クラウドセキュリティガイドライン活用ガイドブック

２０１３年度版

経済産業省　商務情報政策局

情報セキュリティ政策室

目次

1. はじめに

クラウドサービスが提供され始めた当初から、クラウドサービスの利用に関する懸念事項として情報セキュリティが挙げられています。これは現在も変わらず利用者の最大の懸念事項ですが、積極的なクラウドサービスの利用によってリスクの実態も徐々に把握できるようになってきました。

ガイドライン活用ガイドを作成するにあたっては、実際に発生した事故について詳細を把握し、それを反映する必要があると考え、報道されているクラウド事業者における事故について調査しました。

クラウドコンピューティングの技術的な問題だけではなく、クラウドサービスにおける実際の事故・障害などのトラブルを調査したところ、事故・障害の多くはソフトウェアのバグや運用管理上のミスに起因していました。ソフトウェアのバグについては 2011 年の方が多く、現状ではクリティカルな問題は発生していないようですが、ソフトウェアやハードウェアがクラウドコンピューティング環境に対応するためには若干の時間を要したようです。

▶ 調査事例の発生年別内訳

発生年	件数
2011年	20
2012年	31
合計	51

▶ 調査事例の発生国・地域の内訳

国または地域	件数
米国	35
日本	12
韓国	2
カナダ	1
欧州	1
合計	51

▶ 調査事例の問題別内訳

問題の分類		件数
障害（悪意なし）	①ソフトウェア	12
	②ハードウェア	3
	③設計	3
	④運用・管理	9
	⑤ファシリティ	7
攻撃（悪意あり）	⑥サービス妨害	1
	⑦不正アクセス	9
	⑧その他	1
⑨非公開		6
合計		51

図 1 クラウドサービスにおいて発生したトラブル（報道された情報から集計）

この調査結果をもとに、国内外のクラウド事業者やクラウド事業者を取りまとめる団体などへのインタビュー調査を行ったところ、やはりクラウドサービスにおける事故・障害の多くは環境と運用に関するものでした。

- コンピューティング環境における事故・障害
  - 電源に起因するトラブル
  - ネットワークの障害

- ストレージの障害　など

- 運用上の事故・障害
  - 個人のスキルに依存した運用
  - 利用者によるミス　など

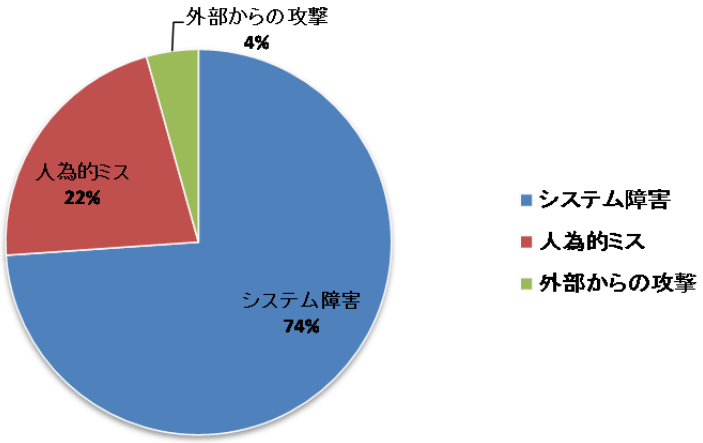

図 2 クラウド事業者へのインタビューによる事故・障害の実例（N=23）

クラウドサービスが提供され始めた当初に懸念されていた情報の流出や内部関係者による窃取、法的問題に関するトラブルなどは、クラウド環境に依存する問題としては現在のところ報告されておらず、インタビュー調査においても明確な事故として捉えていないとの結果が得られています。

内部不正や外部からの攻撃による情報漏えいなどの事故は、サービス提供時から懸念されていた事項であり、各事業者においても対策が検討されているということで事故に至っていないということや、クラウドサービスの運用管理が自動化されていることによって、人が介在しないために通常の運用では内部犯行などが起こりにくい環境にあるといったことも実情のようです。

一方で、クラウドサービスが本格的に利用され始めたばかりということもあり、経験則による対応が難しかったり、新たな技術への対応を求められる中で十分な技術教育や運用手順の標準化などが図られていないという課題もあるようです。

本ガイドラインでは、これらの実際に発生した事故や、事業者が抱える様々なセキュリティ上の課題をベースに、IT サービスとしてのクラウドサービスに関するリスクと対策を、事業者と利用者のそれぞれについて解説します。

また、経済産業省の提供する「クラウドサービス利用のための情報セキュリティマネジメントガイドライン（以下、クラウドセキュリティガイドライン）」の活用についても解説します。

2. クラウドセキュリティとは

2.1. クラウドの整理

クラウドサービスを取り巻く環境は広く変化しており、クラウド利用者とクラウド事業者の関係だけにとどまりません。本章ではクラウドサービスを取り巻く環境を整理することで、クラウドセキュリティの観点を明確にします。

2.1.1. クラウドサービスの構造とセキュリティ

クラウドセキュリティといった場合、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を指す場合と、クラウドサービスの利用に関するセキュリティを指す場合があります。これらは密接に関係していますが、分けて検討することで、様々な問題を整理することができ、具体的な対策を検討しやすくなります。

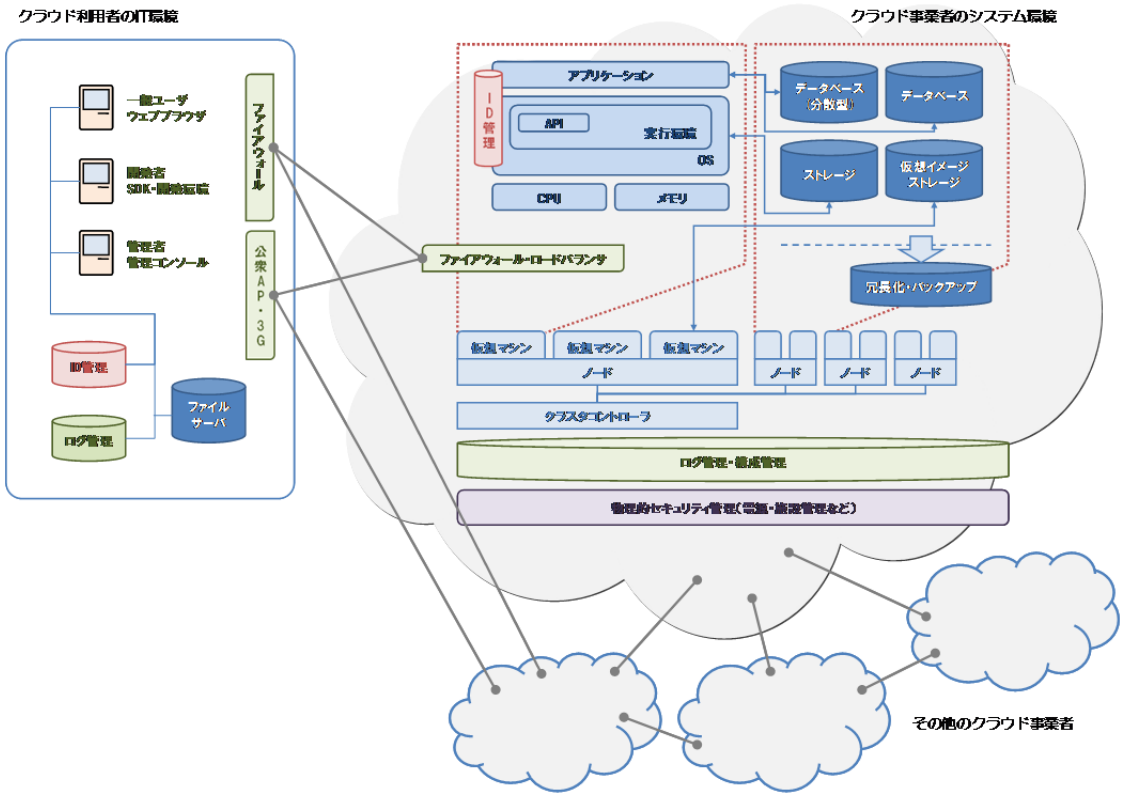

図 3 クラウドサービスを取り巻く環境

企業の中で自らがクラウドコンピューティング環境を構築し、それらを自社内で利用する場合（プライベートクラウド）、主にクラウドコンピューティングに関するセキュリティを検討します。クラウドコンピューティングの基盤となるネットワークや仮想化環境、分散処理などがこれにあたります。

事業者が提供するサービスを利用する場合（パブリッククラウド）は、技術的な問題を利用者が具体的に意識する必要はありません。技術的なリスクは事業者が検討し、対策されたサービスとして利用されることが前提とされるためです。しかしながら、これらのサービスが適切に提供されているかどうかを利用者は確認する必要があります。そのためのセキュリティ対策をクラウドサービス利用のセキュリティとして検討します。

2.1.2. クラウドコンピューティングの課題と対策

クラウドコンピューティングでは分散処理技術や仮想化を利用して、コンピュータ環境の重要な拡張を行うことができるようになっています。利用者が利用したいときに好きなだけコンピュータリソースを利用できるように十分なコンピュータ環境を用意しています。

クラウドコンピューティングの環境においては以下の技術的な要素についてリスクを検討する必要があります。

- 仮想化に関するリスク
- 分散処理に関するリスク

仮想化や分散処理は必ずしもすべてのクラウド事業者で採用されているわけではありませんが、ソフトェアに起因する事故を防止するという意味でも、これらに配慮する必要があります。

クラウドセキュリティガイドラインでは仮想化に関する対策について「7.1.1 資産目録」や「10.1.2 変更管理」などで触れていますが、これは管理上の対策であって技術上の問題ではありません。クラウドセキュリティガイドラインは情報セキュリティマネジメントのためのガイドラインとなっており、技術面についてはそれぞれの項目の「クラウドサービスの関連情報」という欄に記載しています。こちらを参照して、仮想化についてのリスク検討を行ってください。

2.1.3. インフラ上の課題と対策

クラウドコンピューティングでは多くのコンピュータがネットワークで接続され管理されています。さらに仮想化されたコンピュータもネットワークで接続されています。

クラウドコンピューティングのインフラにおいては以下の技術的な要素、物理的な要素についてリスクを検討する必要があります。

- データセンタ
- ネットワーク
- 仮想ネットワーク

クラウドサービスにおいてネットワークは重要な要素となります。ネットワークに関連した内容は「10.6 ネットワークセキュリティ管理」に記載されています。特に 10.6.2 にはネットワークサービスにおける留意点が記載されていますので、参照してください。

2.1.4. 運用上の課題と対策

クラウドコンピューティング環境を利用して提供されるサービスは継続運用される必要があります。IT サービスの継続管理においては以下の管理的な要素についてリスクを検討する必要があります。

- キャパシティ管理
- 変更管理
- バックアップ

クラウドにおけるキャパシティ管理は物理的なリソースだけではなく、論理的なリソースまで管理しなくてはいけません。また、マルチテナントで提供されるサービスであることを考えれば、ピーク時（例えば、クリスマスシーズンなどのオンラインショップの混雑など）の負荷分散なども重要な要素となります。

キャパシティ管理については「10.3.1 容量・能力の管理」に注意事項を記載しています。クラウドの特徴である「オンデマンドセルフサービス」を実現するためにどのような計画を行うのかなど、過去の経験を元に検討する必要があります。そのためにも変更管理や異常管理などの記録などを参照しながら対応する必要があるでしょう。

2.1.5. クラウドサービス利用におけるセキュリティ

クラウドコンピューティグを利用して提供されるサービスをクラウドサービスといいます。クラウドサービスを利用する際には、クラウドサービスがどのような環境で提供されているかを正しく理解し、脆弱性や脅威を把握した上で利用する必要があります。

また、クラウド事業者が行っているセキュリティ対策を把握し、利用上の残存リスクについて検討する必要があります。

クラウドサービスの利用によって外部に管理されている資産だけではなく、システムログなど、情報セキュリティマネジメントシステムの運用において必要な情報が入手しづらくなっていることにも目を向けて、セキュリティポリシの実施が可能か、目的を達成することができるかなどを再度検討することが必要です。

クラウドセキュリティガイドラインは、クラウド利用者のためのガイドラインとして公表されました。クラウドサービス利用における懸念事項がある場合は、関連する項目を参照し、情報セキュリティ対策に役立ててください。

2.2. クラウドセキュリティガバナンスとサプライチェーン

情報セキュリティマネジメントでは、自組織のことをトップダウンで考えるようなセキュリティ計画を実施してきました。これは組織の大きな目標に従ってそれぞれの構成員が努力することによって情報セキュリティのレベルを向上させるというものでした。

マネジメントに関わるすべての情報が即座に上がってくる環境では、トップマネジメントは有効ですが、組織が大きくなったり、小さな組織でも現場の多様性が出てくるようになると、トップダウンのマネジメントだけでは追いつかなくなります。

そこで生まれたのがセキュリティガバナンスです。

それぞれの現場に応じた形でマネジメントしているものを中央に集めて管理することで全体の整合などを取りつつ、現場単位での改善なども実施できるというものです。クラウドサービスのセキュリティにおいては、リソースや資産の一部を外部に置くということもあり、現場単位でのマネジメントを管理するという方法が適しているようです。

本章ではクラウドにおけるセキュリティガバナンスの考え方、そしてクラウド環境を構成するサプライチェーンについて解説し、クラウドセキュリティを検討する観点を明確にします。

2.2.1. クラウドセキュリティガバナンスとは

クラウド利用者は、クラウドサービスを利用することによって、情報の管理や処理をクラウド事業者に委ねてしまうため、サービス利用におけるリスクのすべてをコントロールできないといった問題が生じる可能性があります。これは単にデータがクラウド事業者に存在するということだけを指しているのではありません。マネジメントに必要なシステムログなどを入手しづらくなるといったことも、情報セキュリティマネジメントにおけるインシデントへの迅速な対応を阻害する要因となっています。

クラウド利用者は、クラウドサービス利用時の組織における IT サービスマネジメントや情報セキュリティマネジメントの確立、クラウド事業者とクラウド利用者の間における責任分界点など、クラウドサービスの利用を通じてのガバナンスの適応範囲を整理していく必要があります。

クラウドセキュリティガバナンスにおいては、情報セキュリティマネジメントを実施するにあたって資産がどこにあるのかを把握することから始めることが重要です。

情報資産というとどうしてもデータそのものや機器そのものについて考えてしまいがちですが、IT サービス管理ということでは ID 管理、ログ管理も重要な要素です。ユーザの行動に関するトレーサビリティの確保など、内部統制の要求事項などについても検討し、正しく把握できるようにしなければなりません。そのためにも、マネジメントに

必要な情報を整理し、それを適時に入手し、活用できるかどうかを予め検討しておくことで、クラウドセキュリティガバナンスを確立することができるでしょう。

項目	概要
クラウドサービスに関するコントロール	クラウド事業者は、クラウドサービスにおけるインシデント、サービスの復旧、サイト障害などについて、個社別に十分な対応をとることが困難
クラウドサービスのサービスレベル及びサービスの継続性	契約時と同等レベルでのサービスの継続性。具体的には、クラウド事業者の突然の倒産やサービスの中止、サービス品質の低下、契約更新時における容認できないレベルのサービス利用料の改定など
クラウドサービス上のデータのライフサイクル管理	クラウド事業者が提供するクラウドサービスで保管されるデータのコピー、復元、バックアップなどに関する基準やデータの移植性なども考慮したデータのライフサイクル管理に関するリスク
国外でのデータ保存・処理	クラウドサービスで提供されるデータが国外で保存・処理される場合に、国外の法制度が適用される際のカントリーリスク

図 4 クラウドセキュリティガバナンスの観点

また、クラウド事業者が提供するクラウドサービスの利用に伴い、IT サービスマネジメントや情報セキュリティマネジメントにおいて、内部管理の徹底、監査の共通化、情報セキュリティマネジメントの共通化・自動化、システムの二重化や災害復旧によるリスク低減などの効果が考えられます。

概要	項目
内部管理の徹底	クラウドサービスでは機密ではない情報の保存や処理を行い、自社のオンプレミス環境では機密情報の管理徹底を行うことで、情報漏えいリスクを低減
監査の共通化	クラウドサービス内に保存された情報を共通して監査することにより、オンプレミス環境で構築した情報システムの場合と比べて、個別監査の負担を軽減
情報セキュリティマネジメントの自動化	クラウド事業者が提供する不正アクセスの検知やウイルスの自動アップデートなどのサービスを利用することにより、セキュリティマネジメントを一元化・自動化し、情報セキュリティマネジメントの負荷を軽減
システムの二重化への対応	クラウド事業者がシステムの二重化やデータのバックアップ対応を行うことにより、クラウド利用者による個別システムの二重化やバックアップ対策の負荷を軽減

図 5 クラウドサービスにおけるガバナンスの効果

クラウドセキュリティガバナンスでは、すべてを利用者が実施する必要はありません。クラウドサービスを利用しているのですから、その特性を活かして、サービスとして利用できるものは利用するというスタンスも重要なポイントです。

2.2.2. クラウドにおけるサプライチェーンとは

クラウドサービスを取り巻く環境では、クラウド利用者とクラウド事業者が様々な関係でつながっており、複雑ではないものの全体像を把握することが難しくなっています。

例えば、クラウド事業者が、第三者が提供するクラウドサービスを利用して新たにサービスを提供している場合、このクラウド事業者はクラウド利用者でもあり、クラウド事業者でもあると考えることができます。この場合、このクラウド事業者は、クラウド利用者として自社向けの情報セキュリティ対策と、クラウド事業者として利用者向けの情報セキュリティ対策を個別に考えると同時に、両者の共通化を図ることが想定されます。

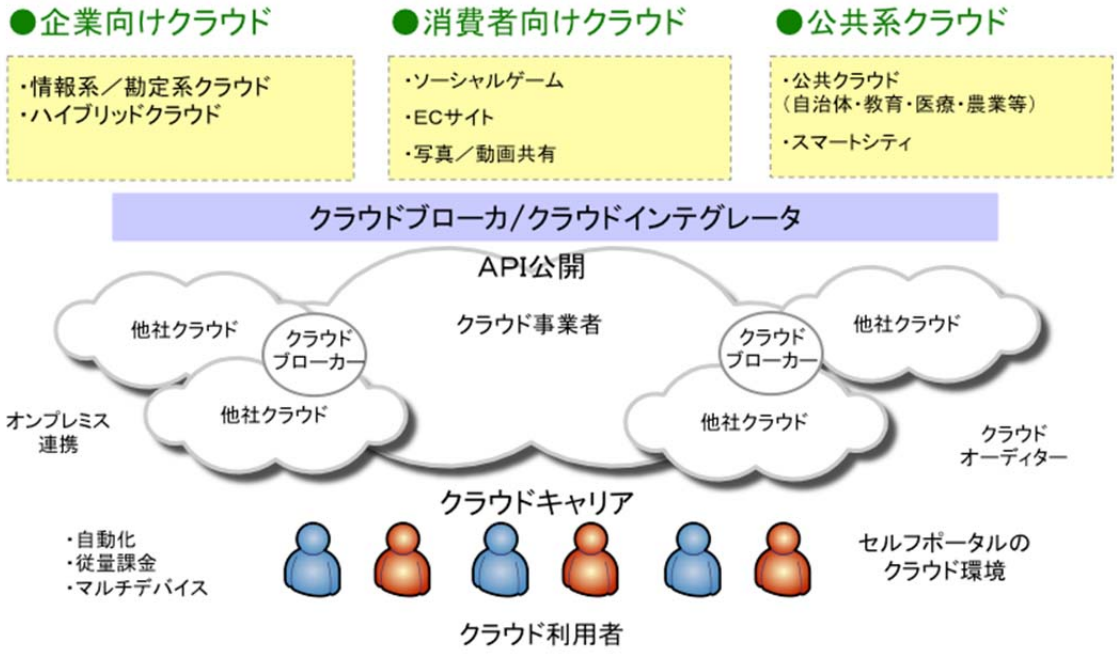

図 6 クラウドサービスを取り巻く環境

クラウドサービスの利用環境では、クラウド利用者、クラウド事業者の他にクラウドサービスの利用をサポートするクラウドブローカー（仲介者）のような、従来は SIer と呼ばれるプレイヤーも登場しました。

クラウドサービスはそれを単体で使うことは少なく、様々なサービスを複合して利用します。また、クラウドサービスをウェブブラウザから使うのではなく、スマートフォンやタブレットなどのアプリケーションから直接使ったり、アプリケーションの一部の機能としてクラウドサービスをアプリケーションプログラミングインタフェース（API）経由で使ったりと、多様な利用環境が想定されています。このような中で利用者がすべての情報を取得し、アレンジするのは非常に難しいということもあり、サービスの相性を見極めたり、サービスの運用のサポートをしたりするクラウドブローカーというポジションが置かれるようになったのです。

クラウド利用とサービスもしくはクラウド事業者の関係を簡単にまとめると、1 つの事業者が提供するクラウドサービスを使う場合、他のサービスを利用して提供されているサービスを使う場合、クラウド利用者が複数のクラウドサービスを複合して使う場合、これらを複合して使う場合の 4 つに分類できます。

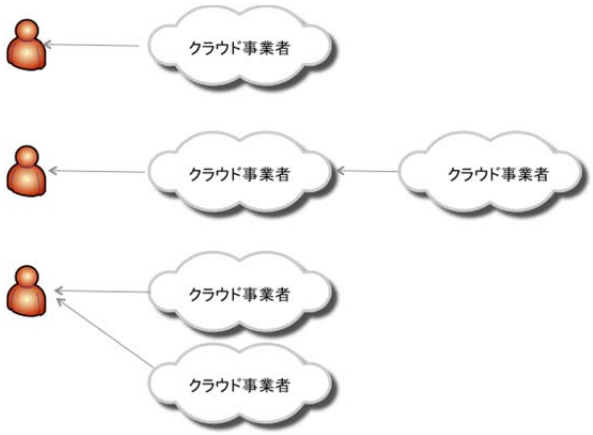

図 7 クラウド利用者と事業者の関係

このような形が複雑に入り組んでくることによって、利用者と事業者の責任分界点が見えなくなってきます。基本的にはサービスの利用における責任は利用者にあるのですが、それは事業者が明確な判断基準を提供していることが前提です。それは契約書であったり、サービスレベル合意だったりしますが、複数の事業者のサービスを利用する場合にどのレベルで検討するのかは非常に難しいといえるでしょう。

2.2.3. クラウドセキュリティガバナンスとサプライチェーン

クラウドセキュリティガバナンスを確保するために、サプライチェーンの構造をよく理解しておくことは重要なポイントです。誰がどのようにしてデータを保管し、どこでどのような記録が取得されているのかなどを知ることによって、情報セキュリティマネジメントの運用に必要な情報を適時入手することができ、安全・安心なクラウド利用ができるようになります。

3. ガイドラインを活用したリスク分析手法

3.1. クラウドセキュリティガイドライン

経済産業省は、クラウドサービスの利用促進とともに、利用者が安心してクラウドサービスを利用できるためのガイドラインとしてクラウドセキュリティガイドラインを2010年4月1日に公表しています。

3.1.1. クラウドセキュリティガイドライン

クラウドセキュリティガイドラインは、クラウドサービスにおける様々な懸念事項を払拭し、安心してクラウドを利用する準備をするために、利用者はどのようなことを考慮することが望ましいのか、そして事業者はそれに対応するためにどのような情報を提供すればよいのかを提案するガイドラインとして公表しました。

