなく、それらを遵守しなければならない

クラウドコンピューティングのサービス手続きを行うに際して、多くの法的制限事項が存在している。これらの制限事項は、連邦法あるいは州法とそれらに関連する規制に起因している。それらはまた、国際規格や先在する協約に由来するものもある。また、外国の法律、およびその他のソースから関係するものもある(G51頁)。

これらの多くの法的制限事項に対する認識が重要になってくる。

クラウドサービス事業者が倒産する場合も想定できるであろうし、争議が発生した場合、預かったデータを人質に取るかもしれない。データの物理的な場所は、データを統制する法律の選択に直接影響するため、企業にとっては、データが保管さ

れている国がどこであるかを理解することは重要である(G52頁)。

適用に関しては、データの場所が重要な役割を果たすことが多い。これが、主権の発露から正当化される点については、論じている(第２・３ 参照)。

企業は、その顧客や従業員に関するプライバシー情報の保護や、このようなデータが二次利用されないこと、また、第三者に対して開示を行わないという法的義務を有する(G53頁)。

企業は、自社の知的財産、その他の資産、および従業員や顧客、契約にかかわる個人情報を保護するため、常に妥当なセキュリティレベルを確保しておかなければならない。こうした義務は、数多くの法律、規制、国際規格、ケース、およびベストプラクティスに起因している(G56頁)。

適用される法的遵守事項に関して、個人情報保護、プライバシー、情報セキュリティに関する法律が、きわめて重要な役割を果たすことは、いうまでもないことである。そして、利用者は、クラウド事業者などについても適切なセキュリティ手段等を講じることを要求しなければならないと定められているのである。

5 クラウドサービスの国際性がもたらす法適用の問題

クラウドの国際性から生じる国際的な法律の適用問題について十分に理解しなければならない。データ保護、e-ディスカバリ、法執行対応について十分な検討が必要である。

クラウドサービスを活用したいグローバル企業は、その利用によって、アメリカ国内で適用されているよりも多く異なる制限事項を含む海外の法律の規制を受けることになり、自社の子会社や顧客、ビジネスパートナー、およびその他の関係者が不利益を被らないことを確保したいと望んでいる(G54 頁)。

クラウドサービス事業者は、戦略的にサーバー（自社サーバー、あるいは提携先）をどの国・地域に置くべきかを検討する必要がある。サーバーを置く場所の選択は、直接、司法が絡む問題と法の選択に関係する(G54 頁)

クライアント企業側では、情報データの機密性、秘匿性を保全することから、アクセス要求に対して抵抗する能力を高めたいと考えている(G58 頁)。

クラウドサービスの有する国際性からする具体的な問題点については、本解説の第 2・3 において詳述されている。そこでふれられたリスクについては、具体的な評価および対応策が検討されなければならない。