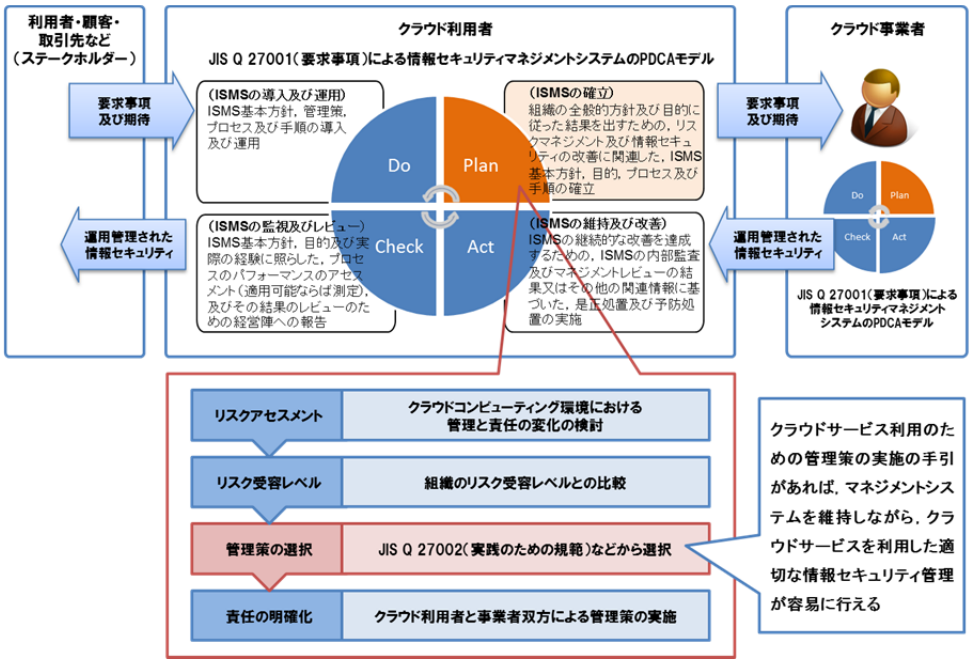

図 8 クラウドサービス利用に関わる管理策の選択（クラウドセキュリティガイドラインより）

国内では多くの企業や団体がISMS認証を取得したり、JIS Q 27001をベースにした情報セキュリティマネジメントシステムを構築しています。その中で、セキュリティ管理策の選択にはJIS Q 27002を参照していることから、利用者が情報セキュリティマネジメントシステムを変更することなく、またリスクアセスメントの手法などを変更することなく取り入れることができるように、クラウドセキュリティガイドラインもJIS Q 27002をベースに作成しました。

クラウドセキュリティガイドラインには、目的、管理策、クラウド利用者のための実施の手引き、クラウド事業者の実施が望まれる事項、クラウドサービスの関連情報というそれぞれの項目を、JIS Q 27002 の管理策の構造のままに掲載しています。

クラウドセキュリティガイドラインが公表された 2010 年当時は、まだクラウドサービスの利用が始まったばかりで実際の事故・障害などもあまり発生しておらず、利用者にとっても事業者にとっても現実的なリスクを提示し、検討することが十分にはできませんでした。

本活用ガイドと共に公表された 2013 年度版のクラウドセキュリティガイドラインでは、これまでのクラウドサービス利用における様々なインシデントや、運用上の経験から今後懸念される様々なトラブルなどを検討し、新たな対策を盛り込んでいます。特にクラウド事業者自らが取り組むべき情報セキュリティ対策についても検討し、追加しています。

3.1.2. クラウドセキュリティガイドラインの国際標準化

本ガイドラインの活用によって、利用者にとっては、国内だけではなく国外のクラウドサービスを安心して利用できるように、また事業者にとっては、国外でもサービスを提供できるように、クラウドセキュリティガイドラインを国際標準化する作業を行っています。

本ガイドラインを国際標準化するために、ガイドラインを英訳し、2010 年 10 月に JTC1 SC27 の秋季ベルリン会合に提案しました。この提案は参加各国に受け入れられ、現在は 2015 年の発行を目標に内容の検討が行われているところです。

米国からの提案には NIST からの提案なども含まれ、Cloud Security Alliance などの事業者団体もリエゾンパートナー（国際標準化会議に意見を提出する団体）として、彼らの提供するガイドラインなどの内容を盛り込む形での提案作業を行っています。他にも、ISACA や ITU-T などの団体もシステム監査の観点やクラウドサービスの技術的な観点からの提案を行い、日本のクラウドセキュリティガイドラインをベースにした国際標準が策定されています。

現在策定中のこの標準は、ISO/IEC 27017 として 2015 年 10 月に発表される予定です。クラウド事業者が自らのサービスに関するクラウド特有のリスクを検討してセキュリティ対策を実施していることを証明するために、ISO/IEC 27001（JIS Q 27001）をマネジメントシステムの標準として選択し、また、ISO/IEC 27017 を管理策の標準として選択することで、クラウド固有のセキュリティ認証を受けられるような仕組みも国際標準化会議で現在検討されています。

3.2. クラウドサービスにおけるリスク分析手法

3.2.1. 構造を意識したリスクの洗い出し

クラウドセキュリティガイドラインでは、クラウドサービス利用に関わるリスクを簡単な図を利用して示しています。

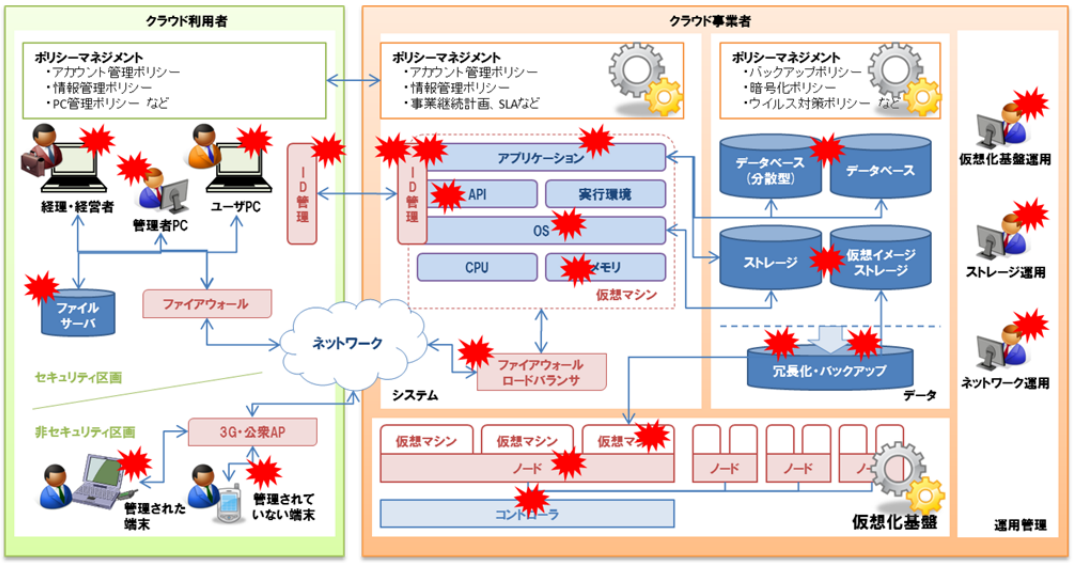

図 9 クラウドサービスのリスクの所在（クラウドセキュリティガイドラインより）

このように図を活用してみると、リスクの所在が分かりやすくなります。簡単な絵でも構いませんので、利用するクラウドサービスと利用者の環境を整理して、全体的なリスクを俯瞰できるようにしましょう。

この図はクラウドセキュリティガイドラインから引用したものですが、利用者のリスク、事業者のリスクを明確にするために附属書 A「クラウドサービス利用にかかわるリスク」で活用しています。また、附属書 B「クラウドサービス利用におけるリスクアセスメントの実施例」では SaaS、PaaS、IaaS という大まかなレベルでのリスクアセスメントですが、自らの環境を図式化することで、より詳細なリスクを知ることが可能です。

3.2.2. 管理策の選択

リスクの所在がわかったら、リスクの軽減を行うために、利用者自身で対応できるものか、事業者からの情報があれば対応できるものか、事業者に対応してもらわなければならないものかを判断しましょう。

自ら作成した図を見ながら、その管理策の実行の主体がどこにあり、管理策の実行主体を判断するための情報がどこにあり、判断するための情報をどのように手に入れることができるのかを考慮します。システムやサービスをクラウドに移行した場合には、それ

までの環境と比較し、どのようなリスクが発生しているか、情報セキュリティマネジメントのために必要な情報を得るためにどのような手順が必要かなどを判断し、情報セキュリティポリシやスタンダード、プロシージャを見直す必要もあります。

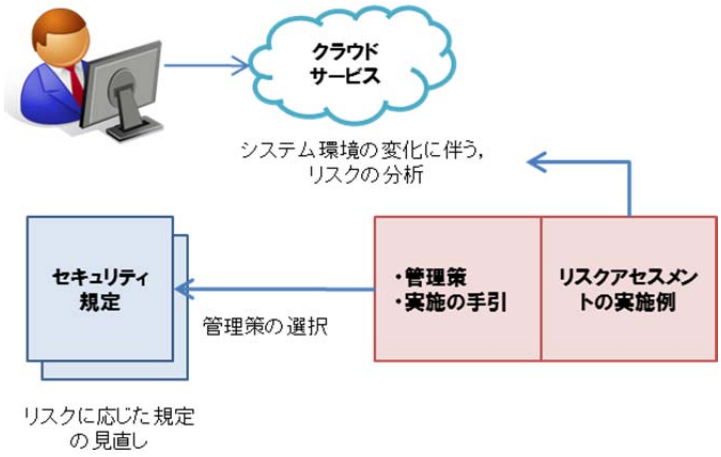

図 10 リスクアセスメントと管理策（クラウドセキュリティガイドラインより）

その上で、具体的な管理策の選択をします。管理策の選択は、クラウドセキュリティガイドラインや本書の「3.3 章 クラウドサービスのリスクと対策」の該当部分を参考にしてください。

クラウドセキュリティガイドラインでは一般的な記述となっているものも、3.3 章では具体的な記述としてあります。その中で自らの組織に合致するものを選択してください。

3.3. クラウドサービスのリスクと対策

3.3.1. インフラに関するリスクと対策

特にクラウド事業者においては、クラウドサービスのインフラについてリスクを検討し、十分な対策を実施しておく必要があります。クラウドサービスのインフラでは以下を対象としてリスクを検討します。

- 物理的な基盤
  - ネットワーク
  - データセンタ
- 論理的な基盤
  - 仮想化基盤
  - サービス基盤
  - 統合管理環境

一般的なデータセンタ管理におけるセキュリティに加えて、クラウド特有の問題として仮想化基盤やそれを取り巻くネットワークや管理システムに関するリスクを検討し、対策を実施する必要があります。

これらのリスクは主にクラウド事業者に関係するリスクですが、クラウド利用者もクラウドサービスの潜在的な問題として認識し、これらの対策を事業者が行っていることを確認するとともに、万が一の事故に備えた対応を実施する必要があります。

ネットワークに関するリスクと対策

クラウドサービス利用におけるネットワークに関するリスクは、主にデータの流出やなりすまし、サービス停止があり、以下のような要因が考えられます。

- 利用者との通信、サーバ間の通信、リージョン間の通信における脅威
    - 通信の傍受
    - 中間者攻撃
    - なりすまし
- コンピュータ環境におけるネットワーク上の脅威
    - ネットワーク管理の不備によるシステムダウン
    - VLAN 構成におけるトラブルによるシステムダウン

通信の傍受への対策

クラウド環境におけるネットワークでは、利用者とサーバ、サーバ間、クラウド事業者のリージョン間での通信がオープンとなっています。これらのオープンな通信環境においては傍受されてはならないデータを流すことがあり、傍受されないような対策を行う必要があります。

流れるデータに応じて通信の暗号化を行うことができるように、SaaS、PaaS などでは予めウェブサーバやアプリケーションサーバなどにおいて暗号通信を標準化もしくはオプションとして選択できるようにしてください（クラウドセキュリティガイドライン 10.8.1 情報交換の方針及び手順を参照）。IaaS ではサーバ構築を行う際に必要に応じて通信の暗号化を実装するようにしてください。

また、クラウド事業者においては複数のリージョン間でデータのやり取りを行うことがあるため、その通信が暗号化されているかどうかを検討する必要があります。事業者はリージョン間の通信において暗号化が実装されているかどうかを利用者に告知するとともに、必要に応じて暗号化を実装するようにしましょう。利用者はリージョン間の暗号化が行われているかどうかを確認するとともに、実装されていない場合は他の方法で通信上のデータを保護できるように検討してください（クラウドセキュリティガイドライン 10.8.4 電子的メッセージ通信を参照）。

中間者攻撃やなりすましへの対策

通信上の傍受と同様に、データを捏造したり、データを外部に持って行ったりしてしまうなど、ネットワークの間に入って様々な損失を与えるのが中間者攻撃です。

クラウドサービスにおいては、認証サービスや決済サービスなどの第三者サービスを利用したり、複数のサービスで API などを利用して活用することが多いと思いますが、その際に身元を捏造してデータや通信そのものを横取りしようというものです。

中間者攻撃に対応するためにはエンドツーエンドでの通信の確認を行う必要があります。利用するサービスがどのようなネットワークで展開されているのかを理解するとともに、間に攻撃者が存在しないことを確認し、もしも攻撃の可能性がある場合にはその間のサーバや端末の相互認証などを行うことが必要になります（クラウドセキュリティガイドライン 11.4.3 ネットワークにおける装置の識別を参照）。SaaS などで他社サービスを利用している場合は特に気をつけてください。

サービス間、機器間でのなりすましがないことを確認するために、必要に応じて証明書などを活用した認証を行うことも重要です（ガイドライン 11.4.3 ネットワークにおける装置の識別を参照）。

内部ネットワーク管理の不備への対策

内部ネットワークにおいては、外部ネットワークと同様に傍受などに気をつけることも重要ですが、クラウドコンピューティングにおいてはネットワークもシステム環境として重要な役割を担っています。例えば、サーバストレージがファイバーチャネルなどを利用したネットワーク構成になっている場合、ネットワークがダウンしてしまうことはデータそのものを失ってしまうことになりかねません。クラウドサービスを構築するクラウドコンピューティングにおいては、ネットワークが重要な要素となり、事業継続管理における脆弱性の対象となっています。

クラウドサービスの環境においてはネットワークが切断されないように、物理的な保護を行うとともに（クラウドセキュリティガイドライン 9.2.3 ケーブル配線のセキュリティを参照）、ネットワークを構成する機器の構成管理や容量管理なども十分に行うこと（クラウドセキュリティガイドライン 7.1.1 資産目録、10.3.1 容量・能力の管理を参照）が重要です。

VLAN 上のトラブルへの対策

クラウドコンピューティングでは仮想化を利用してサービスを構成していることがあり、仮想化で提供されたそれぞれのインスタンス間の通信は仮想ネットワーク（VLAN）を利用していることがほとんどです。これらの仮想ネットワークは通常のネットワークと同様にスイッチングハブなどを利用して通信制御をしていますが、仮想化環境では非常に多くのコンピュータが起動を繰り返し、スイッチングハブのキャパシティを超えた管理を要する場合があります。

クラウドコンピューティングにおいては、ネットワークの通信量だけではなく、接続される機器の数などのキャパシティにも配慮したネットワーク機器の構成管理及びキャパシティ管理を行うことが重要です（クラウドセキュリティガイドライン 10.3.1 容量・能力の管理を参照）。

これまでに保有していた機器を利用してプライベートクラウドの構築を検討している場合には、キャパシティ管理などに特に配慮し、必要に応じてクラウドコンピューティング向けに最適化された機器の導入を検討してください。

データセンタセキュリティに関するリスクと対策

クラウドサービス利用におけるデータセンタに関するリスクには、物理的な攻撃などがあります。また、操作ミスなどの人的セキュリティや電源に関する脅威と脆弱性についても検討する必要があります。

- 物理的な攻撃
  - データセンタへの不正な入退館
  - 機器への直接的な攻撃
- 操作ミスなどの人的セキュリティ
  - 意図しない操作ミス
  - 内部関係者による意図的な攻撃
- 電源に関する脅威と脆弱性
  - 電源の喪失によるサービス停止

データセンタへの不正な入退館への対策

攻撃者はネットワーク上だけではなく、データセンタへの物理的な侵入によって、様々な情報を盗み取ったり、システムに障害を与えようとするかもしれません。クラウドコンピューティングでは管理の集中化を行うことで少人数での運用・管理を可能としている反面、その管理コンソールなどを狙われてしまった場合の被害が大きくなる可能性もあります。また、マルチテナントによる運用ということもあり、利用者が監査などで訪問した場合に、監査対象となる機器などを限定することが難しい場合もあります。

クラウド事業者はデータセンタへの入退館管理を特に厳しくすることが重要です（クラウドセキュリティガイドライン 9.1.1 物理的セキュリティ境界を参照）。また、データセンタの形式が多様化している中で、コンテナタイプのデータセンタなど、単に建物への入室管理だけではなく、敷地への出入りについても十分な管理を行うことが重要です（クラウドセキュリティガイドライン 9.1.1 物理的セキュリティ境界を参照）。

機器への直接的な攻撃への対策

ネットワーク上ではなくデータセンタ内部から直接、機器や管理環境を攻撃することで、ネットワーク上のアクセス制御を超えてシステムを停止させたり、データを破損させたり、盗み出すことが可能です。また、データセンタに入室しなくても、ケーブルや電源などのユーティリティを狙った攻撃によってシステムを停止させることも可能です。

ネットワークや電源などを防御するためには、データセンタ内部だけではなく、敷地に対しても物理的防御を行う必要があります。これらの対策として、データセンタの場所を明確にしないということも一般的でしたが、災害に備えてデータセンタの位置を把握したいという利用者からの要望もあり、現在はデータセンタの大まかな位置は公開されている場合もあります。

これらの状況を考えて、データセンタ及び重要な機器への多層防御を行うことが重要です。一般的には最も重要な機器までの防御は 5 層ほど確保できていることが望ましいと考えられています。重要な機器を特定した上でセキュリティ区画を明確にし、境界防御の具体的な手法を計画し、実装することが重要です（クラウドセキュリティガイドライン 9.2.1 装置の設置及び保護を参照）。

意図しない操作ミスへの対策

クラウドサービスの提供においては技術が変化している最中であり、技術者が十分な知識と経験を持って対応できないことがあります。技術者が操作を行う上でのミスを削減するためには、様々な作業の手順書を作成し、誰が行っても正しい結果が得られるように準備をしておくことが重要です。慣れている作業だということで手順通りに作業を行わなかったことでトラブルが発生しているケースも少なくないからです。

意図しない操作ミスへの対策として、手順書を明確にし、頻繁に行わない作業であっても十分な訓練をして対応することが重要です（クラウドセキュリティガイドライン 10.1.1 操作手順書を参照）。

内部関係者による意図的な攻撃への対策

内部関係者のようにファシリティへのアクセス権を持っていても、実際には作業の実施や機器へのアクセスは許可されていないことがあります。建物への入室や機器へのアクセスについては認可レベルを明確にして、誰がどの領域に入室できて、どの機器をどのように操作できるのかという認可情報を定義し、アクセス制御の方針を決め、実装することが重要です（クラウドセキュリティガイドライン 11.1.1 アクセス制御方針を参照）。

電源の喪失によるサービス停止

クラウドサービスに限らず、コンピューティング環境において電源は重要な要素となります。電源を確保できなければコンピューティグ環境を維持できないためです。クラウドサービスの事故では電源関係のものも少なくなく、バックアップ電源などを確保する

ことも重要なセキュリティ対策となります。万が一の電源トラブルへの対策を十分にするとともに、バックアップ電源などのテストを定期的に行うことも重要です（クラウドセキュリティガイドライン 14.1.3 情報セキュリティを組み込んだ事業継続計画の策定及び実施を参照）。

3.3.2. 仮想化基盤に関するリスクと対策

クラウドサービス利用における仮想化基盤に関するリスクは、新たな技術に対する知識や経験不足による事故対応の不備や IT サービス継続の中断などがあります。

- 事故に備えた対応の不備
    - サービス再開時間の延滞
    - 事故情報の把握ができずに再発防止ができない

事故に備えた対応の不備に対する対策

仮想化された環境においては物理的環境と違い、適切なシステムログを取得できない可能性があります。仮想化レイヤー以上のシステムログは利用者が取得することができますが、仮想化レイヤー以下で起きていることは利用者には把握出来ません。

もしも仮想化レイヤーでのトラブルが発生した場合、これらの情報を取得せずにトラブル対応することはできませんし、深刻なトラブルであった場合はそれに対応するための手段は利用者側にはありません。

仮想化基盤の万が一のトラブルに備えて、インスタンスのバックアップや、システム構築を容易にするためのテンプレートなどを用意しておくとともに、バックアップデータなどのリストアができる他のクラウド事業者のサービスなどを契約しておくことも重要です（クラウドセキュリティガイドライン 14.1.3 情報セキュリティを組み込んだ事業継続計画の策定及び実施を参照）。

3.3.3. サービス基盤に関するリスクと対策

クラウドサービス利用におけるサービス基盤に関するリスクは、単一障害点となる認証サービスへの攻撃や、経済的な損失に直接関係する決済サービスへの攻撃などがあります。SaaS サービスでは他社の提供するサービスへの依存なども検討し、整合性を検討する必要もあります。

- 単一障害点となるサービスに関する脅威
    - 認証サーバへの攻撃
    - 認証サーバのなりすましや中間者攻撃による不整合の発生
- 共有サービスに関する脅威
    - 決済サーバへの攻撃

- マルチテナントで提供されているサービスへの攻撃
- ストレージサーバへの攻撃

単一障害点となるサービスに関する脅威に対する対策

クラウドサービスにおいてはID管理サービスやストレージサービスが単一障害点となります。クラウド上で構築したサービスのコントロールパネルにアクセスするためには認証を受けなければなりません。また、ストレージに様々なデータが保存されるため、適切な保護を実施しなければなりません。

サービスの構成図を作成し単一障害点を明確にすることで、サービスの冗長化などを検討し、事業継続を行うことが重要です（クラウドセキュリティガイドライン 14.1.3 情報セキュリティを組み込んだ事業継続計画の策定及び実施を参照）。

共有サービスに関する脅威に対する対策

クラウドサービスはマルチテナントで運用されています。同じ物理マシンやネットワークを共有している利用者は、他の利用者が攻撃を受けた場合に被害を受ける可能性があります。

物理的にデータの管理を行うためにサービスのリージョン（所在地）を限定してクラウドサービスを受けている利用者がいますが、サービスの継続性という観点では脆弱になりますので、データの所在を確認する他の方法とサービス継続性のトレードオフによって、適切な選択を行うようにしてください（クラウドセキュリティガイドライン 14.1.3 情報セキュリティを組み込んだ事業継続計画の策定及び実施を参照）。

物理サーバが同じ場合ではなくても、ID管理や決済サービスなどは他者と共有している場合があります。これらの共有サービスについても同様の問題が発生する可能性がありますので、サービスについて十分に理解し、対応することが望ましいでしょう。

3.3.4. 統合管理環境に関するリスクと対策

クラウドサービス利用における統合管理環境に関するリスクは、すべてのリソースに攻撃者がアクセスできる可能性があることであり、単体のサーバを狙った攻撃よりも多くの影響をシステムに与える可能性があります。

- 統合管理環境に関する脅威
  - IaaS、PaaSの運用コンソール（GUI、CUI）に対する攻撃
  - SaaSの管理者用パネルに対する攻撃
- 監視環境に関する脅威
  - システム管理のための監視サービスへの攻撃
  - システムログの改ざん

統合管理環境に関する脅威に対する対策

クラウドサービスでは、コントロールパネルからは様々処理を実施できるので、コントロールパネルを攻撃されてしまうと、サービスすべてを止められてしまう可能性があります。

これまではネットワーク上から DDoS などによってサービス不能となるように攻撃をされていましたが、クラウドサービスを利用するようになって、コントロールパネルを攻撃されるようになりました。管理が集約されているために、単一障害点となります。

また、データの管理についても同様です。データの書き換えなどの攻撃が行われてしまうと、正確な情報を提供することがなくなってしまいます。データの改ざんやサービスの停止に備えて、十分な保護を行うことが重要です。サーバの物理的な要塞化が難しいため、サービスレベルでの保護を行うために、やはりアクセス管理を適切に行う必要があります（クラウドセキュリティガイドライン 11.6.1 情報へのアクセス制限を参照）。

認証サービスやストレージサービスへの攻撃やなりすましはシステム全体に被害を及ぼす可能性がありますので。特に重点的に上記の対策を講じる必要があります。

監視環境に関する脅威に対する対策

クラウドサービスの監視は非常に難しいと言われています。
仮想化されたインスタンスが頻繁に起動されたり、シャットダウンされたりするため、ネットワーク越しに継続的にサービスを監視することが難しく、ホストレベルでの監視を行うことが望ましいと言えます。しかしながら、ホストレベルでの監視に IDS などを利用して行うとすると、システムのパフォーマンスに影響を与える可能性が高くなります。

3.3.5. データ管理に関するリスクと対策

クラウドサービス利用におけるデータ管理では以下を対象としてリスクを検討します。データ管理に関連するリスクは主にクラウド利用者が検討するべきものですが、そのリスクを軽減するためにクラウド事業者が提供できる仕組みもあります。クラウド利用者が安心してサービスを利用できるように事業者はシステムやサービスを提供するのが望ましいでしょう。

- データ管理方針
- データ分類（データオーナ、ラベリング、マーキングなど）
- ライフサイクル管理
- バックアップ

クラウドサービスを利用することでデータの所在などが不明瞭になると考える利用者も少なくありません。実際にはそれぞれのデータへのアクセス権に基づいて、様々なデータにアクセスすることができますので、通常の運用においてデータが失われてしまうということはほとんどありません。クラウド利用者がデータ管理方針を明確にして管理することでクラウドサービス上でも適切な管理を行うことが可能です。

データ管理方針に関するリスクと対策

クラウドサービス利用におけるデータ管理方針に関するリスクは、それが徹底されていないことにあり、組織内の利用者が自由にデータをクラウド上に保存したり、クラウド上からデータをダウンロードしたりといった場合に様々な問題が発生することがあります。

- データ管理方針の不徹底
    - データ管理におけるガバナンスの喪失
    - 不正なデータの取得によるウイルス感染

データ管理におけるガバナンスの喪失に対する対策

クラウドサービスの利用によって、様々なデータがクラウド事業者側に保管されることになります。これらが実際にどこにあるのかを把握するのは技術的に難しいのですが、データオーナであれば、適切な権限でアクセスすることで、いつでもデータを参照したり、編集、削除などをすることが可能です。

クラウドでは大きなシステムが一元管理された中で、仮想環境によるインスタンスが立ち上げられ、その中でデータが取り扱われています。それがどのマシンで立ち上がっているのかは仮想化の管理システム上で把握できるものであり、利用者や攻撃者からは把握することはできません。もちろん、サーバの外観からは分かるものではありません。どこにあるか分からないというのは利用者にとっても不安である一方、攻撃者からも把握ができないという利点もあります。

このように、物理的なガバナンスの確保が難しい中で、論理的にデータの所在を把握し、管理をしていくためには適切なアクセス管理を行う必要があります。アクセス管理を適切に行うためには情報分類が重要な要素となります。

クラウドサービスの利用においては、利用者の情報資産の分類方針を明確にし、その中でクラウド上で取り扱うことのできる情報資産の分類を行い、アクセス権を設定して取り扱うことができるかどうか、それが継続的に行われているかどうかを確認することが重要です（クラウドセキュリティガイドライン 7.資産管理を参照）。

不正なデータの取得によるウイルス感染に対する対策

クラウドサービスの利用においては管理するデータを一元化することで管理効率を向上させようとする一方で、ウイルス感染などをした場合の被害も大きくなる可能性があ

ります。SaaS や PaaS 上のデータなどでは実際にはクラウドサービス上でウイルスの実行が行われる可能性は低いため、PC などにデータをダウンロードした際にウイルススキャンを行うことを忘れないようにしてください（クラウドセキュリティガイドライン 10.4 悪意のあるコード及びモバイルコードからの保護を参照）。IaaS では従来のサーバ同様にウイルス対策を実施することを忘れないようにしてください。

クラウドサービス上のデータについては適切にウイルススキャンを行い、アップロード時にもウイルス感染の危険をなくすようにしてください。これらの内容について、クラウドサービス利用の手順に記載するなどして、利用者への気付きを与えられるようにしてください（クラウドセキュリティガイドライン 8.2.2 情報セキュリティの意識向上、教育及び訓練を参照）。

一方で、クラウドサービス上でデータの一元管理を行うことで、PC 上でのウイルススキャンの負荷を軽減させることも可能です。ウイルススキャンによるディスクアクセスや CPU 利用の負荷が軽減されるということもあり、PC の能力を活かして作業を行うことが可能であるというメリットもあります。

3.3.6. データ分類に関するリスクと対策

クラウドサービスの利用時に限らず、データ管理方針に基づいてデータの分類を行い、それにともなって適切な利用を行うのが一般的です。しかし、クラウドサービスによっては自らの組織が決めたデータ分類方針が適用されない場合があります。運用上の問題としてこれらを捉え、適切なルールを作成し直す必要があります。

データを適切に分類できないことで適切なアクセス権を設定できないことがあるというのが、クラウドサービス利用時のデータ分類におけるリスクです。

- データ分類の不徹底
    - 適切なアクセス権の設定不能

適切なアクセス権の設定不能に対する対策

クラウドサービスのアクセス管理、特に SaaS においては、クラウド利用者の組織における権限管理の粒度がサービスで提供されているものと合致しないことがあります。

例えば、利用者組織では管理者権限の他にユーザ権限を 3 段階にしているとしても、サービス側では管理者権限とユーザ権限の 2 つしかないという場合です。このような場合にはクラウドでの利用におけるデータの利用に関するアクセス権を工夫するなどして、対応する必要があります。これらの内容は利用手順に明確に記載するともに、知る必要性や最小権限についても考慮して、権限設定を行いましょう。あくまで主体は利用者組織のポリシにあるということを忘れないようにしてください（クラウドセキュリティガイドライン 11.1.1 アクセス制御方針を参照）。

データのライフサイクル管理に関するリスクと対策

データのライフサイクル管理とは、データを作成してから保管、利用、共有、廃棄などのフェーズにおいて一貫したアクセス権設定ができているかにあります。データオーナが適切なアクセス権を保持したまま、データを管理できるかがポイントとなります。

クラウドサービスの利用において、これらのライフサイクル管理を行うことができるかどうかはサービスや事業者の選択時の重要な要素であり、もしも管理ができないのであれば何らかの対策を行わなければなりません。

- データのライフサイクル管理の未実装
    - データ管理におけるガバナンスの喪失
    - データ漏えい・流出

データ管理におけるライフサイクル管理の欠如に対する対策

クラウドサービスの利用によって、これまでに想定していたライフサイクル管理を行うことができない場合があります。

例えば、ファイルの削除では、復元不可能なように廃棄するということが決められていたとしても、クラウド上では PC 上と物理的な管理手法が違うために、すべてのデータを PC と同様の方法で削除することはできません。クラウドにおける適切な削除方法はどのようなものかを理解し、クラウドサービス上で扱うデータについて、その手順を明確にすることが重要です（クラウドセキュリティガイドライン 10.7.3 情報の取扱手順を参照）。

データ漏えい・流出に対する対策

データの漏えい・流出は、データの管理が適切に行われていない場合に発生することが多いようです。例えば、ISMS においては情報資産一覧を作成してデータなどの情報資産の所在を把握しますが、下書きファイルや送信済みメールなど、実際には把握されていないデータがたくさんあり、そのデータが管理ミスに起因して漏えいしているようです。

管理漏れを起こさないためには、データを不用意にコピーしたり、ローカル PC に保存するなど、データの一元管理を阻害するような行動ができないように適切なアクセス管理を行う必要があります（クラウドセキュリティガイドライン 11.1.1 アクセス制御方針を参照）。

情報セキュリティのコストを適正化するためにも、情報資産を増やさないという方針で、複数の PC やデバイスに情報を無駄にコピーしたり、無作為に印刷したりという業務を行わないようにルールを明確にしましょう。

3.3.7. ID 管理に関するリスクと対策

クラウドサービス上で ID を管理することによって、シングルサインオンなどを比較的簡単に実施できたり、少ない費用で二要素認証や二段階認証などのセキュアな認証システムを導入できる反面、ID のトレーサビリティの管理などが難しくなるといった問題があります。これらのメリットと運用上の問題をトレードオフできるように、十分に検討することが重要です。

クラウドサービス利用における ID 管理では以下を対象としてリスクを検討します。

- ID 管理手法
- ID フェデレーション
- トレーサビリティ

SNS（ソーシャルネットワークサービス）などの SaaS では、Facebook や Google のアカウントを使って他のサービスにログインすることが可能です。このように他のサービスの ID を使ってログインする環境を ID フェデレーションといいます。

クラウドサービスにおいては、ID フェデレーションのために様々なプロトコルが用意されるなど、機能別のサービス提供が行われています。これらの機能をうまく利用することで迅速で安全なサービス提供を行うことも可能です。どのような点に注意してシステム構築を行えばよいのか、またサービスを利用すればよいのかを検討してください。

クラウドにおける ID 管理に関するリスクと対策

クラウドサービスにおいては物理的なデータ管理ではなく、アクセス権に基づくデータ管理を行っているため、ID 管理が重要な機能となります。単一障害点としてだけではなく、様々なデータを結びつけるキーとなるため、ID 管理を適切に行う必要があります。

クラウド上の ID 管理においてはネットワークからの攻撃を受けるため、パスワードの複雑さだけではなく、二要素認証や二段階認証などの単体のパスワードの強度だけに依存しない対策を行うことが重要です。また、クラウドサービスを選択する際にも、コントロールパネルやユーザ管理においてこれらの認証機能が選択できるところを選択するのが良いでしょう（クラウドセキュリティガイドライン 11.2 利用者アクセスの管理を参照）。

ID フェデレーションに関するリスクと対策

ID フェデレーションでは ID 管理の元となるサービスにトラブルが発生した場合に他のサービスにもアクセスできなくなってしまったり、万が一のパスワード漏えいの際には他のサービスまで影響を受けるという可能性がありますので、取り扱うサービスによって ID 管理のレベルを決めておくなど、十分な配慮が必要です（クラウドセキュリティガイドライン 11.3.1 パスワードの利用を参照）。

しかし、ID フェデレーションによって、サービス開発者は ID 管理の部分を他の大きな事業者に委ねることができ、十分なセキュリティを確保することができないサービス事業者においては有効な手段であると言えるでしょう。

ただし、ID フェデレーションを装ってアカウントの搾取を目論む攻撃者もいますので、十分に気をつけてください。どのサービスについて ID フェデレーションが設定されているかは、ID 管理の元となるサービス上で確認ができますので、定期的に確認するようにしてください。

3.3.8. 人員に関するリスクと対策

クラウドサービスだけではなく、どのようなシステムでも、利用したり運用したりするのは人間です。IT 化を進めても、すべてが自動化にならない限りは人員に関するセキュリティ対策は必要です。特にクラウドのように新たな環境においては、これまでの経験では対応できない問題も多く出てくることでしょう。

クラウドサービス利用における人的セキュリティでは以下を対象としてリスクを検討します。

- 利用者のリテラシーに関するリスク
- クラウドサービスの構築・運用・管理に関するリスク

クラウドサービスは利用者が様々な環境から利用できるので、利用者のリテラシーについても多方面から検討する必要があります。また、クラウドサービスを利用したスマートフォンやタブレット向けアプリケーションなどの利用についても、これまでウェブブラウザを利用したサービス利用とは異なったリスクを検討しなくてはなりません。

利用者の環境を十分に考えた人的セキュリティを検討してください。

クラウド利用者のリテラシーに関するリスクと対策

クラウドサービスはまだまだ新しいサービス形態であり、多くの利用者がいる反面、サービスの仕組みについて十分な知識が得られているとは限りません。サービスの内容や機能について理解しないまま自由に使うことは、プライバシの侵害や重要な情報の漏えいにつながる恐れがあります。利用者に十分な注意喚起ができるように気づきを促す資料作成や研修などを行うことが重要です（クラウドセキュリティガイドライン 8.2.2 情報セキュリティの意識向上、教育及び訓練を参照）。

クラウド構築・運用・管理に関するリテラシーに関するリスクと対策

クラウドサービスの利用が進み、クラウド事業者も様々なトラブルを体験しながら知識やスキルを身につけてきたところですが、トラブル時の対応やトラブルが発生しないための対策や手順などを明確にすることで、被害を最小限に食い止めることができるようになります。

個々のエンジニアのスキル向上だけではなく、組織として全体のリテラシーの底上げを行うためにも、手順などの文書化と研修を実施することが重要です。また、経験に基づく対応を適切に行うために、監視環境を構築し予兆管理などもできるようにしておくことが重要です（クラウドセキュリティガイドライン 8.2.2 情報セキュリティの意識向上、教育及び訓練を参照）。

4. クラウド利用者のためのガイドライン活用

4.1. 利用者におけるガイドラインの活用シーン

クラウドサービスの利用による大きなメリットは調達時間の短縮です。これまでは物理的に用意していたサーバやシステムを、オンライン上で契約するだけですぐに利用を開始することができるようになりました。その一方で、調達に関わる契約やシステム構築に関する検討を行うことが充分でない場合があります。

本章では、クラウドサービスを利用して IT サービスやシステムを構築する際に、クラウド利用者がクラウドセキュリティガイドラインを利用してチェックを行う方法などを解説します。

4.2. クラウドサービスを利用してシステムを構築する

クラウドサービスを安全に利用する場合、どのような点に気をつけたら良いのでしょうか。この章ではクラウド利用者のみなさんに安心してクラウドを利用していただくためのクラウドセキュリティガイドラインの活用方法について、いくつかの活用シーンを例に解説します。

システムの構築の最初のフェーズはシステムの取得です。システムの取得については、クラウドセキュリティガイドラインの「12.1 情報システムの取得、開発及び保守」に記載されています。

特に重要な事はこれから構築するシステムについて情報システムのセキュリティ要求事項を明確にする事です。クラウドサービスを利用して構築するシステムのコンポーネントのそれぞれについて、どのようなセキュリティ機能を実装し、それが正しく機能しているかどうかを判断できるようなしくみを作ることが重要です。

クラウドセキュリティガイドラインでは 12.1.1 セキュリティ要求事項の分析及び仕様化で示しているように、組織の情報セキュリティ基本方針をもとにセキュリティ要求事項の仕様を決定していかなければいけません。

本章ではこれをそれぞれの組織で検討する際の着眼点として、コンポーネントごとにどのようなセキュリティ機能を実装することができるかのヒントとなる情報を提供しています。公開 WEB サイト、従業員向け業務システムについて、一例となるコンポーネントを紹介していますので、システムのセキュリティ仕様を検討する際の参考にしてください。

なお、他者のクラウドサービスを利用してクラウドサービスを提供している事業者もクラウドサービスの利用者として扱っています。また、クラウドサービスを利用して社内サービスを構築しているシステム管理部門も利用者として捉えています。

図 11 クラウドサービスのサプライチェーン

本章では活用シーンを想定したクラウドセキュリティガイドラインの活用の他に、「クラウド事業者の選択」、「クラウドサービスの契約」及び「クラウドサービスにおけるインシデント対応」についても解説しています。

特にクラウドサービス利用における契約については、契約書のサンプルを参考資料として添付していますので、利用者だけではなく、これからクラウドを利用してサービスを提供しようと考えている事業者も参考にしてください。また、サービスレベル合意（以下、SLA）についても参考資料を添付しています。考え方などの参考になれば幸いです。

ここではクラウドの利用方法について以下の２つのパターンで考えます。

1. 公開 WEB サイト
2. 従業員向け業務システム

それぞれ次のような特性を想定しています。詳細は 4.2.1 及び 4.2.2 をご覧ください。

	公開WEBサイト	従業員向け 業務システム
利用者	一般消費者など	従業員
	不特定	特定されている
インターネット公開	公開されている	限定的
SaaS利用	×	○
PaaS利用	○	○
IaaS利用	○	○
再販の可能性	○	×

図 12 利用シーンの比較

4.2.1. 一般的なウェブサイトを構築する場合

まずはクラウドサービスを利用して、一般的なウェブサイトを構築する場合を考えてみましょう。

ウェブサイトは一般的に公開情報のみを掲載しています。公開情報に対しては情報漏えいなどの心配をする必要はありませんが、情報の改ざんなどについては気をつけなくてはいけません。情報の改ざんはどのように行われるのでしょうか。

情報の改ざんは、サーバ上のファイル管理の権限を奪取されてしまうことが原因で発生します。これはファイルアップロードのためのパスワードが盗まれてしまったり、ファイル管理システムの管理者権限そのものを奪われてしまうことが原因です。クラウド環境においては、サーバそのものを管理するためのコントロールパネルというものがあり、そのアクセス権を侵害されることで、システム全体を乗っ取られてしまうこともあります。サーバ管理の権限について十分に理解し、どのような構成になっているのかを把握しておく必要があります。

クラウドを利用したウェブサイトの多くは以下のような構成になっています。ここではデータ管理用のデータベースなどもその範囲としています。

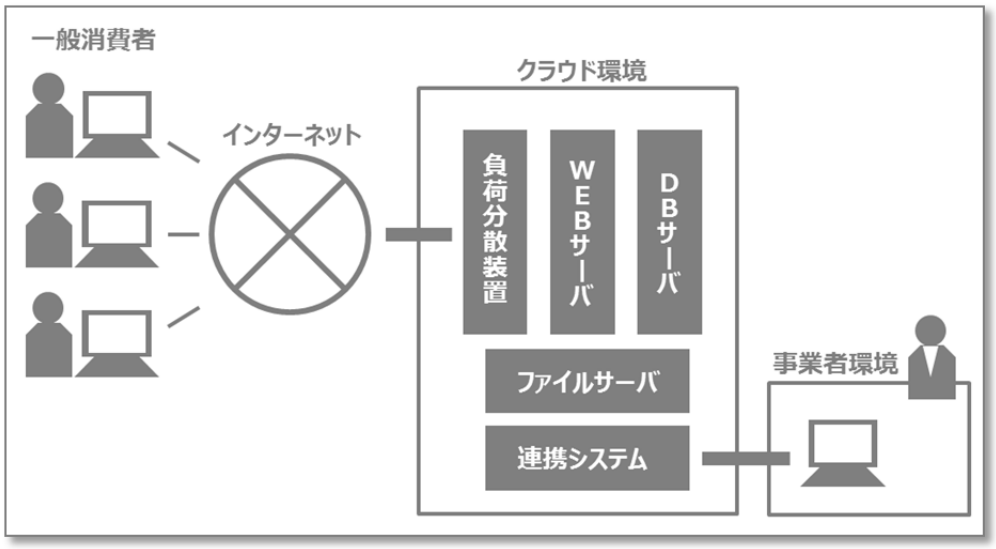

図 13 利用シーンにおけるクラウドの構成

この場合、次のような構成要素（コンポーネント）についてリスクの検討が必要となります。

a) インターネット～クラウド環境間のネットワーク

b) 負荷分散装置

c) ウェブサーバ

d) DB サーバ

e) ファイルサーバ

f) クラウド環境～事業者間のネットワーク

また、次のようなリスクを検討する必要があります。

1) 障害などにより WEB サイトが長期間閲覧できなくなるリスク

2) アクセス集中により WEB サイトが長期間閲覧できなくなるリスク

3) 障害などにより WEB サイト上のコンテンツやデータが消失するリスク

4) 悪意の第三者により、WEB サイトが改ざんされたり、本来秘匿すべき中間データや公表前情報が流出するリスク

個々のリスクについてどのように対策するかを検討しましょう。

a) インターネット～クラウド環境間のネットワーク

クラウド事業者の障害により、インターネットに接続できなくなるリスクを考えてみましょう。通常のクラウド事業者は、この部分を広帯域で冗長構成していると考えられるので、ほとんど問題になることはないと考えられます。回線の敷設自体は大きな投資であり、その費用はクラウド事業者が負います。個々の利用者が増設などを要求することは難しいといえます。この部分に障害が起きればクラウド事業者自体もサービス提供できない（＝利用料を課金できない）のみならず、SLA によってはペナルティを支払わなければなりません。クラウド事業者側が回線の早期普及に全力を上げるであろうことは想像に難くありません。現実問題として、このような構造を理解しつつ、過去の障害発生状況などを勘案して、利用者側がリスクを受容することになると考えられます。

b) 負荷分散機能

クラウド事業者側が「装置」を提供しているのではなく「サービス」として提供している例が多いようです。a)と同様の理由から、この部分の障害発生率は極めて低く、また、障害発生時の短期回復も見込めることから、対応としても a)と同様となると考えられます。また、後述する「広域負荷分散」が必要な場合においては、これが実現可能なサービスを選択する必要があります。なお、サービスとしての利用は、自分で負荷分散装置やソフトウェアを導入／設定するよりも容易に速やかに利用を始められますが、一方で、細かい設定がどこまでサポートされているかなど、技術面の事前の確認が必要です。

世界中のインターネットユーザにサービス提供するような場合においては、広域負荷分散の実現も必要不可欠です。ここでは２つの意味があります。

1. 各々のユーザが地理的にもネットワーク論理的にも「近い」データセンタにアクセスすること（レスポンス確保）。
2. 一つの地域で障害が発生しても、別の地域のデータセンタを用いて可用性が担保できること（ディザスタリカバリ）。

いずれにおいても、負荷分散装置に適切な機能が具備されている必要があります。

c) ウェブサーバ

まず、ウェブサーバ自体の死活が問題になります。ここでは PaaS を利用しているか、IaaS を利用しているかで責任分界が変わります。また、一時的なピークアクセスや、将来予想されるアクセス増に備え、伸縮自在に（＝エラスティックに）ウェブサーバのスペックや台数を増減する方法が問題になる場合もあります。

PaaS を利用する場合、ウェブサーバの障害監視やフェイルオーバー、エラスティックなリソース増減は PaaS 事業者側の責任となると考えられます。利用者側は積極的な死活監視の必要が薄く、また、障害発生時のフェイルオーバーの仕組みを準備する必要が

なくなっていると言えます（いずれも PaaS 事業者自らが。サービス提供業務の一環として実施します）。

IaaS を利用する場合、その仮想サーバの用途はクラウド事業者側では把握できません。ウェブサーバとしてのセットアップ、管理、死活監視、エラスティックなリソース増減の設定は利用者側の責任となります。必要に応じてシステム・インテグレータなどのクラウドブローカーに支援を依頼することも検討します。

ウェブサーバにクラウドを活用することは、非常にクラウドらしい使い方だと言えます。自分でサーバなどのハードウェアを調達し数年間利用する従来の方法だと、将来予想されるピークの処理性能に合わせた機器構成になるため、一般的に過剰な構成となりがちで、普段の稼働率は低くなり、無駄が多くなります。これに対してクラウドでは、必要な時に、必要な処理性能のサーバを、必要な数だけ調達します。このような増強（スケールアウト、と言います）を速やかに実現できるというクラウドならではの特性を活かすことが重要です。

d) DB サーバ

前項同様に、まず、DB サーバ自体の死活が問題になります。ここでも PaaS を利用しているか、IaaS を利用しているかで責任分界が変わります。物理層（サーバやデータセンタなど）に障害が発生した場合に備え、定期的に（例えば、毎晩深夜など）バックアップを取得するのはもちろんのこと、複数のサーバを組み合わせた冗長構成を組んでおくことも有益と考えられます。

PaaS を利用する場合は、ウェブサーバと同様に、DB サーバの障害監視やフェイルオーバーも PaaS 事業者側の責任となると考えられます。利用者側は積極的な死活監視の必要が薄く、また、冗長構成に関する設計上の対応を行う必要がありません（いずれも PaaS 事業者自らが、サービス提供業務の一環として実施します）。バックアップの取得も利用者が頻度や取得タイミングを指定するだけで済むケースもあります。

IaaS を利用する場合、DB サーバとしてのセットアップ、管理、死活監視、バックアップ、冗長構成を考えた設計などは、利用者側の責任となります。必要に応じてシステム・インテグレータなどのクラウドブローカーに支援を依頼することも検討します。

e) ファイルサーバ

中間ファイルやスタティックなファイルの置き場、あるいは、メンテナンス時の作業ファイルの置き場としてファイルサーバを置くことがあります。普段は使わないのであれば、寝かせておく（稼働させないでおく）ことでコスト減を図ることができます。逆に、ミッションクリティカルなシステム全体に組み込まれているのであれば、ウェブサーバ、DB サーバ同様の監視やバックアップが必要です。PaaS 利用か IaaS 利用かで、責任分界が変わるのは他のサーバと同様です。

f) クラウド環境～事業者間のネットワーク

システム管理者がメンテナンスのために接続したり、事業のためにシステムから重要な情報を取得したりするために利用します。非常に強い権限を持つ管理者がアクセスしますので、従来は、「メンテナンス用の回線」として、ISDN 接続（着信番号規制をする）や、低帯域の専用線接続を用意することが一般的でした。クラウドではこれらの回線を利用できない場合があります。したがって、一般的なインターネット接続を用いた VPN 接続（環境毎）などの手段を検討します。この手段をクラウド事業者が標準的に提供している場合もありますが、提供されていない場合は、利用者が自ら組み込む必要があります。この他にも、悪意のある第三者による不正なサイト改ざんやウイルスの混入を防ぐために、電子証明書による送信者の認証と通信路の暗号化（sftp や scp による）や、送信者の IP アドレスの特定（制限）などの措置を講じます。

以上がコンポーネント単位でみたリスクとその対応になります。以下ではクラウド利用者からみたリスク全般について解説します。

1) 障害などにより WEB サイトが長期間閲覧できなくなるリスク

仮想サーバの障害を想定するのであれば、複数の仮想サーバを用いた冗長構成を組みます。自前の環境でシステムを構築する場合と全く同じ発想です。

データセンタレベルの障害を想定するのであれば、複数のデータセンタをまたいだ構成を検討します。自前の環境で同様のことを実現しようとすると著しくコストがかかりますが、クラウドを使えばその費用は限定的です。

大規模災害などで、複数のデータセンタすら利用不能になる事態まで想定するのであれば、国境を越えた構成を組むことも、クラウドなら可能です。これによって極めて高いレベルでの可用性を担保できます。

単一のクラウド事業者に依存することは、事業撤退などのリスクを受容することになりますが、これが受容できない場合には、複数のクラウド事業者のサービスを組み合わせることで、更に高い可用性を確保することが可能です。

このリスクに関しては、クラウドセキュリティガイドラインの「10.2 第三者が提供するサービスの管理」および「10.3.1 容量・能力の管理」を参考にしてください。

2) アクセス集中により WEB サイトが長期間閲覧できなくなるリスク

b)負荷分散装置や、c)ウェブサーバでも触れましたが、適切な負荷分散及び拡張的な利用により、アクセス集中による障害／遅延を回避することが技術的に可能です。場合によっては、国境を越えたロードバランシング（グローバルロードバランシング）を行うことで、可用性と負荷分散を同時に確保することも可能になります。

このリスクに関しては、クラウドセキュリティガイドラインの「10.2 第三者が提供するサービスの管理」、「10.10.2 システム使用状況の監視」を参考にしてください。

3）障害などにより WEB サイト上のコンテンツやデータが消失するリスク

重要なシステムやデータについては、バックアップを取得します。これは自前のシステムを構築・運用する場合と全く同じです。クラウドサービスの利用において、利用者はハードウェアを保有してなくても良いという反面、システムやデータの復旧をハードウェアレベルでできないという問題もあります。手元のマシンであれば、ハードディスクのクラッシュなどでデータを失った場合でも、何らかの手法で復旧することは容易なように思えます。それでも障害発生の可能性はあり、常にバックアップや遠隔保管などの措置を講じます。この考え方はクラウド上のシステムでも大きな変化はありません。したがって、バックアップなどの措置を、誰が、どのように実施し、また、どのような可用性や稼働実績を持ったインフラを使うのか、充分確認する必要があります。

データのみならずシステムのバックアップも重要な事項です。この点においてクラウドは、手元に置いたシステムと比べて圧倒的に利便性が高いのが特徴です。ほぼすべてのクラウド事業者（PaaS、IaaS）が、容易にバックアップ（マシンイメージ、スナップショットなど）が取得可能な仕組みを用意しています。また、SaaS については、そもそも利用者においてシステムのバックアップを検討する必要がありません。

PaaS、IaaS の利用者においては、システムの運用において、誰がどのようなタイミングで上述のようなバックアップを取得しているか、確認すべきです。必要に応じ、一時的にコンピュータリソースを借りるなどして「バックアップからの復旧」の演習をすることも好ましいと言えます。

このリスクに関しては、クラウドセキュリティガイドラインの「10.5 バックアップ」を参考にしてください。

4）悪意の第三者により、WEB サイトが改ざんされたり、本来秘匿すべき中間データや公表前情報が流出するリスク

自前でシステムを構築する場合、何らかの侵入防御の仕組みを自ら構築し、また、運用する必要があります。クラウドであれば、クラウド事業者がこのような仕組みを予め持っている場合があり、ユーザはこの点について運用負荷やコストを軽減させることが可能になります。利用するクラウドサービスが、このような仕組みを組み込んでいるか否か、事前にホワイトペーパーなどで確認をしておきます。

このリスクに関しては、クラウドセキュリティガイドラインの「10.1.2 変更管理」および「10.4 悪意のあるコード及びモバイルコードからの保護」、「11 アクセス制御」を参考にしてください。

4.2.2. クラウドサービスを利用して社内システムを構築する場合

ここでは複数の拠点を持つ企業が、その従業員向けに業務システムをクラウド環境上で利用しているケースを検討します。従業員の大半は同企業のオフィス内から業務システ

ムを利用しますが、一部例外的に移動中にモバイル機器で利用する者や在宅勤務者など、インターネット経由での利用者が居ることも想定します。主な構成例を下図に示します。

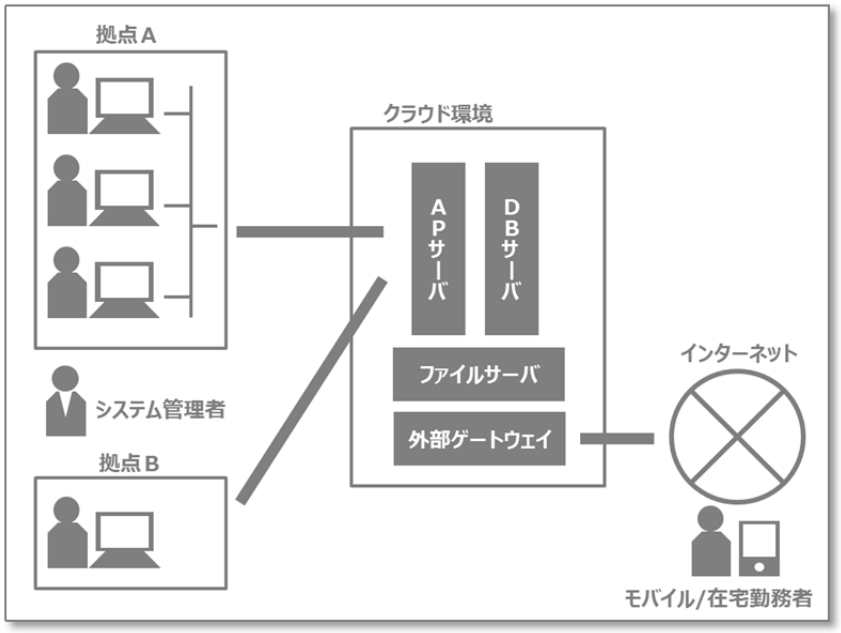

図 14 利用シーンにおけるクラウドの構成

この場合、次のような構成要素についてリスクの検討が必要となります。

a) 各拠点～クラウド環境間のネットワーク
b) AP サーバ
c) DB サーバ
d) ファイルサーバ
e) クラウド環境～インターネット間のネットワーク
f) モバイル機器
g) テレワーキング（在宅勤務）

また、次のようなリスクを検討する必要があります。

1) 障害などによりアプリケーションが長時間利用できなくなるリスク
2) 利用したい時間と、クラウド事業者側の計画保守などによる停止時間が重なるリスク（障害ではない停止）
3) 障害などによりアプリケーションのデータが消失するリスク
4) 悪意の第三者がアプリケーションにログインし、不正な行為をなすリスク

個々のリスクについてどのように対応するかを検討しましょう。

a) 各拠点～クラウド環境間のネットワーク

この部分では、業務上、重要なデータが行き来します。第三者が不当な接続を行わないよう、かつ通信経路上での情報漏えい（盗聴）が発生しないよう、利用者（企業）における LAN／WAN 環境の延長としてクラウド環境を構成することが望ましいといえます。接続にはインターネット VPN や IP-VPN などの技術を用います。更にレスポンスを確保したい場合には専用線接続などを検討することになります。クラウド事業者によっては、すべての選択肢が利用可能とは限りませんので、留意が必要です。

b) AP サーバ

一般的なウェブサーバと同様の検討が必要です。従業員の数や入出力のデータが大幅に変動することは考えにくいので、エラスティックな構成を考える必要はありません。業務の重要度によっては可用性を高めた設計が必要になります。

a)で述べたようにこの AP サーバは論理的に LAN／WAN 上にある状態になります。エンドユーザの PC などから直接接続されることが想定されますので、適切なウイルス対策などを講じる必要があります。

c) DB サーバ

公開用の DB サーバと同様の検討が必要です。また、AP サーバ同様にウイルス対策などを適切に行う必要があります。

d) ファイルサーバ

公開用のファイルサーバと同様の検討が必要です。ウイルス対策などについても b)、c)同様に検討します。

e) クラウド環境～インターネット間のネットワーク

自前でデータセンタを借りてシステム構築する場合と比べて、クラウド環境はインターネットとの親和性が高いと言えます。この例にあるように、モバイル利用や在宅勤務者向けに開かれた構成を組むことは非常にやりやすい一方で、設計を誤ると大きなセキュリティ上の懸念を生み出す原因にもなります。SaaS や PaaS を利用する場合であれば、この種の接続をセキュアに行うためのオプションを用意している例もありますが、IaaS を利用する場合は、この部分の設計や技術的対応は利用者の責任となります。

f) モバイル端末

IT サービスの利用においてモバイル端末（持ち出し PC やスマートフォン、タブレットなど）を利用する場合には、接続したネットワークから必要以上の情報を取得することができないように、データ及びネットワーク上の制限をしておくことが望ましいでしょう。

g) テレワーキング（在宅勤務）

モバイル端末での運用と同様に在宅勤務においては専用の PC が用意されていない場合があります。対策としてはモバイル端末と同様に、接続したネットワークから必要以上の情報を取得することができないように、データ及びネットワーク上の制限をしておくことが望ましいでしょう。

以上がコンポーネント単位でみたリスクとその対応になります。続いて、サービスにおけるリスク全般についての認識と個々のコンポーネントへの落とし込みを解説します。

1) 障害などによりアプリケーションが長時間利用できなくなるリスク

g)の検討と同様です。想定されるリスクと業務に必要な可用性、コストを総合的に判断して、仮想サーバレベル、データセンタレベル、あるいはリージョンレベルでの冗長性を確保します。複数のクラウド事業者のサービスを組み合わせて高い可用性を確保することも可能です。

このリスクに関しては、クラウドセキュリティガイドラインの「10.2 第三者が提供するサービスの管理」および「10.3.1 容量・能力の管理」を参考にしてください。

2) 利用したい時間と、クラウド事業者側の計画保守などによる停止時間が重なるリスク（障害ではない停止）

計画停止は障害ではないので、ある程度の間隔で発生することはありえます。クラウド事業者は多数の利用者を有しており、すべての利用者の都合に合わせることは事実上不可能です。計画停止のスケジュールは、一方的な通告により、交渉の余地なく行われると考えた方が良いでしょう。事前にクラウド事業者の SLA や、過去の計画停止などの実績を十分に把握しておくことが必要と言えます。

このリスクに関しては、クラウドセキュリティガイドラインの「10.2 第三者が提供するサービスの管理」を参考にしてください。

3) 障害などによりアプリケーションのデータが消失するリスク

障害などによってサービスが使えないだけではなく、データそのものが消失してしまうことがあります。これらの問題に対応できるように、適切な期間でバックアップを取得することができるようにしましょう。バックアップデータの大きさによっては、ネットワーク越しのダウンロードなどで非常に時間がかかってしまうことが予想されます。差分バックアップや増分バックアップ、他のクラウドサービスへの複製、レプリケーションなど、適正なバックアップ取得を検討してください。

このリスクに関しては、クラウドセキュリティガイドラインの「10.5 バックアップ」を参考にしてください。

4) 悪意の第三者がアプリケーションにログインし、不正な行為をなすリスク

これはクラウド独特の問題ではなく、利用者側による ID 管理の問題です。クラウドにおいては適切な管理が重要な要素となっています。

このリスクに関しては、クラウドセキュリティガイドラインの「10.1.3 職務の分割」および「10.4 悪意のあるコード及びモバイルコードからの保護」、「11 アクセス制御」を参考にしてください。

4.3. クラウド事業者の選択

4.3.1. クラウドセキュリティガイドラインを利用した選択

クラウドサービスはその多くが、下位のレイヤーを隠ぺいします。つまり、IaaS はハードウェアのレイヤーを隠ぺいすることで利用者にメリットを生み出しており、PaaS もアプリケーション稼働環境までを隠ぺいします。従って、クラウドを選定する上では、この隠ぺいされた部分への不安感が原因となり利用が推進できない事態を生みだす傾向が見られます。

クラウド事業者を選択する際には、クラウドセキュリティガイドラインに従って情報提供している事業者を検討し、自らの必要とする情報を入手することができるかどうかを判断してください。セキュリティ上の観点から情報公開のレベルを抑制している事業者もあり、その場合には、事業者が取得している第三者認証や、事業者が開示しているホワイトペーパー、公開事例、また、事業者の情報公開に対する姿勢（障害時の初期対応、原因や背景などの公表、改善策の開示など）を参考に補完することになるでしょう。

サービスの種類（SaaS、PaaS、IaaS）を選ぶ際の注意点について、リスクの観点から簡単に触れます。まず、クラウド利用者側でクラウドサービスを利用する目的を明確にします。これにより、どのような機能が必要であるのか、そして、どのようなデータをクラウドサービスに預けることになるのかを、併せて明らかにします。クラウドサービスに預けるデータが明らかになれば、データの重要性などから必然的に求められるセキュリティレベルや実施すべき対応が明らかになります。どのような対応が必要なのか、ガイドラインなどを活用し、確認することが望ましいといえます。

他のポイントとしては、データバックアップなどの利用者が最低限行う必要のある行為をサポートしているか利用者が確認したい情報（各種ログ、障害情報など）を望むタイミングで取得することができるかといった、運用管理という観点も考慮することをおすすめします。

最後にクラウドらしいサービスの選定の方法を紹介します。従来と違い、クラウドサービスではフリーミアムと呼ばれる、一定期間無料で利用ができる場合も多く、また従量課金制度などにより最小限の単位で実際のサービス内容を利用して確かめることが可

能です。これらの特徴を活かして、できるだけ正式採用前に実際に使って試してみることも重要な選定方法と言えます。

特にクラウドセキュリティガイドラインの「12.1 情報システムのセキュリティ要求事項」を参考にしながら、自らの情報セキュリティポリシーに従ったシステムのセキュリティ仕様に見合った事業者を選択することが重要です。サービスの機能だけではなく、その機能に伴うセキュリティ機能やそれを担保するためのログなどの証拠が取得できるかなどを検討し、事業者やサービスの選択を行ってください。

4.3.2. インシデント事例に基づくクラウド事業者の選択

調査結果でも出ていたように、クラウドサービスのインシデントの多くはクラウド事業者の環境の問題（ハードウェアやソフトウェアのトラブル）に起因しています。残念ながら、これらのトラブルへの対応はクラウド利用者が関与することはできません。

クラウド利用者は万が一のトラブルに備えてバックアップを取っておくこと、バックアップデータなどをリストアできる別の事業者と契約しておくことが重要です。この観点から、「バックアップを取得しやすい事業者」、「取得したバックアップをリストアしやすい（互換性のある）事業者」を選択するのが良いでしょう。

また、現在は大きく報道されていない事故で、大きな被害をもたらす可能性がある脅威としては、コントロールパネルを狙ったサービス不能攻撃があります。

コントロールパネルへのアクセス制御を行うために「多要素認証（二段階認証、二要素認証など）に対応していること」、「管理者用ネットワークの制限ができること」などが重要な機能となります。コントロールパネルへのアクセスについて、これらの機能を有しているもしくはオプションで選択することができるクラウド事業者を選択するのが良いでしょう。

インシデント対応についてはクラウドセキュリティガイドラインの「13 インシデントの管理」を十分に検討し、自らの組織の情報セキュリティマネジメントにおけるインシデント管理、特に情報収集の時間やバックアップからの復旧の時間など、システムやサービスの回復などについて注目しながら、検討を行ってください。

クラウドサービスの利用においては、バックアップの考え方が自らシステムを保有している場合と異なります。特にバックアップの取得やバックアップからの復元のしやすさなどについて、クラウドセキュリティガイドラインの「10.5 バックアップ」を参照しながら検討してください。

本ガイドブックの「4.5 インシデントに備えた準備と対応」でも解説しています。

4.4. クラウドサービスの契約

クラウドサービスの利用は、IT サービスの利用の側面と、運用管理のアウトソーシングの側面を持っています。契約についてもこれらについて十分に配慮し、検討する必要があります。

クラウドセキュリティガイドラインでは「6.2.3 第三者との契約におけるセキュリティ」で触れていますが、これらを実現するための具体的な内容として、本章では Appendix A、B に掲載した契約書及び SLA のサンプルを活用した契約の検討について解説します。

4.4.1. 利用契約、約款の重要性

消費者・事業者がクラウドサービスの利用を考える目的は様々です。クラウドサービスの利用には様々なリスクが伴いますが、このリスクは、利用者がどのような目的で、どのような情報をクラウド上で取り扱おうとしているのか、それぞれの利用態様によって異なります。

そこで、利用者がクラウドサービスを利用するにあたっては、クラウド事業者の提供するサービスが利用者の具体的な利用目的を達成するものであるか、データ保護の仕組みやサービスが止まってしまった場合の損害賠償は取り扱うデータの重要性に照らして適切なものであるか、といった点を確認する必要があります。そして、これらを定めているのが、クラウド利用契約・約款（以下「クラウド利用契約」といいます。）です。

クラウドサービスにおいては、多数の利用者に対して、同種のサービスが一律に提供されることが通常であり、そのため、具体的な契約条件を交渉によって決するという場面は多くなく、むしろ、契約条件は、クラウド事業者の用意するクラウド利用契約にそのまま従うという場面がほとんどであると考えられます。そのような場面においては、利用者にとっては、クラウド利用契約や SLA の内容がクラウド事業者の選択基準に直結します。その意味でもこれらクラウド利用契約は重要であるといえます。

4.4.2. 契約面におけるクラウドサービス利用のリスク

欧州 ネットワーク情報セキュリティ庁（ENISA：European Network and Information Security Agency）の発行した「クラウドコンピューティング：情報セキュリティに関わる利点、リスク及び推奨事項」（Cloud Computing: Benefits、 risks and recommendations for information security）によれば、クラウド利用のリスクは、「①ポリシ及び組織的リスク」、「②技術的リスク」及び「③法律的リスク」に分けられます[1]。

---

1 http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computi

①ポリシと組織関連のリスクとしては、いわゆる「ロックイン」(“Lock-In”)や「ガバナンスの喪失」(“Loss Of Governance”)というリスクが挙げられます。「ロックイン」とは、データ及びサービスをあるクラウド事業者から他のクラウド事業者に移転・変更することが可能となる仕組みが充分に想定されていないために、利用者が現在利用しているクラウド事業者から他のクラウド事業者に移行することなどが困難になってしまうリスクです。利用中のクラウド事業者が倒産したり、クラウド事業を廃止したりした場合には、問題は一層大きくなります。また、「ガバナンスの喪失」とは、クラウドサービスにおいては、クラウド事業者が利用者の保有するデータを直接管理することとなり、利用者において利用者の判断で当該データの管理を行うことが充分にはできなくなることに起因するリスクです。

②技術的リスクとしては、「隔離の失敗」(“Isolation Failure”)などが挙げられます。「隔離の失敗」とは、一つのサーバやネットワークなどが複数の利用者により共有されているクラウドサービス（いわゆるパブリッククラウド）において、複数の利用者のストレージやルーティングを隔離するメカニズムが充分に用意されていないことに起因するリスクです。

③法律的リスクとしては、「司法権の違いから来るリスク」(“Risk From Changes of Jurisdiction”)が挙げられます。クラウド事業者のサーバは日本国外に設置されている場合もありますが、仮に、当該地が法制度の十分に整っていない国である場合に、法的に問題のあるサーバの差押えなどにより、サーバ内のデータが強制的に没収されるなどのリスクをいいます。また、法制度は整っていても、当該地の法律が広範な捜査権を捜査機関に付与していたり、法律の適用に不明確な点があるなどの理由で、予期せぬ形でサーバ内のデータの開示を余儀なくされる、などといったリスクもここに含めてよいでしょう。特に、複数の利用者が物理的に同一のサーバ機器などを共有しているクラウドサービスにおいては、他の利用者に関する捜査であっても、システム停止などの影響を受ける可能性があり得ることに注意が必要です。この点、しばしば言及されるものとして米国パトリオット法が挙げられます。同法は、2001 年 9 月 11 日に発生した同時多発テロを受け、従来から存在する複数の法律をテロ対策に円滑に適用することを目的として体系化された法律です。従来から存在する法律の手続きを踏まえつつ、テロリズムやコンピュータ詐欺及びコンピュータ濫用罪に関連する有線通信や電子的通信を傍受する権限、あるいは電子メールやボイスメール（留守番電話）を入手する権限などが捜査機関に与えられるものとなっています。

4.4.3. 契約からみた事業者と利用者の責任分界点

クラウド利用契約の重要なポイントの 1 つに、クラウド事業者と利用者の責任の分担の問題があります。例えば、「当社の設備に接続するためのインターネット接続サービス

---

ng-risk-assessment

の不具合などの利用者における接続環境の障害については、クラウド事業者は責任を負わない。」と規定されるのが通例です。クラウド事業者は、利用者側の環境に起因して発生した損害までは負担しないとするのが公平だからです。

クラウド事業者のサービスは、他社のインフラサービス、環境を基礎として提供されることも多く、様々なサプライチェーンの上に成り立っていることがありますが、クラウド事業者が開発していないソフトウェア及びデータベースに起因して発生した損害をクラウド事業者の責任から除外していることもあります。例えば、「クラウド事業者は、本サービスの提供にあたり用いられている当社の設備のうち当社が製造したものではないソフトウェア及びデータベースに起因して利用者に生じた損害については、責任を負わない。」と規定されるのが通例です。このような場合には、クラウド事業者に対してソフトウェアや、インフラ環境　を提供している事業者の落ち度でサービスに不具合が生じた場合でも、利用者と契約しているクラウド事業者は責任を負わないので、注意が必要です。

4.4.4. サービスレベル合意（SLA）の考え方

SLA とは、利用者に提供されるサービスの品質・レベルを規定するものです。クラウド利用契約と別立てで定められることも、クラウド利用契約内に定められることもありますが、いずれにせよクラウド利用契約と一体となって契約を構成します。したがって、クラウド事業者が SLA において満たすべき義務として規定されたサービスの品質・レベルを満たすことができなかった場合は、契約違反の問題となります。もっとも、SLA には、クラウド事業者の努力目標として定められたもの（努力義務規定）も含まれています。もし、クラウド事業者が SLA に定められたサービスの品質・レベルを満たすことができなかったとしても、それが努力義務規定により定められたものである場合には、当該サービス品質・レベルの不達成が直ちに契約違反の問題を惹起することはありません。しかしながら、この場合にも、クラウド事業者には、当該サービス品質・レベルの達成のための努力をすべき義務があり、仮にクラウド事業者がこのような義務を果たしていない場合には、そのことが契約違反の問題となることがあります。

4.4.5. 契約や約款における推奨事項

契約書の具体的な項目例とその目的・内容について、詳細は章末の Appendix A「契約の具体的な内容例と解説」をご覧ください。また、SLA については、章末の Appendix B「SLA に関する解説と例示」をご覧ください。

4.5. インシデントに備えた準備と対応

クラウドサービスの利用においては、自己保有のシステムでの IT サービスと違い、手元に資産や情報がないことによってインシデント時の対応も異なります。

4.5.1. データのバックアップ

一例として、データの喪失時の対応を検討してみましょう。

クラウドサービスの利用において、利用者はハードウェアを保有してなくても良いという反面、システムやデータの復旧をハードウェアレベルでできないという問題もあります。手元のマシンであれば、ハードディスクのクラッシュなどでデータを失った場合でも、何らかの手法で復旧することは容易なように思えます。それでも障害発生の可能性はあり、常にバックアップや遠隔保管などの措置を講じます。この考え方はクラウド上のシステムでも大きな変化はありません。したがって、バックアップなどの措置を、誰が、どのように実施し、また、どのような可用性や稼働実績を持ったインフラを使うのか、充分確認する必要があります。

4.5.2. システムのバックアップ

データのみならずシステムのバックアップも重要な事項です。この点においてクラウドは、手元に置いたシステムと比べて圧倒的に利便性が高いのが特徴です。ほぼすべてのクラウド事業者（PaaS、IaaS）が、容易にバックアップ（マシンイメージ、スナップショットなど）が取得可能な仕組みを用意しています。また、SaaS については、そもそも利用者においてシステムのバックアップを検討する必要がありません。

PaaS、IaaS の利用者においては、システムの運用において、誰がどのようなタイミングで上述のようなバックアップを取得しているか、確認すべきです。必要に応じ、一時的にコンピュータリソースを借りるなどして「バックアップからの復旧」の演習をすることも好ましいと言えます。

4.5.3. 他の事業者との契約

システムやデータセンタの冗長化を図ったとしても、単一のクラウド事業者のサービスの範囲内で行うのは不安だという考え方もあるでしょう。特定の事業者のあるサービス全体が損壊するケースや、あるいはその事業者がクラウド事業そのものから撤退するリスクを懸念する人もいます。ここまで考えるのであれば、複数のクラウド事業者にまたがる「マルチクラウド」構成も検討することになるでしょう。

マルチクラウドを検討するにあたっては、事業継続管理手続きに基づくことは当然ですが、技術的にはデータやシステムの移行のしやすさや、様々なコスト増などを勘案して選ぶことになります。

ただし、二重三重の措置を講じても、リスクをゼロにすることは不可能です。最終的にはコストとの兼ね合いで、どのレベルのリスクまで受容できるか判断することになります。この点は従来のシステムと同様です。

4.5.4. その他のインシデントへの対応

一般的にクラウド事業者は、多数の利用者を対象として標準化されたサービスを提供しているため、個々の利用者に対してきめ細かいインシデントの対応をすることは必ずしも容易ではありません。したがって、インシデント発生時に個別に即時のレポートを求めたり、障害回復状況を小刻みに報告させるなどの（従来的な）対応を求めることは適切ではありません。

しかしながら、クラウド事業者の中には、高レベルのサポートサービスを有償ながら提供しているものもあり、システムの重要度などに応じて適宜検討することが推奨されます。

5. クラウド事業者のためのガイドライン活用

5.1. 事業者におけるガイドラインの活用シーン

「クラウドサービス利用のための情報セキュリティマネジメントガイドライン」は、「利用者のための」と銘打たれています。このため一見すると、クラウドサービスを提供する事業者側には関係ないガイドラインに思えます。しかし、クラウドセキュリティガイドラインには、クラウドサービスを提供する事業者側にとって有用な情報が数多く記載されています。その理由は、クラウドサービスは多数の不特定の顧客に安心できるサービスを提供してこそ成り立つビジネスだからです。もともとクラウドセキュリティガイドラインが策定された目的は、利用者側にクラウドサービスを安全に安心して使うための指針を提示し、その結果、クラウドサービスの利用を促進することです。

クラウドセキュリティガイドラインが発表された平成 23 年当時に比べれば、多くの団体・企業でのクラウドサービス利用意向が高まり、着実にクラウドサービスの利用が拡大していますが、それでも日本国内での実際の普及率は 20%前後と言われています。

それではなぜ、企業や団体はクラウドサービスを利用しないのでしょうか？　その 1 つの要因としてクラウドサービスにおける情報セキュリティに対する懸念が挙げられます。

なぜ利用者側が懸念を抱くのか？　その原因を掘り下げると大きく以下の 3 つに集約されます。

1) 情報セキュリティポリシとの不整合
2) ハードウェアを保有、管理、運用できないことへの不安
3) 情報を他社に預けることへの不安

顧客となる利用者組織は、それぞれに情報セキュリティポリシや個人情報保護ポリシを策定し、それに基づいた IT システムの運用を実施しています。そしてその基礎となる規格が ISMS です。

ISMS は ISO/IEC 27001 を日本語化した JIS Q 27001:2006 を規範として審査・認証される情報セキュリティ認証資格です。認証取得の有無を問わず委託元とのサプライチェーン関係なども考慮しており、今日の日本では、多くの企業において情報セキュリティの規範のベースになっているといっても過言ではないでしょう。

ISMS という規範がありながら、なぜ情報セキュリティへの懸念がクラウドサービス利用の阻害要因となるのでしょうか？

それを理解するためには ISMS の制度設計そのものが持つ特徴を理解する必要があります。

第一に ISMS は情報セキュリティのマネジメントの考え方を表したもので、情報セキュリティのレベルを定義するものではありません。セキュリティのレベルは各組織で決定するものなのとなっています。このため、ISMS には情報セキュリティ保護にかかわる具体的な対策手法や手順については規定されていないのです。このために各組織では JIS Q 27001 及び実施規範となる JIS Q 27002 に記載された管理項目とその目的に応じ、それぞれに管理策を定義し文書化しています。ISMS 認証とは、これらの管理策が定義され、その PDCA が正しく回っているかを審査しているものに他ならないのです。

これらの前提に加え、JIS Q 27001 及び JIS Q 27002 がベースとなった ISMS はコンピュータシステムなどの IT 資産を「所有」することを前提として作られた規格です。ハードウェアやソフトウェアを「利用」するクラウドサービスでは、従来の ISMS の実施規範をそのまま適用できないことになります。これらの要因から、利用者組織においてクラウドサービス利用を検討する際に、情報セキュリティポリシとの不整合を生み出し、コンピュータシステムを所有しないことに対する不安を生み出すことになります。このギャップを埋めるための対策をまとめた文章がクラウドセキュリティガイドラインなのです。

したがって、クラウド事業者側では利用者の不安を解消し、より多くの利用者を獲得していくためにも、クラウドサービスの構築時点でクラウドセキュリティガイドラインに記載された「目的」と「管理策」に応じた「クラウドサービス事業者が実施すべき事項」を実装することを念頭におき、その事実について利用者側に適切に情報提供することが大切な対応となります。

5.2. クラウドサービスの構築

クラウド利用者組織が、クラウドセキュリティガイドラインを参照し ISMS の取得を行い、継続して PDCA サイクルを実施していくことを前提としてクラウドサービスを構築する具体的な事例や方法をご紹介していきます。

クラウド事業者として実施が望まれる管理策が記載されている箇条はクラウドセキュリティガイドラインの 5～15 となります。これらの箇条はクラウド利用者が JIS Q 27002（実践のための規範）の箇条 5～15 の管理策を実施するための補足として活用できるように、次のような構成となっています。

目的 JIS Q 27002（実践のための規範）における目的がそのまま引用されています。 管理策

JIS Q 27002（実践のための規範）における管理策がそのまま引用されています。

クラウド利用者のための実施の手引

クラウドサービス利用者が管理目的を満たすために実施することが望まれる管理策や情報が記載されています。

クラウド事業者の実施が望まれる事項

クラウドサービス利用者が情報セキュリティ対策を行うためにクラウド事業者の協力が必要となる管理策についてクラウド事業者の実施が望まれる事項にかかわる情報が記載されています。

クラウドサービスの関連情報

クラウドサービス利用者がクラウドサービスを利用する際に考慮が必要と思われる関連情報（関連するクラウドサービスの種類，利用環境又は利用技術に関する情報など）が記載されています。

なお、いずれの項目でも、クラウドサービスに固有の事項が存在しない場合には記載がありませんが、一般的な管理対策として参照し、クラウドサービスの実装に反映した方が適切な項目については反映するようにし、情報公開を実施してください。

では、実際の箇条 7「資産の管理」をサンプルに実装の検討と実装例の提示を行ってみます。箇条 7 の目的と管理策は以下の通りとなっています。

7.資産の管理

7.1　　資産に対する責任

目的：組織の資産を適切に保護し，維持するため。

すべての資産を明らかにし，その管理責任者を指名することが望ましい。

管理責任者をすべての資産について明確にし，適切な管理策を維持する責任を割り当てることが望ましい。組織が適切と判断した場合には，管理責任者は具体的な管理策の実施を委任してもよいが，資産の適切な保護に関する責任は管理責任者にとどまる。

7.1.1　　資産目録

管理策

すべての資産を明確に識別し，また，重要な資産すべての目録を作成し，維持することが望ましい。

ここまでの目的と管理策は「JIS Q 27002（実践のための規範）」がそのまま引用されていますが、クラウド事業者が利用者に対してすべての資産を明らかにすることは事実上不可能です。したがって、この管理目的を達成するために管理策にクラウド固有の事項が記載される形となります。

クラウド利用者のための実施の手引

クラウド利用者は，クラウドコンピューティング環境にある組織の資産を資産管理の適用範囲に含めることが望ましい。クラウド利用者は，資産目録にクラウドサービス名及びクラウド事業者名を追加することが望ましい。

クラウド利用者は，クラウド利用者による資産管理を支援する機能がクラウドサービスに付帯するかを確認することが望ましい。

クラウド利用者側は「どの会社が運営している」「どのクラウドサービス」に「何を預けて（利用して）」いるかを目録化することが望まれる対応として定義されています。

したがって、クラウド事業者側はクラウド利用者が資産目録の作成を行いやすい仕組みをサービスに実装することが求められることになります。これが「クラウド事業者側の実施が望まれる事項」の項目となります。なお、「7.1.1 資産目録」の項目では以下の記載となっています。

クラウド事業者の実施が望まれる事項

クラウド事業者は，クラウドコンピューティング環境にあるクラウド利用者の資産に関する資産目録の一覧が取得できる機能をクラウド利用者に提供することが望ましい。

例えばIaaSにおいてはダッシュボードと呼ばれるサーバやストレージなどの利用機能一覧、SaaSにおいては登録情報の見出し一覧と情報件数などが一覧視できるインタフェースを実装することが望まれているということが分かります。 このようにクラウドサービス構築時に「クラウド事業者側の実施が望まれる事項」で記載された事項を実装していくことでクラウド利用者組織の不安や懸念事項を1つ1つ減らしていくことが可能となります。

図 15 クラウドサービスのダッシュボード

なお、クラウドサービスの提供種別によっては、事業者として望まれる実施内容が異なることも想定されます。このような場合には「クラウドサービスの関連情報」の項目に付随情報が記載されていますので、提供しているサービス内容によって対策を行う際の参考資料としてください。

クラウドサービスの関連情報

クラウド事業者は大規模な IaaS の上で PaaS や SaaS を展開している場合があり，クラウド利用者がクラウドサービスに関連するシステムのすべてを資産目録に詳細に記載することは困難である。また，データ管理のために様々なメタデータ（データに関する情報）などが付与されており，これらのすべてをクラウド利用者が管理することも困難である。しかしながら，クラウド利用者は，自らがクラウドコンピューティング環境

においたデータやプログラムなどを資産目録に記載することは可能であり，これらをもれなく記載することが期待される。

上記の関連項目の解説では、クラウドサービスが利用するサプライチェーンの把握などが難しく、利用するクラウドサービス名や事業者名を特定することが難しい場合にも、クラウドサービスに預けたデータを資産として取り扱い、データの目録を作成することで管理目的を達成することも可能であることが記載されています。

これらの項目の記載を理解し、実際のクラウド利用者がクラウドセキュリティガイドラインを利用して ISMS 認証を受けることを想定した機能の実装や情報の開示も大切です。下の図は EC 事業者（店舗主）が本ガイドラインを利用した場合に必要となるであろう情報の例をマッピングしたものです。

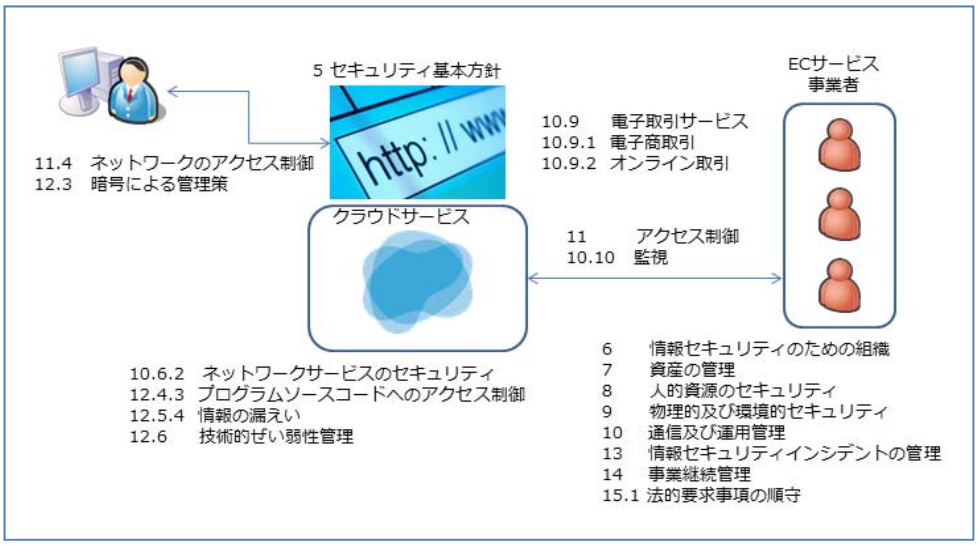

図 16 EC 事業者から見たクラウドセキュリティガイドラインの適用事項の例

クラウド事業者として必要な対策は、EC 事業者が利用するに足るクラウドサービスであるための必要な要素を実装し、そしてその情報を開示する必要があるということです。

上の図でクラウドサービスと EC 事業者を結ぶ箇所で例えるならば、EC 事業者がクラウドサービスを利用する際のアクセス制御、例えばアカウントの管理機能が実装されており、権限設定（アカウントロール）などが実装されているか、またアクセス経路上の暗号化の手法や専用線・閉域網・VPN などのアクセス制限手段が存在するか、操作ログが残されているかなどの情報が EC 事業者側にとって必要であることが分かります。

同様にユーザ（購入者）から Web 公開画面へのアクセスにおいては不正侵入の探知を行う IDS（Intrusion Detection System）機能や意図しないポートへのアクセスを制限するファイアウォール機能の有無、Web サイトの脆弱性の対策や情報の改ざんを図る行為を防御する WAF（Web Application Firewall）の有無なども実装が望まれる項目といえるでしょう。

上記ではクラウド利用者が EC サイトを構築し運営する例を挙げ、その一部の問題について実装対策の一例を述べましたが、多種多様な利用目的・ユースケースについてクラウド事業者側がすべてを対応し、情報をユースケースごとに公開していくことは大変困難な行為といえます。したがって、細目については各クラウド利用者に個別に判断していただく方式が現実的な対応となります。この際、クラウド事業者がクラウドセキュリティガイドラインの各項目についての実装を情報公開することで、クラウド利用者側が自ら均一の尺度で複数のクラウドサービスを比較することができるようになります。

5.3. セキュリティホワイトペーパーの活用

クラウドサービス利用者の不安や懸念を解消することが、クラウドサービスの利用者拡大につながる大きな要因であることをここまでご説明してきました。クラウド事業者にとっては、多大な努力で対策を施していても、利用をご検討いただいている方々に情報が届かなければ意味がありません。このような観点から、しっかりと情報セキュリティ対策を実施しているクラウド事業者であればあるほど、情報を開示すべきだと考えます。

開示方法として主にホワイトペーパーの公開、チェックリスト、外部監査・認証の取得の 3 方式があります。

それぞれの方式には一長一短があります。例えばホワイトペーパーでは、クラウドサービスへの実装状況をクラウド事業者自らが開示する方式ですから、事業者にとってはコストが低減されるメリットがあります。反面、利用者にとっては、情報の信ぴょう性を担保するに値する根拠をどのように確保するのかが問題となります。また、クラウド事業者として情報を公開する範囲を適切に定義して、利用者が必要とする情報を提供する必要性が生じます。

チェックシート方式では、利用者が提示するチェックシートに対して事業者が回答する場合（利用者側の様式に従う方式）と、事業者側が自らチェックシートを開示する場合（事業者側の様式に従う方式）があります。事業者側が自らチェックシートを開示する場合には信頼性の担保が課題となります。利用者が提示するチェックシートに事業者が回答する場合、事業者側における個別対応が都度生じ、チェックシートに回答できる専門知識を持つ人員の確保など人的工数の負担がかかる反面、利用者側からは高い満足感を得られるメリットがあります。この場合にも信頼性を確保するための根拠は明らかにする必要は生じます。

外部監査方式は第三者による外部監査を受けるものですから、利用者側の立場からは高い信ぴょう性を得られる反面、事業者側では、監査にかかるコストや工数が必要となるデメリットが生じます。SOC3（WebTrust、SysTrust）などの監査認証資格も存在します。

いずれの方式を採用するのかの判断は、想定される顧客や顧客の取り扱う情報が要求する機密性のレベルなどによって判断すると良いでしょう。

5.3.1. 国内のセキュリティホワイトペーパーの事例

クラウドセキュリティホワイトペーパーは、事業者側がクラウドサービスに実装する各種のセキュリティ対策を利用者側に詳細な内容とともに説明できる方式です。自己言明方式の一種となります。

クラウドセキュリティガイドラインでクラウド事業者の実施が望まれる事項とされている項目や付属書 A に記載されるクラウドサービス特有の利用者から判断できない事項について説明を行う冊子式のセキュリティの取り組みの紹介となります。

事業者が自ら情報を詳細に開示することで、利用者側からの信頼感を得ることが可能となります。クラウドセキュリティホワイトペーパーの書式などは特に定義されていません。セキュリティホワイトペーパーは、クラウドサービス構築時にはぜひ作成し、公開して欲しい情報です。

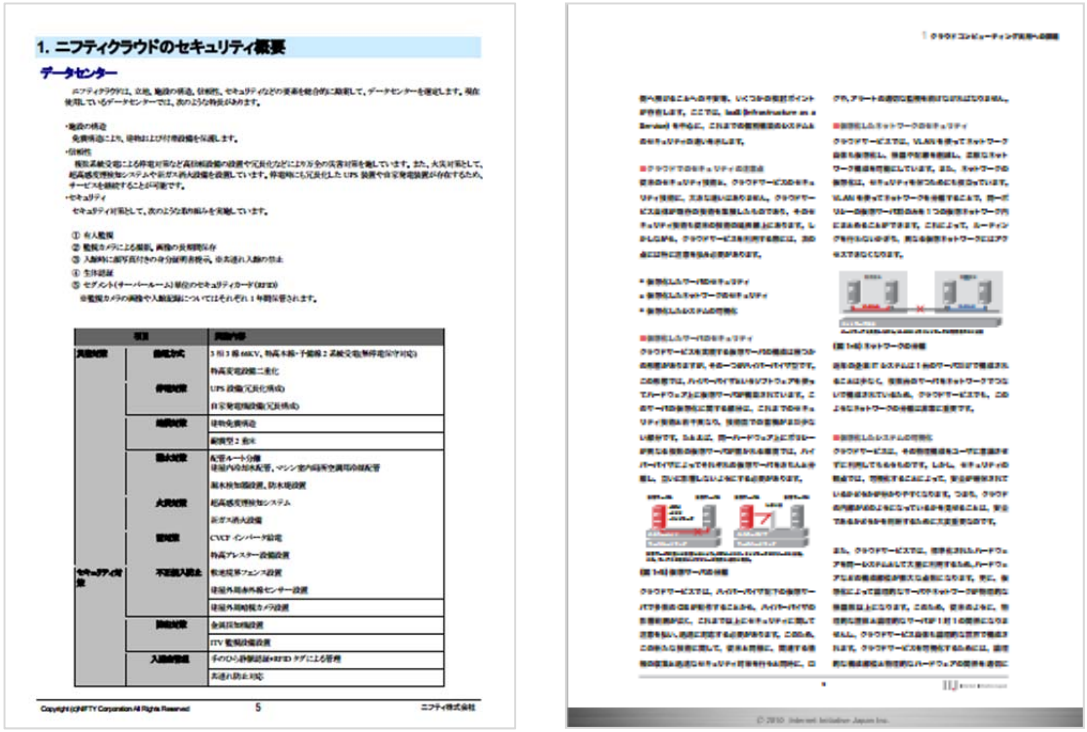

図 17 国内ベンダのホワイトペーパーの例

左：ニフティクラウドのセキュリティホワイトペーパー
http://cloud.nifty.com/pdf/security_whitepaper.pdf

右：IIJ GIO のホワイトペーパー
http://www.iij.ad.jp/GIO/wp/pdf/wp02.pdf

5.3.2. 海外のセキュリティホワイトペーパーの事例

グローバルに展開している外資系のクラウドサービスを利用する場合には、「クラウドセキュリティガイドライン 15.1 法的要求事項の順守」に記載の通り、クラウドサービスの裁判管轄及び適用を受ける法令・規制を確認・文書化し、最新に保つことが望まれます。これは国内の SaaS 事業者が国外のクラウド事業者が提供するクラウドサービスを利用している場合にも同様で、クラウド事業者はクラウド利用者との合意に基づいて

法令、規制及び契約上の要求事項が適用される地理的場所にクラウド利用者のデータが保持されていることを確実にし、法的要求事項の順守を監視する必要が生じます。

これらの問題は日本のみならず、すべての国において ISMS の実施規範で問題になりますから、ドメスティックに展開する国内事業者に比べ、外資系のクラウド事業者ではセキュリティホワイトペーパーをはじめとする方法により、きめ細やかな情報提供が実施されています。残念ながら多くの場合には日本語ではなく英語による情報提供となっていますが、データを預けるクラウド事業者の情報を閲覧し、法令や規則、または組織で規定する情報セキュリティポリシに反しないかを確認することは大変重要です。

また、今後、海外での事業展開を検討しているクラウド事業者はこれらの先行事例を参考にグローバル展開にふさわしい情報開示の体制を検討してください。

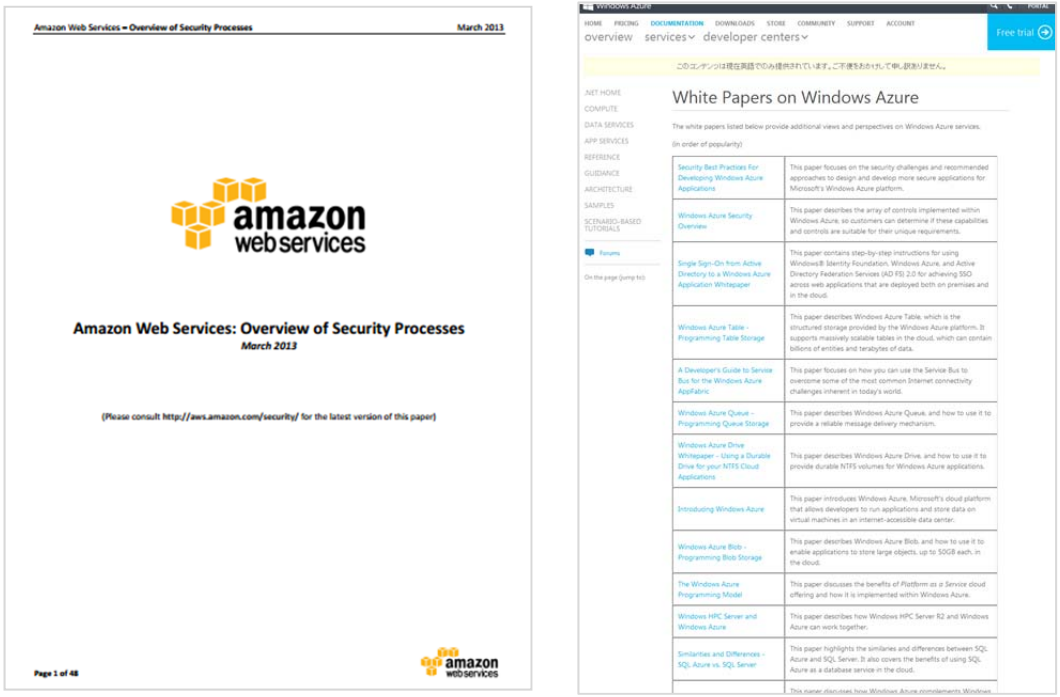

図 18 海外事業者のホワイトペーパーの例

左：Amazon Web Services: Overview of Security Processes
http://awsmedia.s3.amazonaws.com/pdf/AWS_Security_Whitepaper.pdf

右：White Papers on Windows Azure
http://www.windowsazure.com/en-us/develop/net/other-resources/white-papers/

5.3.3. その他の情報発信

クラウド事業者における定期的な情報セキュリティの実施状況の報告や処理能力の報告なども、クラウド利用者が IT サービスマネジメントや情報セキュリティマネジメントを適切に行う上で重要な判断材料となります。

チェックリストによるセキュリティ関連情報提供

セキュリティチェックリストを作成し公開することもホワイトペーパーと同じ自己言明方式の一種です。クラウド事業者の立場でサービスを運営・提供していく上で、よく問い合わせを受ける項目などを予め公表しておくことで、問い合わせへの対応負荷を減らす効果を期待でき、さらに、クラウドサービスへのセキュリティの取り組みをアピールできるなど、利用者側からの信頼度や満足度の向上も図ることができる手法です。

チェックリストの実装例としては、グローバルなクラウドセキュリティ監査の利用促進有識者会議でサンプルが提言され公開されています。

○○○○年○月○日作成

クラウドサービスにおける情報セキュリティ対策に関するチェックリスト（記入済み例）
対象：Aサービス（X株式会社）

番号	リスクの種類	事業者による説明（実施している対策の概要）	利用者記入欄	
			判断	判断の根拠
H01	クラウドサービスにおける資産集約化がもたらす悪影響	何らかの異常や大災害が生じた場合でも、サービスの全面停止を防ぐため、地理的に離れた3箇所以上の拠点でサービスを提供しています。いずれかの拠点が稼働していればサービスの継続が可能です。	○	対策として適切と判断。
H02	クラウドサービスを構成する仮想システムで障害が発生することによる被害	機器の障害や操作ミスがサービスに影響を及ぼさないようにするため、自動監視システムを実時稼働し、異常の早期検知を図るとともに、仮想システムで異常が生じにくくなるような設計を行い、厳格なテストを通じてその効果を検証済みです。	○	自社運用よりも障害可能性は低いと見込まれることから、適切と判断。
H03	クラウドサービス内の他利用者の活動による悪影響	パブリッククラウドサービスの性質上、他のお客様の活動による影響を完全に排除することは困難です。他利用者の影響が気になるお客様にはプライベートクラウドサービスをお勧めしております。	×	他利用者の影響を受けることは避けたいが、コスト的にプライベートクラウドの利用は困難。
H04	クラウドサービスの提供に必要な資源の枯渇による被害	通常の利用ではお客様が必要とされる資源が不足する心配はございませんが、万一不足となった場合はサービス約款に基づく対応をさせていただいております。	○	これまでのX社の運用実績から障害可能性は低いと判断。
H05	クラウドサービスにおいて他利用者が自分のデータにアクセスすることによる被害	お客様毎にデータは完全に隔離されています。この隔離が失われることのないよう、弊社の情報セキュリティポリシーのもとにシステムの脆弱性対策を実施するとともに、不正アクセスの早期検知のための監視システムを実時稼働させております。	○	これまでのX社の運用実績から障害可能性は低いと判断。
H06	クラウドサービスの基盤インフラへの攻撃がもたらす被害	Aサービスの基盤インフラは、お客様用の通信回線とは別の回線を通じて管理しており、外部からの攻撃を困難にしております。さらに、弊社の情報セキュリティポリシーのもとにシステムの脆弱性対策を実施しております。	○	これまでのX社の運用実績から障害可能性は低いと判断。
M07	クラウドサービス事業者内での内部不正による被害	Aサービスの運用に係る操作はすべて記録されており、運用担当者はその記録を停止したり、改ざんすることができない仕組みとなっております。こうした仕組みと監視体制により、内部不正を行うことは困難です。	○	これまでのX社の運用実績から障害可能性は低いと判断。
M08	クラウドサービスの管理用システムが不正利用されることによる被害	Aサービスの基盤インフラは、お客様用の通信回線とは別の回線を通じて管理しており、外部からの攻撃を困難にしております。	○	これまでのX社の運用実績から障害可能性は低いと判断。
M09	クラウドサービスと利用者の間の通信回線上での攻撃による被害	オプションのVPNサービスをご利用いただくことで、お客様との通信回線におけるデータの暗号化が可能となっております。	○	オプション利用により対策可能と判断。

図 19 監査に利用するチェックリスト

出典：平成２３年度企業・個人の情報セキュリティ対策促進事業（グローバルなクラウドセキュリティ監査の利用促進）

このチェックリスト案はクラウドサービスで想定される典型的なリスクをチェックリスト化したもので、クラウドセキュリティガイドラインの「附属書 A（参考）クラウドサービス利用にかかわるリスク」と「附属書 B（参考）クラウドサービス利用におけるリスクアセスメントの実施例」に記載されたクラウド特有のリスクに基づいて作られています。したがって、チェックシートは付属書 A で定義されたリスクに対する回答ができているか、また、クラウド利用者が付属書 B にしたがってリスクアセスメントを実施する際に過不足のない情報が記載されているか記載内容には確認が必要です。

処理性能・パフォーマンス情報の開示

クラウドサービスはサービスを構成するシステムのセキュリティだけでなく、稼働性能に関する特性も、契約前の利用者側からは一定の尺度で評価するのは難しいため、クラ

ウド利用者側の動作に密接にかかわる処理性能に係る一定の情報は契約前に開示すべき情報であるといえるでしょう。

例えばハードディスクドライブは、従来、接続方式や読み書き速度の尺度を表す rpm などの数値が諸元として公開されていました。しかし、クラウドサービスでは容量は開示されていても速度の基準は公開がなされていない場合がほとんどです。しかし、RDBMS 利用など利用用途によって速度性能の情報が必要となる場合がありますので、クラウド利用者目線からは、性能面に関する情報の開示も望まれる対応の 1 つです。

ストレージタイプ	ディスクストレージ		オブジェクトストレージ
適応データ	Disk200：DBなどオンライン用 Disk40：アーカイブ用		バックアップ、ログなどコールドデータ
サイズ	100GB～最大2TB(Disk40) 1VMにつき4台まで利用可能		1GB～無制限
課金方式	容量×期間(月額・従量)		月内最大利用容量
利用方法	同一リージョン内にある ニフティクラウドのVMにマウント 複数のVMでの共有利用はできない		REST APIによるhttp/https通信 インターネット経由でどこからでもアクセス可能
料金	4,000円～/月(Disk40) 5,000円～/月(Disk200)		11円～/GB/月
データ保護	RAID6相当		RAID6相当
データロスト実績	なし		なし
速度(参考値)	Disk40	Read 200MB/s Write 7MB/s	外部からのアクセス 10MB/s
	Disk200[A/B]	Read/Write 200MB/s	ニフティクラウド上のサーバーからのアクセス 50MB/s

図 20 国内事業者のストレージ種別による性能種別

5. 4. 第三者認証の活用

クラウドサービスのセキュリティ対策の実施状況について第三者認証を得る形で証明や保証を実施する方法も存在します。第三者の専門家による監査を伴うため、利用者にとっては高い信頼感を得ることができる反面、クラウド事業者側にとっては金銭的なコストや監査にかかる工数などがかかる方式です。

代表的な第三者認証として ISMS 認証（JIS Q 27001）やプライバシーマーク（JIS Q 15001）などの情報セキュリティマネジメントに係る認証や、個人情報や取引情報などを含むクレジットカード情報の取扱いを規定した PCI DSS、品質マネジメントシステムである QMS（JIS Q 9000）、IT システムマネジメントにかかわる ITSMS（JIS Q 20000）など、管理目的に応じた多様な認証が存在します。

また、内部統制評価保証を行う SOC1、2 及び 3 が存在します。SOC1 は実務指針第 86 号監査「受託業務に係る内部統制の保証報告書」や ISAE 3402（旧 SAS70）に該当する認証で保証内容は財務内容に関する内部統制に限定されています。SOC2 及び 3 はセ

キュリティ、可用性、処理のインテグリティ、機密保持、プライバシなど財務内容以外の内部統制への保証内容に含まれる監査となっています。

SOC2 と SOC3 の大きな違いは SOC2 が利用者を限定するのに対し、SOC3 は不特定多数の利用者に開示できる内容となっている点にあります(SysTrust、WebTrust など)。

いずれも組織単位で取得する認証であり、クラウドサービスそのものの安全性を直接的に保証するものではありませんが、ISMS や P マークなどの公的認証を取得している場合には取得認証資格を開示することも信頼性の向上につながる活動といえるでしょう。

なお、外資系を含む国内の代表的な事業者における取得情報を公開情報から検索したところ以下の通りの取得状況となっています。しかしながら国内事業者において取得認証を Web などから一覧で閲覧できるインタフェースを提供している事業者はほぼ存在せず、対して外資系事業者は英語のみで提供されている情報が多いものの、利用者に分かりやすく一覧化されたページが配置されており、各クラウド事業者においても、一覧化や分かりやすいリンクなど良い点は取り入れるべきであるといえるでしょう。

事業者名	IIJ	ニフティ	NTT コミュニケーションズ
サービス名	IIJ GIO	ニフティクラウド	クラウドエヌ
ISMS 認証	○	○	○
プライバシーマーク	○	－	○
PCI DSS	○	○	－
内部統制評価保証	SSAE16 Type2	－	－
その他	－	－	ISO/IEC 20000 など
公開ページの有無	なし	あり	なし

図 21 国内クラウド事業者の第三者認証取得事例

事業者名	マイクロソフト	グーグル	アマゾンウェブサービス
サービス名	Windows Azure	Google Apps	Amazon Web Services
ISMS 認証	○	○	○
プライバシーマーク	－	－	－

PCI DSS	○	○	○
内部統制評価保証	SSAE16 / ISAE 3402	SSAE 16-2 / ISAE 3402	SOC 1/SSAE16 / ISAE 3402 / SOC 2 / SOC 3
その他	EU Model Clauses / HIPPA	FISMA	FISMA / DIACAP FedRAMP / HIPPA
公開ページの有無	あり	あり	あり

図 22 海外クラウド事業者の第三者認証取得事例

多くの事業者が取得しているのが、ISMS 認証です。経済産業省が 2010 年に実施したアンケートでも、クラウド利用者が事業者に望む第三者認証としてトップに挙げられていたのが ISMS 認証でした。このような要望を実現しつつ、競争力の確保のために様々な認証を取得しているというのが現状のようです。

クラウド事業者もその上でサービスを構築するベンダも多くの場合はクレジットカードでの決済を行っていますので、PCI DSS 認証を取得したり、業界の要求事項として海外ベンダでは HIPPA や FISMA などを取得したりしています。

それぞれのサービスではサービスの紹介ページなどで第三者認証の取得状況を公開していたり、会社案内やホワイトペーパーなどに記載しているなどして、事前に利用者が情報を取得できるようにしています。

ただし、情報が分散していると利用者に分かりにくいということもありますので、必要な情報をまとめて掲載しておくことも重要です。

5.5. 監査の活用

5.5.1. 内部監査の活用

クラウドサービスのセキュリティへの取り組みを対外的に公表する活動は、利用者拡大につながることが期待されます。しかし、クラウドセキュリティガイドラインをベースとする ISO/IEC 27017 の運用は 2015 年からの予定であり、クラウド事業者が公的にセキュリティへの取り組みについて認証を受けるためには、SOC2 など事業者側の負担が大きい方式を取らざるを得ない状況です。

そこで、中小規模のクラウド事業者にも負担が少なく、かつ、利用者に対して適切なセキュリティ対策の実施を一定レベルで担保できる方法が、クラウドセキュリティガイドラインを利用した定期的な内部監査の実施と、その情報のホワイトペーパーやチェックリストによる公開です。この方法を上手に活用することで、事業者の負担を減らしながら利用者の望むセキュリティレベルを利用者自らのサービス選定にも活かしてもらえるようになるでしょう。

クラウドセキュリティガイドラインを活用した内部監査とはいえ、利用者への安全性を担保するための活動ですから、本来は情報セキュリティに関する監査のトレーニングや資格を取

得した監査人による監査の実施が望まれますが、監査人が所属しない組織でもクラウドセキュリティガイドラインを活用した監査が実施できるよう簡易的に一般的な内部監査の流れを例示します。クラウド事業者のみなさんは、ぜひクラウドセキュリティガイドラインを活用した内部監査を行ってみてください。

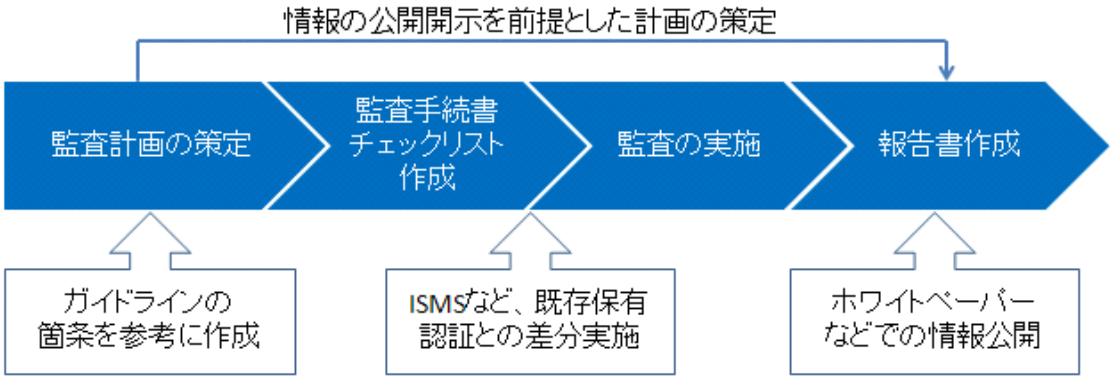

図 23 内部監査のフェーズ

監査計画の策定方法

まず初めに実施するのが「監査計画書」の策定です。なぜ内部監査を実施するのか、その目的や対象のサービス、実施時期や実施方法などを定義します。内部監査であってもクラウドサービスを運用する様々な人員や組織の協力が必要となりますので、まずは計画書を策定し、関係する人員からの理解を得るようにしてください。

１．監査の目的
　　→利用者へ安全なサービスを提供し信頼を高めるため、など目的を記載
２．監査対象とする範囲
　　→内部監査を実施するサービス名、など
３．監査の判断の基準等
　　→クラウドサービス利用のための情報セキュリティマネジメントガイドライン
４．監査対象とする期間又は期日
５．監査対象とする段階
　　→バージョンなどが存在する場合に記載する
６．監査対象に係る監査目標
　　→利用者へのチェックリストやホワイトペーパーによる情報開示のため、など
７．監査の重点項目
　　→例えば、クラウド特有の脅威に係わる部分のチェックなど、力を入れる点を記載
８．監査業務の管理体制
　　→内部監査を実施する体制を明らかにする
１０．監査スケジュールの概要
　　→予定している内部監査のスケジュールを明らかにする

図 24 監査計画書の項目案

監査手続書・チェックシートの作成

実際に監査する項目を定義し、どのような監査を行うかを決める書類の作成です。最終的にチェックシートの形式で利用者に開示する場合には、開示する情報を先に定義して、該当項目の情報を記載するようにすると良いでしょう。

クラウドセキュリティガイドラインの箇条「5 セキュリティ基本方針」から「15 順守」までの項目が基本的な項目設定のベースになりますので、表計算ソフトなどで表にしておくと便利です。なお、実際の監査技法として「質問（ヒアリング）」「観察（視察）」「閲覧（レビュー）」「再実施」がありますので、他の参考資料を参照しながら方法の記載もしておくと良いでしょう。

目的(箇条)	管理策	詳細管理策	事業者の実施が望まれる対応	監査技法	監査対象	結果
5 セキュリティ基本方針	5.1 情報セキュリティ基本方針	5.1.1 情報セキュリティ基本方針文書	情報セキュリティ基本方針をクラウド利用者に明示してい	観察	Webページ	○／×
		5.1.1 情報セキュリティ基本方針文書	第三者による評価結果（ISMS認証取得証明書、外部監査報告書及び内部監査報告書など）状況の明示	観察	Webページ	○／×
6 情報セキュリティのための組織	6.1 内部組織	6.1.2 情報セキュリティの調整	操作マニュアル及び連絡先情報を必要に応じて提供することが望ましい			
・ ・ ・	・ ・ ・	・ ・ ・	・ ・ ・	・ ・ ・	・ ・ ・	・ ・ ・
15 順守	15.1 法的要求事項の順守	15.1.1 適用法令の識別	クラウド事業を営む地域（国，州など），データセンターの所在する地域（国，州など）及びクラウド事業者自らが適用を受ける法令，規制及び契約上の要求事項の明示	観察 閲覧	Webページ 会社登記書類 関連法令書類 データセンター契約書	○／×
	・ ・ ・	・ ・ ・	・ ・ ・	・ ・ ・	・ ・ ・	・ ・ ・

図 25 監査手続書・チェックシートの例

上記の参考例からも分かる通り、目的や管理策、詳細管理策、そして事業者の実施が望まれる項目の多くはクラウドセキュリティガイドラインからそのまま引用することが可能です。

監査の実施

監査の実施は先に作成した監査手続書やチェックシートで定めた監査技法で監査対象を確認することにより実施します。証拠として確認した書類の名称や Web サイトの URL、ヒアリングした人の氏名及び役職名などを記録しておくようにしましょう。

報告書の作成

監査の実施が完了すると、最後は報告書の作成です。各項目の実施状況やその証拠などを記載した監査報告書を作ります。もともとの監査目的が利用者向けのセキュリティチェックシートの作成や公開であった場合には、監査結果に基づいてそれらの書類も併せて作成すると良いでしょう。

作成した監査報告書はクラウドサービスの責任者や担当者にもフィードバックし、修正すべき点は改善項目としてサービス向上の資料にすると、より良いサービスに成長していくことが期待されます。

なお、これらの情報開示の事例については本書「4.3 セキュリティホワイトペーパー」の項目で記載していますので、先行事例を参考にしてみてください。

ここまで、クラウド事業者内部に専門資格を保有した監査人が存在しない場合でも、クラウドセキュリティガイドラインに基づいたクラウドサービスの内部監査を行う方法を簡単にご案内してきました。ただし、本来、監査はそれが内部監査であったとしても実施方法も含め、専門的なトレーニングを経て、資格を取得している専門知識を持った人員が行うのが正しい姿です。今後、クラウドセキュリティガイドラインの国際標準化も予定されていることも踏まえ、専門知識をもった人材の育成や、可能な範囲での外部監査の実施や第三者認証の取得も検討してください。

6. その他の活用

6.1. クラウド監査人への活用提案

クラウドセキュリティガイドラインは先にご説明した通り、将来的に ISO/IEC 27017 として国際標準の規格になるものです。また、それは同時にクラウドを提供しているクラウド事業者が、またクラウドを利用している組織が ISMS（JIS Q 27001）の認証を受ける際に、27001 付属書 A を補完するものとして、クラウド固有の管理策として対応が必須な基準となることを意味します。

ISMS では、各組織が項目に沿った管理策を定めて実施し、各組織の定めた規定に基づいて正しく PDCA サイクルを回しているかを、審査員が内部監査などの証跡の閲覧や実施状況の観察などを通じ監査し、認証が行われます。したがって、ISMS とクラウドサービスの認証を将来的に考慮するならば、できるだけ早い段階でクラウドサービスの利用、またはクラウドサービスの提供に係る部分に関しては、クラウドセキュリティガイドラインを利用した管理策及び詳細管理策の制定と定期的な内部監査の実施が推奨されます。現段階から実行しておくことにより、2015 年以降に予定される 27001+27017 の認証を速やかに受けることができますし、なによりクラウド利用者からの信頼が高まり、クラウドサービスの拡販にもプラスに働くことでしょう。

ただし、大きな問題は ISMS 同様、クラウドセキュリティガイドラインには監査項目の設定や手法など監査手続きの具体例は記載されていません。その問題を補完するため、経済産業省では平成２３年度企業・個人の情報セキュリティ対策促進事業（グローバルなクラウドセキュリティ監査の利用促進）においてクラウドサービス利用を前提とした「クラウド情報セキュリティ管理基準」を策定しました。同管理基準は、日本セキュリティ監査協会のホームページからダウンロードすることができますので参照してみてください。

なお、この「クラウド情報セキュリティ管理基準」は一般に利用されている情報セキュリティ監査制度を活用して、クラウド事業者のセキュリティレベルに一定の保証を与えることによって、クラウドコンピューティングの普及・発展を促進するために経済産業省が策定したもので、情報セキュリティ監査制度における主体別・業種別管理基準のクラウドサービス業に向けて作られたものです。クラウド事業者は必要に応じて本管理基準の項目などを取捨選択、追加することによって、クラウド事業者またはクラウドサービスごとの管理基準を策定してください。

同様に、監査手続きについては「クラウド情報セキュリティ監査手続きガイドライン」の策定が進んでおり、2013 年中の公開が予定されています。検査技法などの監査手続きの実施方法や内部監査報告書の様式などは同資料の公開に合わせて参照してください。

6.2. クラウドサプライチェーン管理者への活用提案

クラウドサービスの普及に伴って新たに発生している問題がクラウドサプライチェーンです。

クラウドサプライチェーンとは、例えばクラウド利用者がクラウドブローカー（SIer、再販業事業者など）を介して SaaS サービスの利用契約を行ったとします。クラウド利用者は、クラウドブローカー、SaaS サービス及びその SaaS サービスを提供するクラウド事業者については契約段階での認知が可能です。ところがその SaaS サービスが第三者の PaaS サービスを利用して構築したものだった場合、クラウド利用者は意図せず PaaS サービスの利用者になっていることになります。さらに PaaS サービスが IaaS サービスを利用している場合もあります。またそれぞれのサービスがサービス構築に他の事業者の製品やサービスを利用している場合もあります。このような関係をクラウドサプライチェーンと呼びます。

図 26 クラウドにおけるサプライチェーンの考え方

クラウドサプライチェーンの大きな問題は、クラウド利用者から見た契約先に問題がない場合にも、配下に存在する PaaS や IaaS に問題が生じた際、連鎖的な問題に巻き込まれることです。一番の典型事例が障害によるサービス停止です。IaaS の障害が PaaS の障害につながり、SaaS の障害の原因となった場合でも、クラウド利用者からは SaaS の障害という認識となります。仮に障害が要因となり事業活動に何らかの損害が生じた場合、クラウド利用者は何らかの損害賠償を請求することが想定されます。その際に、責任を負う事業者は誰であるのかが問題となります。

クラウド利用者はクラウドブローカーに、クラウドブローカーは SaaS 事業者に・・・、という流れで損害が正常に補償されれば良いのですが、サプライチェーン階層が深ければ深いほど解決に時間がかかることになりますし、補償されないリスクも高まります。また間の事業者の経営体力などの問題からサプライチェーンの中にある事業者の事業継続が困難になってしまった場合には、サービス全体の運営継続が脅かされる場合もあります。システム障害と同様に、サプライチェーンに係るリスクの中には法律的な問題も存在します。法規制上の問題やクラウド利用者の情報セキュリティポリシなどから外国や外国法適用配下に情報を置いてはならないにも関わらず、サプライチェーンの配下

に該当する事業者が存在し、クラウド利用者の意図に反する状態に陥ってしまう可能性があります。

このような問題からクラウド事業者は自社の提供するクラウドサービスに関連するクラウド事業者やクラウドサービスについても、クラウドセキュリティガイドラインを活用した手法によって自社が提供するクラウドサービスと同等のセキュリティ監査とその状況の把握を継続的に実施すべきといえるでしょう。また、クラウド利用者に対しては契約前にクラウドサプライチェーンを構成する関連事業者の情報を監査状況とともに開示するなどの配慮も必要です。

情報セキュリティに関するリスクは、正常稼働している平時にはまったく問題にならないものがほとんどです。しかし万が一、何か問題が発生した際も、クラウド利用者側にもクラウド事業者自身にも耐えがたい大きなダメージとならないよう、万全の準備と対応を行うことがクラウド事業者として、サービスの継続や事業継続性を利用者に担保する重要な事項であるといえるでしょう。

7. 最後に

クラウドセキュリティガイドラインは、すでに国内だけでの利用にとどまらず、海外の政府や事業者からも注目されるものとなっています。

経済産業省としてもクラウド利用促進及びクラウド事業者の海外展開などを見据えた形でクラウドセキュリティガイドラインを定期的に更新しており、今後も最新のインシデントなどに備えた形で情報セキュリティ対策ができるガイドラインとして活用いただけるようにしていきたいと考えています。

クラウドセキュリティガイドラインが国際標準に先駆けて作成されたこと、海外の他のクラウドセキュリティ関連団体などに受け入れられていることなどをご理解いただき、ますますこのガイドラインを有効に利用していただけるよう、活用ガイドブックを策定いたしました。

新たなリスクに対応できるような事例集として活用いただければ幸いです。

8. 付録（Appendix）

8.1. Appendix A　契約の具体的な内容例と解説

（契約の成立）

１．利用者は、本利用契約の内容を承諾の上、当社が定める方法により申込みを行うものとします。 ２．当社は、第１項の申込みについて承諾する場合は、申込者に対し、承諾書をもって通知します。 ３．本利用契約は、承諾書を発送した日をもって成立するものとします。

【解説】

本条は、クラウド利用契約の成立について定めるとともに、クラウド利用契約の申込みについて定めた規定です。

消費者向けのクラウドサービスにおいては、申込みの方法として、ウェブサイト上の申込ページから申込ボタンをクリックすることを定めることもあります。この場合、クラウド事業者としては、消費者の申込みの意思表示の有無について確認を求める措置などを講じておく必要があります（電子消費者契約及び電子承諾通知に関する民法の特例に関する法律第３条参照）ので、注意が必要です。逆に、このような措置を講じておかなければ、消費者がクラウド利用契約の申込みを行う意思がなかったとしてクラウド利用契約の無効を主張した場合には、クラウド事業者は、これに応じなければならなくなります。具体的には、クラウド事業者としては、申込みの内容を明示し、そのボタンをクリックすることで、クラウド利用契約の申込みの意思表示となることを消費者が確認できる画面を設置するなどの措置を講じることが望ましいといえます。

（本サービスの利用料）

１．本サービスの利用料は月額〇円とします。 ２．利用者は、毎月月末限り、当社の指定する口座に振込送金する方法により、利用料を支払うものとします。なお、振込手数料は利用者の負担とします。 ３．利用者は、前二項の規定に違反して利用料の支払を遅延した場合、当社に対し、前項の定める支払日から支払済みまで年〇％の割合による遅延損害金を付加して支払うものとします。

【解説】

本条は、本サービスの利用料及びその支払方法などについて定めた規定です。

クラウド利用契約においては、クラウドサービスの実際の利用日数に応じて日割計算で利用料を定める例や、何らかの事情によってクラウドサービスを受けられない場合に利用料が減額されることを定める例もあります。利用料の支払義務は、利用者にとって、クラウド利用契約における中心的な債務になりますので、この点については、事前に十分確認しておく必要があります。

第3項は、利用者が利用料の支払を遅延した場合の遅延損害金について定めていますが、利用者が事業者ではなく消費者である場合、遅延損害金の割合の上限は14．6%となります（消費者契約法第9条第2号）ので、注意が必要です。なお、ここでいう「消費者」とは、個人（事業としてまたは事業のために契約の当事者となる場合の個人を除きます。）をいいます（同法第2条第1項）。

（本サービスの利用方法）

1．当社は、利用者に対し、本サービスを利用するために必要となるアカウント情報（ユーザID、パスワードその他本サービスを利用するために必要な情報をいい、以下「アカウント情報」といいます。）を提供します。 2．利用者は、アカウント情報を第三者に対して開示、貸与、共有せず、第三者に漏えいすることのないよう厳重に管理するものとします。アカウント情報の管理不備、使用上の過誤、第三者の使用などにより、利用者が損害を被ったとしても、当社は一切の責任を負わないものとします。 3．第三者が利用者のアカウント情報を用いて本サービスを利用した場合、当該第三者の行為は利用者の行為とみなします。ただし、当社の責めに帰すべき事由により利用者のアカウント情報が第三者に利用された場合はこの限りではありません。

【解説】

本条は、アカウント情報について定めた規定です。

アカウント情報は、権限のない第三者がクラウドサービスを利用することを防止するとともに、事業者が各利用者によるクラウドサービスの利用態様を把握するためにありますので、利用者としても、アカウント情報を適切に管理・使用する必要があります。

また、法人である利用者にクラウドサービスに関するトラブルが発生した場合、利用者は、クラウド事業者から関連するログ（記録）の開示を受けた上で、トラブルの原因を分析することになりますが、複数の従業員がアカウント情報を共有していると、ログ（記録）からクラウドサービスを利用した従業員を特定することができず、トラブルの原因究明に支障をきたすことになります。この点からも、アカウント情報の適切な管理・使用は重要となります。

（利用者データの取扱い）

1．当社は、利用者データ（利用者が本サービスに関して当社に提供する一切のデータをいいます。以下同じ。）の安全性、秘密性を保護するために、適切な措置を講じるものとします。 2．当社は、法令により強制される場合、本サービスの管理運営上やむを得ない場合または利用者から要求があった場合を除き、以下の各号に定める事項を行わないものとします。 (1) 利用者データへのアクセス (2) 利用者データの改変 (3) 利用者データの第三者への開示。

【解説】

第 1 項は、クラウド事業者が安全管理措置を講ずべきことを定めた規定です。クラウド事業者は、①サーバへのアクセス権限を有する従業員の限定（退職した従業員のアクセス権限を直ちに無効化する措置なども含まれます。）、②従業員によるサーバへのアクセス状況の監視、③ファイアウォールの設置、④安全管理に関する内部規程・マニュアルの作成、⑤サーバへのアクセス権限を有する従業員や委託先との秘密保持契約の締結、⑥従業員に対する安全管理に関する教育研修の実施など、各種の安全管理措置を講じなければなりません。利用者としては、クラウド事業者がどのような安全管理措置を講じているのか、SLA も併せて、事前に確認しておく必要があります。

第 2 項は、裁判官の発付する令状により強制処分として捜索・押収などがなされる場合、その他裁判所の判断または法令により強制される場合、サーバがウイルスに感染して管理運営上やむをえない場合など一定の例外的な場合を除き、クラウド事業者が利用者データへのアクセスなどを行うことを禁止した規定です。

（バックアップ）

利用者は、利用者データについては、本サービスの提供にあたり用いられている当社の設備の故障その他の理由による消失に備え、バックアップを取っておくなど、自らの責任と費用で必要な措置をとるものとします。

【解説】

本条は、クラウドサービスを利用するにあたり、利用者データのバックアップについては、利用者の責任と費用で行うべきことを定めた規定です。

もっとも、仮にこのような規定が設けられていない場合であっても、クラウドサービスにおいて利用者データが消失した場面において、利用者がデータ消失に供えてバック

アップを取得していないことは、利用者側の過失として考慮され（過失相殺）、利用者にとって不利に解される可能性があります。

（禁止事項）

１．利用者は、本サービスの利用に関し、以下の行為を行わないものとします。

(1) 当社または第三者の権利・利益を侵害する行為またはそれらのおそれのある行為

(2) 法令・条例などに違反する行為もしくは公序良俗に反する行為またはそれらのおそれのある行為

(3) 犯罪行為もしくはこれに類する行為またはそれらのおそれのある行為

(4) 他人のIDもしくはパスワードを不正に使用する行為、またはそれらに類似する行為

(5) 利用者のIDもしくはパスワードを他人に利用させる行為、またはそれらに類似する行為

(6) コンピュータウイルスなど、他人の権利・利益を侵害するまたはそのおそれのあるコンピュータ・プログラムを作成、使用、送信または掲載などする行為

(7) 当社または第三者の設備、通信に支障を与える行為またはそれらのおそれのある行為

(8) 前各号のほか、当社が本サービスの利用に不相当と判断した行為

２．利用者が前項で規定する禁止行為に該当する行為を行っていると当社で判断した場合、当社は、本サービスの提供を停止できるものとします。また、当社は、かかる利用者の行為により当社が被った損害について、利用者に対し賠償を請求することができるものとします。

【解説】

本条は、利用者が本サービスの利用にあたり禁止される行為を列挙した規定です。クラウド事業者や第三者の権利・利益を侵害する行為や、犯罪行為またはこれを助長する行為の他、同じサービスを利用する他の利用者に悪影響が及ぶ恐れがある行為（コンピュータウイルスの作成など）について一般的に禁止するのが通常です。

第 2 項は、利用者が禁止規定に違反した場合にクラウド事業者が採り得る措置を定める規定です。

（譲渡禁止）

利用者は、当社の書面による事前の同意を得ることなく、本利用契約上の権利もしくは義務または契約上の地位の全部または一部を、第三者に譲渡、移転、担保権の設定その他の方法により処分してはならないものとします。

【解説】

本条は、利用者によるクラウド利用契約上の権利義務の譲渡及び契約上の地位の移転を禁止する規定です。本条とは異なり、クラウド利用契約の中には、クラウド事業者による権利義務の譲渡の禁止についても明記するものや、譲受人がクラウド利用契約に拘束されることを条件として利用者による権利義務の譲渡を認める例もあります。利用者は、本サービスに係る権利義務または契約上の地位の移転を予定している場合には、クラウド利用契約上、いかなる範囲の譲渡や移転がクラウド事業者の同意を得ることなく可能とされているかにつき、事前に確認する必要があります。

（本サービスの一時的な提供停止）

1．当社は、次の場合には、本サービスの全部または一部の提供を一時停止することができるものとします。 (1)　当社の設備の保守または工事を行う必要があるとき (2)　当社または他の電気通信事業者の設備の障害などの発生またはその防止のためにやむを得ないとき (3)　当社の設備に不正アクセス、クラッキングなどの行為があったとき、またはこれらの行為が行われていると疑われるとき (4)　利用者が本利用規約に違反したとき 2．本サービスの提供を一時停止するときは、やむを得ない場合を除き、当社は利用者に対し、その旨とサービス提供停止の期間を事前に通知します。なお、本サービスの提供の一時停止により利用者に損害が発生した場合であっても、当社は一切責任を負わないものとします。

【解説】

本条は、クラウド事業者が一方的にサービスの提供を一時的に停止することができる場合について定めています。多くのクラウド利用契約において、設備の保守、工事などのサービスを停止する技術上の必要が生じた場合や、利用者が利用料の支払を遅滞した場合に、クラウド事業者は一方的にサービスの提供を一時的に停止することができる旨が定められています。技術上の理由に起因する一時的な利用停止が一定の確率で発生する

ことはやむを得ないとも考えられることから、利用者は、かかる事態を想定した上でサービスの利用の適否を決定する必要があります。

また、サービスの停止により利用者が被った損害につき、クラウド事業者が賠償義務を負わない旨の定めが置かれることもあります。クラウド事業者としては、サービスの一時停止事由を合理的な事由に限定するとともに、これらを可能な限り具体的かつ網羅的に規定しておくことにより、サービスの停止事由について利用者に対し予見可能性を与え、不測の事態に備えることが重要となります。

（本サービスの廃止）

当社は、次の各号のいずれかに該当する場合、本サービスの全部または一部を廃止し、廃止日をもって本利用契約の全部または一部が終了するものとします。 (1) 廃止日の2か月前までに利用者に通知した場合 (2) 天変地異などの不可抗力によって本サービスを提供できない場合

【解説】

本条は、本サービスの廃止、それに伴うクラウド利用契約の終了について定めた規定です。

第１項は、クラウド事業者が、業績不振などの理由により、クラウド事業の継続が困難になった場合には、自らの経営判断で本サービスを廃止できることを定める反面、本サービスが突然打ち切られる場合の利用者の不利益の大きさを考慮して、事業者に対して、本サービスの廃止について、一定の制約を課しています。

利用者としては、代替的なクラウドサービスに乗り換えるための準備期間として、本サービス廃止の予告期間が十分であるかを事前に確認しておく必要があります。

なお、利用者が個人であり消費者契約法が適用される場合で、クラウド事業者がサービスの全部または一部について予告期間なく廃止し、これにより消費者に大きな不利益を生じるような場合には、たとえクラウド利用契約にその旨の定めがある場合であっても、そのような一方的な廃止措置は、消費者契約法第 10 条により無効となり得ます。

（本契約終了後の処理）

１．利用者は、本利用契約が終了した場合、本利用契約の終了後30日以内に、当社に対し、当社のサーバ上に保存された利用者データに関し、汎用性のあるデータ形式に変換した上で、交付するよう請求することができます。 ２．当社は、本利用契約が終了した場合、本利用契約の終了後30日が経過した時、または利用者から利用者データを廃棄または削除するよう求められた時は、利用者デー

タを削除するものとします。当社は、利用者の求めに応じて、利用者データを廃棄または削除したことを証明する文書を発行します。

【解説】

本条は、契約の終了後の処理について定めた規定です。クラウドサービスの利用は、クラウド事業者が利用者データを預かるという特殊性がありますので、クラウド利用契約の終了後の処理について詳細な定めを置くことが紛争防止の観点から望ましいといえます。

第１項は、利用者が、クラウド利用契約の終了後に、クラウド事業者にデータを汎用性のあるデータ形式に変換するよう請求できることを定めた規定です。利用者は、汎用性の低いデータ形式でしかデータの返還を受けられないとすると、別のクラウド事業者が提供するサービスに移行することが極めて困難になりますので、契約終了後に受領可能なデータ形式については事前に確認しておく必要があります。

第２項前段は、クラウド事業者が、クラウド利用契約の終了から一定期間が経過した場合または利用者からの請求があった場合に、データを廃棄・削除することを定めています。クラウド事業者を利用者データの保管・管理義務から解放するため、また、利用者の視点からは、データの漏えい防止など利用者の情報セキュリティを確保するため、確実にデータを廃棄・削除しておく必要があります。第２項後段は、クラウド事業者は、利用者から要求を受けた場合、当該利用者に関する情報を廃棄・削除したことを証明する文書を提出しなければならないことを規定しています。これは、利用者において、クラウド事業者が真にデータを削除したか否かを確認する手段に乏しい点に配慮したものです。

（損害賠償の制限）

１．当社の責めに帰すべき事由により利用者に損害が生じた場合であっても、当社は、特別の事情から生じた損害（予見の有無及び可否を問わない。）、間接的損害、派生的損害及び逸失利益については損害賠償責任を負わないものとします。

２．当社の責めに帰すべき事由により利用者に損害が生じ、当社が利用者に対し賠償責任を負う場合であっても、その賠償額は、請求原因の如何を問わず、本サービスの利用料の1か月分の金額を上限とします。

３．当社の故意または重大な過失により利用者に損害が生じた場合については、前二項の規定は適用しません。

（免責）

当社は、以下の損害については、請求原因の如何を問わず、損害賠償責任を負わないものとします。

(1) 天災地変、騒乱、暴動などの不可抗力に起因して利用者に生じた損害

(2) 当社の設備に接続するためのインターネット接続サービスの不具合など利用者の接続環境の障害に起因して利用者に生じた損害

(3) 第三者の提供する電気通信役務の不具合に起因して利用者に生じた損害

(4) 本サービスの提供にあたり当社が第三者から提供を受けているコンピュータウイルス対策ソフトが対応していない種類のコンピュータウイルスの侵入に起因して利用者に生じた損害

(5) 本サービスの提供にあたり用いられている当社の設備などへの第三者による不正アクセスもしくはアタックまたは通信経路上における傍受で、善良なる管理者の注意をもってしても防ぐことができないものに起因して利用者に生じた損害

(6) 本サービスの提供にあたり用いられている当社の設備のうち当社が製造したものではないソフトウェア及びデータベースに起因して利用者に生じた損害

(7) 本サービスの提供にあたり用いられている当社の設備のうち、当社が製造したものではないハードウェアに起因して利用者に生じた損害

(8) 本サービスの利用にあたり当社が定めているセキュリティ手段などを利用者が遵守しないことに起因して利用者に生じた損害

(9) 裁判所の命令または法令に基づく強制的な処分に起因して利用者に生じた損害

(10) その他当社の責めに帰すべからざる事由に起因して利用者に生じた損害

【解説】

損害賠償の制限に関する規定は、クラウド事業者の責めに帰すべき事由により利用者に損害が生じた場合に、クラウド事業者が支払う損害賠償額を制限しようとするものです。また、免責に関する規定は、一定の事由に基づいて発生した利用者の損害について、クラウド事業者の責任を免除する規定です。

このような規定により、利用者にとっては、生じた損害の全部または一部の賠償を受けられない可能性が生じる反面、クラウド事業者のリスクが限定されることによってクラウドサービスの利用料が抑えられるという面もあり、その意味で、このような規定を設けることには一定の合理性があるといえます。

損害賠償の制限に関する規定の第 1 項は、損害賠償を損害の性質の面から制限する規定です。多くのクラウド利用契約では、「間接的損害」、「派生的損害」といった損害概念を用い、これらの損害に対する賠償責任の制限に関する規定が設けられています。また、逸失利益とは、債務不履行がなければ得られたであろう利益のことをいいます。例えば、利用者がクラウドサービスを利用して顧客にサービスを提供していたところ、クラウドサービスに不具合が発生したために利用者の顧客へのサービスも停止してしまった場合、利用者のサービスによって得られたであろう収益は逸失利益に該当します。

次に、損害賠償の制限に関する規定の第 2 項は、損害賠償を金額の面から制限するものです。利用料を基準に制限を定める場合のほか、一定の金額を基準に制限を定める場合などもあります。

そして、損害賠償の制限に関する規定の第 3 項は、上記の第 1 項及び第 2 項の規定が適用される場面を制限するものです。故意または重過失に基づく損害については、損害賠償責任を制限する条項は無効であるとの判例上の解釈に基づくものといえます。また、利用者が消費者である場合については、消費者契約法によって、事業者の故意または重過失に基づく損害賠償責任を一部免除（損害賠償額の制限はこれに当たります）する契約条項は無効になるとされています（同法第 8 条第 2 号）。

なお、利用者側に損害の発生・拡大について落ち度があるケース（利用者に、データのバックアップ義務がある、またはバックアップが容易であるのに、これを怠っていた場合など）においては、落ち度の程度に応じて、利用者側にも過失が認められ、過失相殺により利用者が請求できる損害賠償額が減額されることもあります。利用者側で自衛措置を取ったか否かということも、法的な損害賠償請求権の判断に影響があることに留意が必要です。

（本利用規約の変更）

1．当社は、本利用契約を随時変更することができるものとします。 2．当社は、前項の変更を行う場合、〇日間の予告期間をおいて、当社のウェブサイトにおける告知、書面、電子メールその他当社が適当と判断する方法により、変更後の本利用契約の内容を利用者に通知するものとします。

【解説】

本条は、クラウド事業者は、一定の予告期間をおいて、クラウド利用契約を変更することができる旨を定める規定です。一般的なクラウド利用契約では、クラウド事業者は、各利用者の個別の承諾を得ることなくクラウド利用契約を変更する権限を付与されています。このため、利用者は、当該変更の内容を受け入れることが困難な場合には、サービスを解約せざるを得ないのが通常です。そこで、利用者は、クラウド利用契約上、サービスの解約がどのような条件のもとで可能かにつき事前に確認する必要があります。

クラウド事業者にクラウド利用契約の一方的な変更権限を付与する本条のような規定は、直ちにその効力が否定されるものではありません。しかし、利用料の著しい増額、サービス内容の著しい低下など、利用者に大幅に不利益となる変更が一方的になされた場合、当該条項は無効となる可能性があります。

（輸出法の遵守）

利用者および当社は、本サービスの利用および運用にあたり、日本および外国の輸出管理に係る法令を遵守するものとします。

【解説】

本条は、各当事者に輸出管理に係る法令の遵守を求める条項です。

例えば、クラウドサービスに用いられるデータセンタが日本国外にある場合、日本国内の利用者が兵器に関連した技術、暗号化技術などの特定の技術情報が含まれたデータを同データセンタ内に保管する場合、以下のような契約を結んでいる場合に限り、外国為替及び外国貿易法（外為法）における輸出管理規制の適用を受けません。

- 利用者自らが使用するためにデータを保管することのみを目的とする契約
- 犯罪捜査の裁判所命令、サービスを運営するために不可欠等による正当で特別な理由がない限りは、クラウドサービス提供者が利用者のデータを閲覧・取得することはないことが記されている契約

これらの契約が結ばれていない場合は輸出管理規制の適用を受ける可能性があります。

このため、現状では、利用者は、クラウドサービスの利用にあたり、データセンタはどの国に所在するのか、データセンタに移転させる情報が外為法の輸出管理規制の適用を受ける特定の技術情報に該当する可能性はあるのかなどについて確認の上、外為法などの輸出管理に係る法令の適用の有無につき事前に検討を行うことが必要となります。[2]

（合意管轄）

本利用契約に起因または関連して生じた一切の紛争については、当社の所在地を管轄する裁判所を専属的合意管轄裁判所とします。

【解説】

本条は、クラウド利用契約に関し生じた紛争は、クラウド事業者の所在地を管轄する裁判所において解決されることを規定します。一般的なクラウド利用契約においては、ク

---

[2] 平成 25 年 6 月 21 日付経済産業省貿易経済協力局長通達
http://www.meti.go.jp/policy/anpo/law_document/tutatu/t10kaisei/130621ekimu_tutatu.pdf

ラウド事業者の本店所在地などのクラウド事業者にとって簡便な地域に所在する裁判所が専属的な管轄裁判所として定められることが多く、クラウド事業者が海外事業者である場合には海外の裁判所が定められることもあります。

海外の裁判所が専属的な管轄裁判所としてクラウド利用契約に定められた場合、利用者がクラウド事業者のクラウド利用契約上の責任を追及するときは、海外での訴訟遂行を強いられることとなり、国内での裁判と比較して費用、時間などの負担が重くなるおそれがある点に留意する必要があります。

なお、海外のクラウド事業者のクラウド利用契約には、利用者が消費者である場合であっても、利用者の住所地国ではなく、クラウド事業者の所在地国の裁判所を専属的な管轄裁判所と規定しているものもあります。しかし、利用者が消費者である場合、このような管轄合意は有効とは認められないことから(民事訴訟法第3条の7第5項第1号)、利用者は、クラウド事業者に対する訴えを日本の裁判所に提起することができる場合があります（同第3条の4）。

（準拠法）

本利用契約の準拠法は日本法とし、日本法に従って解釈される。

【解説】

本条は、クラウド利用契約に適用される準拠法について規定しています。

一般的に、準拠法は、管轄合意と同様、クラウド事業者の本店が所在する国または地域の法が定められることが多く、クラウド事業者が海外の事業者である場合には海外の法が準拠法として定められることもあります。

ただし、利用者が日本国の消費者の場合、外国法が準拠法として規定された場合であっても、消費者契約法第8条（事業者の損害賠償の責任を免除する条項の無効）、第9条（消費者が支払う損害賠償の額を予定する条項等の無効）及び第10条（消費者の利益を一方的に害する条項の無効）などの準拠法を問わず適用されるいわゆる絶対的強行法規は、依然として当該クラウド利用契約に適用される点に留意する必要があります。

8.2. Appendix B　SLA に関する解説と例示

8.2.1. サービスレベル合意（SLA）締結の目的

SLA は、クラウド事業者と利用者との間で、サービスの範囲・内容・前提事項及びサービスレベルへの要求水準を明確化し、共通認識を形成することを目的として締結されるものです。

8.2.2. 義務規定とベストエフォート規定の差異

SLA の中で、クラウド事業者は「本サービスの稼動率」などサービスのレベルを定めていますが、このサービスレベルは、保証義務規定と努力義務規定に分けられます。

保証義務規定は、SLA で定めたサービスレベルを達成することを、クラウド事業者が保証する規定です。これに対し、努力義務規定は、SLA で定めたサービスレベルが、クラウド事業者の努力目標にとどまる規定であり、当該サービスレベルの不達成が直ちに契約違反の問題を惹起することはありません。ただし、この場合、クラウド事業者には、当該サービスレベルの達成のための努力をすべき義務があり、仮にクラウド事業者がこの義務を果たさない場合には、契約違反の問題となり得ます。

例えば、SLA 項目例「オンライン応答時間」では、「データセンタ内の平均応答時間は 3 秒以内とします。」と規定されており、これはクラウド事業者が、平均応答時間 3 秒以内というサービスレベルを保証するもので、保証義務規定に該当します。そして、サービス利用者は、このサービスレベルが達成されない場合には、クラウド事業者の契約責任を問うことが可能です。

これに対し、SLA 項目例「利用者への通知」では、「（中略）、当社は、初期の対応、それに続く状況報告を行い、各インシデントについて下表に記載の時間内に解決するよう努めます。」と規定されており、この解決時間はあくまで努力目標とされていることから、努力義務規定に該当します。そのため、利用者は、解決時間内にインシデントが解決しなかったとしても、クラウド事業者が同時間内に解決できるよう相応の努力をしている限り、クラウド事業者の契約責任を問うことはできません。

8.2.3. SLA の構成

SLA は、一般的には、クラウド利用契約の付属書類として添付され、以下のような要素から構成されています。ただし、①前提条件、②委託範囲、③役割と責任については、通常、クラウド利用契約に記述されますが、その内容を補足する事項がある場合には、SLA にも補足事項が記載されます。

	SLA 構成要素	構成要素の概要

①	前提条件	サービスレベルに影響を及ぼす業務上／システム上の前提条件		
②	委託範囲	合意された委託内容がカバーする範囲		
③	役割と責任	クラウド事業者と利用者の役割と責任を明確化した分担表		
④	サービスレベル項目		分類	分類項目の概要
		ア）	アプリケーション運用	システムの使い勝手に関わる項目（可用性／信頼性／性能／拡張性）
		イ）	サポート	障害対応や一般的問合せ対応に関わる項目
		ウ）	データ管理	データバックアップを含む利用者データの保証に関わる項目
		エ）	セキュリティ	公的認証や第三者評価（監査）を含むセキュリティに関わる項目
⑤	サービスレベル未達の場合の対応	サービスレベルが達成されなかった場合の対応方法（補償）		
⑥	運営ルール	クラウド事業者と利用者間のコミュニケーション（報告・連絡）のルール		

図 27 SLA の構成要素

SLA の構成要素の説明

以下では、④サービスレベル項目、⑤サービスレベル未達の場合の対応、⑥運営ルールの各 SLA 構成要素について、規定例を解説します。以下に述べる各種数値の定義については、事業者によって異なる場合がありますので、確認の必要があります。（例　再ービス停止時間等）

サービスレベル項目

ア）アプリケーション運用

○ サービス提供時間・・・当社は、本サービスを、1年365日、週7日、1日24時間提供します。 なお、本サービス提供停止の通知は、実施の72時間前までに行うものとします。

クラウドサービスでは、利用者が、利用したいときに正しく利用できることが大きなポイントとなります。そこで、サービスレベル項目のひとつとして、サービスの提供時間や、点検保守のためのサービスの一時的な提供停止等が規定されます。

また、以下の式のように、サービス提供時間とサービス停止時間から、サービス稼動率が計算されます。そして、一定の稼働率に満たない場合には、クラウド事業者が返金を行う規定（サービスレベル未達の場合の対応）が、多くの SLA に設けられています（後記、「返金」の規定参照）。

サービス提供時間　―　サービス停止時間　×１００

サービス提供時間

○ オンライン応答時間・・・データセンタ内の平均応答時間は 3 秒以内とします。

○ バッチ処理時間・・・バッチ処理（一括処理）の応答時間は 4 時間以内とします。

サービスレベルを性能面から規定する項目としては、利用者が、アプリケーションのある機能に対してオンライン処理要求を行ってから、回答を得るまでに要する時間である「オンライン応答時間」や、バッチ処理（一括処理）の要求を行ってから、処理が完了するまでの時間である「バッチ処理時間」などがあります。

そして、これらの項目が保証義務規定であれば、サービスがこの基準に達しない場合には、契約違反を問うことができ、SLA 上で補償として返金を行う旨の規定が設けられている場合があります。ただし、サービス提供のために利用されているネットワークやサーバなどは、クラウド事業者以外の者が提供している場合も多い上、処理能力は、ストレージ、アプリケーションなどシステム構成要素それぞれの処理性能に依存します。そこで、クラウド事業者は責任を負う範囲を限定するために、「ただし、利用者のハードウェア、ソフトウェアによるパフォーマンス上の問題の場合には、この補償は適用されません。」など、免責の条項を設けている場合があります。

○ カスタマイズ性・・・利用画面上の項目変更や新規項目の追加が設定画面より可能です。

○ 外部接続性・・・当社は、本サービスの API を公開しています。

クラウドサービスにおいては、利用者の将来的な取引量の増大や、業務手順などの変更に対応できることが必要です。また、クラウドサービスのアプリケーションの中には、外部インタフェース API を提供し、API を利用して異なるシステムやアプリケーション間の有機的な連携を可能とするものがあります。しかし、API は各クラウド事業者が独自に定義している場合があることから、既存システムや他社クラウドサービスのアプリケーションとの連携が必ずしも可能とは限りません。そこで、拡張性に関し、カスタマイズができること、API がインターネットの標準技術で構成され、仕様が公開されていること、API の利用制限や将来の変更可能性などを確認することが必要です。

○ 同時接続利用者数・・・同時にオンライン上で 50 ユーザの利用を保証します。

クラウド利用契約や SLA では、前提条件として、利用者の業務量や利用者数などが規定されている場合があります。その上で、クラウド事業者は、サービスレベルのひとつとして、利用者が同時に接続してサービスを利用することができるユーザ数を SLA に

定めることがあります。この場合、この規定が保証義務規定なのか、努力義務規定なのか、最大接続時の性能などについても確認する必要があります。

○利用者への通知・・・当社がインシデントを認めた場合は、アカウントマネージャーが利用者に電子メールまたは電話にて本サービスの提供停止を事前通知します。当社は、初期対応、それに続く状況報告を行い、各インシデントについて下表に記載の解決目標時間内に解決するように努めます。

優先度	対応開始までの時間	解決目標	対応時間	状況報告
緊急	【サービスデスク窓口時間帯】 10 分以内 【上記時間帯以外】 60 分以内	4 時間以内	24 時間 （土日祝も含む）	1 時間ごと
重要	3 時間以内	1 営業日以内	9 時～5 時 （月～金）	1 日ごと
軽微	1 日以内	1 週間以内 （5 営業日）	9 時～5 時 （月～金）	1 週間ごと

サービスの信頼性という観点からは、利用者としては、インシデントが発生した場合には、直ちに通知をしてもらい、早急に解決してもらう必要があります。SLA においては、通知までの時間や方法、解決時間、解決率、経過報告の方法・タイミングなどが規定されています。また、クラウド事業者によっては、営業時間内と営業時間外で異なる対応を行っている場合があるため注意が必要です。そして、どのような対応をした場合でも、クラウド事業者による報告書提出に関する項目があることを確認することが有用です。

また、利用者とクラウド事業者が想定するインシデントの程度が異なる場合には、インシデントが発生していても、クラウド事業者からの通知が行われない可能性があります。そこで、利用者は、何をもって「通知すべき事象とみなすのか」について確認する必要があります。

○ ディザスタリカバリ・・・災害発生時には、遠隔地のバックアップ用データセンタで保管している日次バックアップデータと予備システムへ切り替えます。

○ 重大障害時の代替手段・・・早期復旧が困難な場合には、バックアップデータの取得が可能なウェブサイトを用意します。なお、代替措置では、データは CSV 形式で提供します。

クラウドサービスでは、津波や地震などの災害により、サービスが一時的に停止するだけでなく、サービスの復旧に要する時間も特定できない程の事態が発生する可能性もあります。そこで、サービスの継続性を確認する上では、災害時、障害時にどの程度シス

テムが停止する可能性があるのか、停止した場合にはどのような対応（代替手段を用いた復旧方法など）がなされるのかを確認する必要があります。

イ）サポート

○ サポート窓口・・・03-○○○○-△△△△ （9:00-18:00 月曜日～金曜日） ○ サービスデスクの窓口時間外では、以下の事由が発生した場合、緊急窓口（03-△△△△-○○○○）に連絡することで対応します。 ・システムダウン、システムの全面停止

クラウド事業者からのサポートとしては、サービスデスクの受付方法（電話、電子メールなど）や営業時間外の対応について確認する必要があります。また、海外のクラウド事業者が日本国内に拠点を持たない場合には、電話や電子メールでのサポートに時間を要する場合があることに注意が必要です。また、質問そのものを英語などの外国語で行わなければならない場合があることにも注意が必要です。

○ サービス提供状況の報告方法・・・利用者数、法改正への対応などのサービス提供状況は、月に一度　ホームページ上で公開します。

クラウドサービスのサポートとしては、法令改正への対応などの確認も必要です。クラウドサービスでは、人事や給与、経理に関するサービスなども提供されます。そして、これらに関するクラウドサービスにおいては、最新の法令（税法、労働法など）の改正に対応できる体制がクラウド事業者に構築されているかどうかについても確認が必要です。例えば、労務管理に関するクラウドサービスを提供しているクラウド事業者が、法令改正後にアプリケーションをアップデートしていなければ、クラウドサービスから得られるアウトプットは、労働法上要求される要件を満たしていないデータになる可能性があります。特に、日本国の法令に対応していない海外のクラウド事業者などのサービスを利用する場合には、法令改正への対応だけでなく、日本の個人情報保護法上要求される水準のデータ管理ができているかなど、利用者データの保全などの観点からも注意が必要です。

ウ）データ管理

○ バックアップの方法・・・○時間毎にバックアップを遠隔地のデータセンタに保管します。また、バックアップデータは 3 年間保管します。

クラウドサービスを利用する上では、万一利用者データが消失した場合には、業務が継続できなくなるなど、重大な問題が発生します。そこで、自社のサービス対象業務の重要性を考慮しつつ、バックアップの頻度や、保管場所、保管期間、利用者でのバックアップの可否について、確認することが重要です。

○ ログの取得・・・セキュリティ（不正アクセス）ログ及びバックアップ取得結果ログは、利用者の要望に応じて提供します。

クラウドサービスはインターネットを通じて提供されるサービスであることから、誰でもインターネット上からサービス利用の窓口となるログインページにアクセスでき、第三者が不正ログインを試みるリスクが存在します。このような問題に備えて、連続したログイン失敗時の処理方法（一定時間ログインできなくなる、ログが保存される、管理者へ通知するなど）について確認する必要があります。

また、自社所有のシステムであれば、トラブルの発生原因分析を行うため、必要なログを全て残しておくことが可能ですが、クラウドサービスにおいては、クラウド事業者が想定している内容での記録しか行われないという問題があります。そこで、クラウド事業者から取得できるログの内容などについても確認が必要です。

ログが保存されていれば、何かの問題が発生した場合に行為者を見つけだすことができるだけではなく、ログが保存されることを従業員に周知することにより、従業員の不正行為を抑止する効果も期待できます。また、効果的にログを解析するためには、各従業員のアカウントとログが一対一に紐付けされていることが必須です。なぜなら、クラウドサービス上で複数の従業員がひとつのアカウントを利用していた場合や部下が上司のアカウントを借用していた場合などでは、ある問題を誰が起こしたのか判別が不可能となる場合があるためです。

エ）セキュリティ

○ 情報取扱者の制限・・・利用者のセキュリティ管理者の許可を得た者に限り、かつ、それぞれのアクセス権限の範囲内でのみ本サービスを利用できます。

クラウドサービスを利用する場合には、利用者の組織において規定しているアクセス制限と同等の制約が、クラウドサービス上でも実現できるかどうかを確認することが必要となります。たとえ、利用者内において、情報管理規程などを定め、職種別に情報へのアクセス権を細かく管理しているとしても、利用するクラウドサービスによっては、利用者で実施しているレベルまで情報や職種を細かく分類していないことも考えられます。

○ 情報取扱環境・・・当社のオフィスは、IC カードによる運用で入室可能な社員などを最小限に制限しており、PC には全てパスワードを設定しています。

本規定はクラウド事業者の利用者データへの物理的アクセスを定めたものです。クラウドサービスから利用者の業務に関する情報が漏えいすることを防ぐためには、十分なセキュリティの確保が欠かせません。

そこで、利用者の情報を扱うクラウド事業者のデータセンタやクラウド事業者のオフィスのセキュリティについて、十分な機密性、完全性、信頼性を保持していることが保証されていることを確認することが重要です。

利用者が個人情報保護法に規定された個人情報取扱事業者（同法第 2 条第 3 項）に該当する場合、利用者は個人情報保護法の規制を受けることになります。そして、利用者からクラウド事業者に移転される個人情報が個人情報保護法上の「個人データ」 に該当する場合、このような個人情報の移転は、個人情報保護法上は「委託」に該当すると理解されており、利用者は、当該個人情報の安全管理が図られるよう、クラウド事業者に対し必要かつ適切な監督を行う義務を負います（同法第 22 条）。

ここにいう監督の実施としては、まず、クラウド事業者における個人情報の保護水準を踏まえて適切に委託先となるクラウド事業者を選定することが重要です。なお、クラウド事業者のサーバが日本国外にある場合には、個人情報が日本国外に移転されることとなります。個人情報が日本国外に移転されること自体について、個人情報保護法は特段の規制を設けていないものの、この場合、サーバ所在地の法律によってサーバ内の個人情報が差押などを受ける可能性があります。そのため、利用者が第三者（当該個人情報の開示者など）から取得している個人情報の種類によっては、高い監督義務が課せられ、当該利用者による当該クラウド事業者の選定の適切性が問われるおそれもあるので注意が必要です。

また、経済産業省が定める「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」（平成 21 年 10 月）においては、個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失または毀損の防止その他の個人データの安全管理のため、組織的、人的、物理的及び技術的な安全管理措置を講じなければならないとされていることから、クラウドサービスにおいて個人情報を取り扱う必要がある場合には、これらのガイドラインに準じた措置が講じられていることを確認する必要があります。

そこで、利用者の情報を扱うクラウド事業者のデータセンタやクラウド事業者のオフィスのセキュリティについて、十分な機密性、完全性、信頼性を保持していることが保証されていることを確認することが重要です。また、クラウドサービスにおいては、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ことから、クラウド事業者の従業員（派遣社員なども含みます）のアクセス制限、閲覧制限、アクセスログ、セキュリティ教育体制などのアクセスに関する規定及び保護措置についても定め、保証を受けることが求められます。

なお、クラウド事業者のサーバが日本国外にある場合には、個人情報が日本国外に移転されることとなります。個人情報が日本国外に移転されること自体について、個人情報保護法は特段の規制を設けていないものの、この場合、サーバ所在地の法律によってサーバ内の個人情報が差押などを受ける可能性があります。そのため、クラウド事業者に移転される個人情報について利用者が負っている秘密保持義務の程度によっては、当該クラウド事業者の選定の適切性が問われるおそれもあるので注意が必要です。

○ 通信の暗号化レベル・・・データは 128bit の SSL（Secure Socket Layer）により暗号化しています。

○ ウイルス対策管理・・・ウイルス発生の検知から対処を開始するまでの目標時間は３０分とします。

クラウドサービスを利用する場合、データが常にクラウド事業者のサーバにあり、加えて他のサービス利用企業の情報と同じデータベースに蓄積されることもあるため、データの格納形態や暗号化の状況、アクセス時の承認プロセスやウイルス対策などの状況を確認することが重要です。

○ 公的認証取得・・・当社は、ISMS を取得しています。

○ サービスに関する第三者評価・・・当社は、年１回、外部検査機関により本サービスの脆弱性に関する評価を受け、速やかに指摘事項に対して対策を講じています。

クラウドサービスの安全性検証の観点からは、セキュリティ対策の実施状況を確認することが重要です。クラウド事業者のセキュリティの実施状況について、利用者自ら監査及び確認を行うことも考えられますが、セキュリティ対策の実施状況を各利用者に開示すること自体がクラウドシステムの脆弱性を高めることから、第三者機関による安全性検証試験やセキュリティ診断を定期的に実施し、結果を利用者に対して公開することでセキュリティ対策の実施状況の保証に代えることが行われています。また、セキュリティ確保を保証する指標として、公的認証を取得していることを確認することは有益です。

5)サービスレベル未達の場合の対応項目

○ 返金・・・クラウド利用契約の損害賠償の規定にかかわらず、月間稼働率が特定の月において 99.9%を下回った場合、利用者は次の返金割合で当該月間の利用料の返金を受けることができます。

月間稼働率	返金割合
99.9%未満	5%
99%未満	10%
95%未満	15%

サービスレベルが未達の場合に、利用者がクラウド事業者へ求める対応としては、①クラウド事業者が改善を行うなどの運用上の対応、②クラウド事業者が返金などを行う金銭上の対応、③契約解除などを行う契約上の対応、の 3 種類が考えられます。本規定は、金銭上の対応として、クラウド事業者からサービス利用者に返金が行われる旨を定めた規定です。

金銭上の対応としての返金は、クラウド利用契約上の損害賠償とは別に定められているもので、「賠償額の予定」（民法第 420 条第 1 項）であると解される場合があります。本規定では、クラウド利用契約の損害賠償の規定にかかわらず、月間稼働率が規定の数値を下回った場合には返金が行われると規定されており、損害賠償の予定であると考えられます。この場合、利用者は、サービスの提供停止などによる損害の発生やその額の立証をすることなく、返金を受けることができるというメリットがありますが、他方、予定賠償額を上回る損害が発生したことを立証したとしても、増額を請求することができません。

なお、稼働率の低下以外の、利用者データの消失などの原因により利用者に損害が生じた場合には、この返金規定ではなく、クラウド利用契約の損害賠償の条項に基づき、利用者は損害賠償請求を行うことになります。

6) 運営ルール項目

○ SLA の評価・・・当社は、サービスレベルの設定によって定められた項目について実績情報を管理し、評価・分析の上で定期的に報告します。

SLA はクラウド利用契約の附属資料として締結されることが一般的であり、クラウド事業者は、実際の業務に即してクラウド利用契約とともに定期的に見直し、変更することが望ましいといえます。

執筆

株式会社電通国際情報サービス	渥美　俊英
TMI 総合法律事務所	大井 哲也
株式会社電通国際情報サービス	加藤　章
株式会社ディアイティ	河野　省二
atoll project	川田　大輔
ニフティ株式会社	久保田　朋秀
国際大学　グローバルコミュニケーションセンター	林　雅之

（執筆者五十音順、2013 年 4 月現在）

執筆支援

TMI 総合法律事務所	柴野　相雄
	米山　貴志
	小林　央典
	梅田　宏康
	江頭　あがさ
	畠山　大志

監修及び編集

新日本有限責任監査法人	高橋　可祝
	仲宗根　友恵
	岡田　成晃

協力企業一覧

クラウドセキュリティガイドライン活用ガイドブック（2013 年度版）

株式会社あくしゅ

株式会社インターネットイニシアティブ

株式会社エヌ・ティ・ティ・データ・イントラマート

株式会社エヌ・ティ・ティピー・シーコミュニケーションズ

株式会社 co-meeting

株式会社サーバーワークス

サイボウズ株式会社

TIS 株式会社

株式会社電通国際情報サービス

ニフティ株式会社

日本ユニシス株式会社／ユニアデックス株式会社

バリオセキュア株式会社

株式会社日立製作所

富士通株式会社

（五十音順、2013 年 4 月現在）