情報セキュリティガバナンス協議会

クラウドサービスの利用に係るセキュリティリスク対処

報告書

2014 年 3 月

情報セキュリティガバナンス協議会

目次

はじめに

自社の情報資産の管理を他社に委ねることとなるクラウドサービスの利用は、ユーザ企業の情報セキュリティガバナンスの運営に大きな影響を与えます。クラウドサービスは定型のサービスであり、ユーザ側で情報資産を管理できる範囲が制限されるため、クラウドサービス事業者まで情報セキュリティガバナンスが及びにくいことがその理由です。

多くのクラウドサービス事業者は、サービス提供に伴うリスクに対して真摯に対応していますが、まだ情報の開示が十分でなく、ユーザ側にはリスクへの対応状況が把握しにくいのが現状となっています。

こうした背景を踏まえて、経済産業省では 2011 年 4 月に「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」を発行し、それに基づき、特定非営利活動法人日本セキュリティ監査協会（以下「JASA」といいます。）－クラウドセキュリティ推進協議会では、クラウド情報セキュリティ監査制度の策定に取り組んでいます。

また、クラウドサービス事業者の情報開示を促進するため、一般財団法人マルチメディア振興センターが「クラウドサービスの安全・信頼性に係わる情報開示認定制度」を運営しています。

そこで、当ワーキンググループでは、ユーザがクラウドサービスの利用について判断する際に、どのような情報が必要か、そうした情報が入手可能かを調査し、ユーザにクラウドサービス利用検討の際の有益な情報と共に、安全なクラウドサービス利用に向けたクラウドサービス事業者に対する要望を報告書としてとりまとめました。

この報告書の内容は、ユーザ企業における安全なクラウドサービスの利用を促進し、さらには経済産業省の施策や、JASA－クラウドセキュリティ推進協議会の活動に寄与することを期待するものです。

1. クラウドサービス利用状況

最初に、クラウドサービスが現在どのように企業で利用されているかを整理します。そのため、検討メンバーにおける利用事例や一般的なクラウドサービスの利用状況について示します。

1.1 検討メンバーにおけるクラウドサービス利用事例

1.1.1 各社における利用事例

検討メンバー各社における利用事例を表 1-1 に示します。

表 1-1　各社の利用事例

メンバー	利用事例	クラウド分類		
		デリバリーモデル	共有形態	利用用途
A社	外部DCで運用される 電子メールサービス	SaaS	パブリック	周辺システム
	外部DCで運用される ファイルサーバーサービス	SaaS	パブリック	周辺システム
B社	外部DC内に電子ファイルを保存	SaaS	パブリック	周辺システム
	大容量業務用データの外部保存による授受	SaaS	パブリック	周辺システム
	Office365のグループウエア利用 （電子メール、掲示板、予定表）	SaaS	パブリック	周辺システム
	メール送信時の自動的暗号化機能利用（外部サービス）	SaaS	パブリック	周辺システム
	メール送受信データの一定期間保管、管理者閲覧（外部サービス）	SaaS	パブリック	周辺システム
C社	業務用モバイル端末からの印刷サービス	SaaS	パブリック	周辺システム
	大容量業務用データの外部保存による授受	SaaS	パブリック	周辺システム
	SNSのサービスを利用した、客先とのデータ共有	SaaS	パブリック	周辺システム
D社	電子メール／グループウェア	IaaS	プライベート	周辺システム
	家庭向け省エネ・節電コンサルティングサービス	SaaS	パブリック	周辺システム
E社	関連会社のOAシステム	SaaS	パブリック	周辺システム
	社内メール便追跡サービス	SaaS	パブリック	周辺システム
	環境情報管理システム	SaaS	パブリック	周辺システム
F社	大容量ファイル受け渡しサービス	SaaS	プライベート	周辺システム
	e-learningによる教育	SaaS	プライベート	周辺システム
	与信管理支援サービス（ASP）	SaaS	パブリック	周辺システム
	安否確認システム	SaaS	プライベート	周辺システム
	電子契約サービス（ASP）	SaaS	パブリック	周辺システム
	WEB会議システム	SaaS	プライベート	周辺システム

1.1.2 利用事例における傾向

検討メンバーの利用事例を俯瞰してみると、全体的には下記のような状況です。

- クラウドサービス利用はまだ多くありません。
- 基幹システムでの利用事例はなく、グループウェアや一部の業務利用などの周辺システムに限られています。
- 各社ともクラウドサービスを利用しているが、デリバリーモデルは Software as a service（以下「SaaS」といいます。）がほとんどです。

1.2 一般的なクラウドサービス利用状況

1.2.1 クラウドサービスの定義と分類

クラウドコンピューティングとは、共用の構成可能なコンピューティングリソース（ネットワーク、サーバ、ストレージ、アプリケーション、サービス）の集積に、どこからでも、簡便に、必要に応じて、ネットワーク経由でアクセスすることを可能にするモデルです。クラウドサービスとは、クラウドコンピューティングを利用したサービスの総称です。

クラウドサービスには様々なものがあります。ここでは、クラウドサービスに関するセキュリティを考える上で、様々なクラウドサービスを分類・整理します。

まず、クラウドサービスの提供される仕組みの形態により、以下の 3 つのデリバリーモデルに分類されます。デリバリーモデルにより、クラウドサービス事業者と利用者の責任分界点
が異なります。

・ソフトウェアの提供（SaaS）

電子メール、グループウェア、顧客関係管理（以下「CRM」といいます。）などのソフトウェアパッケージ（アプリケーション）がネットワーク経由で提供されます。
（業務用途に応じたアプリケーションを利用します。）

例：Google Apps for Business（Google 社）
Office 365（Microsoft 社）
SalesforceCRM（Salesforce.com 社）

・プラットフォームの提供（PaaS）

仮想化されたアプリケーションサーバやデータベースなどのアプリケーション実行（本番・開発）用プラットフォームが、ネットワーク経由で提供されます。
（プラットフォーム上に自らのアプリケーションを配置・運用します。）

例：Google App Engine、AppScale（Google 社）

Windows Azure（Microsoft 社）
Amazon S3（Amazon.com 社）

・インフラの提供（IaaS）
サーバ仮想化やデスクトップ仮想化や共有ディスクなどのハードウェアやインフラが、ネットワーク経由で提供されます。
（OS などを含め自らのシステムを導入・構築します。）
例：Amazon EC2（Amazon.com 社）

次に、提供サービスの共有形態により、以下のとおり分類されます。IT リソースを共有するかしないかでリスクも異なります。

・パブリッククラウドサービス
一般利用者を対象に提供されるクラウドサービス。多種多様な企業や組織、あるいは個人といった、不特定多数の利用者を対象に広く提供されます。

・プライベートクラウドサービス
特定の利用者を対象として提供されるクラウドサービス。企業が、専有する環境下でクラウドコンピューティングを整備し、企業内の部門やグループ会社等に提供されます。

最後に、クラウドサービスの利用用途による分類です。企業にとって重要な基幹システムに利用するのか、そうでない周辺システムに利用するのかによって、セキュリティ等に関する要件も異なるためです。

1.2.2 クラウドサービスの利用状況

検討メンバーは 6 社と母集団が少なく、一般的なクラウドサービス利用状況と傾向が異なる可能性があるため、調査会社等による調査結果を確認します。

まずは、クラウドサービス全体の利用状況についてです。図 1-1 は、ここ 3 年のクラウドサービスの利用検討状況を示しています。

クラウドの認知度は向上しており、クラウドの利用率、導入率とも堅調に増加しています。2013 年の調査では、「検討したが利用しない」との回答が大幅に減少し、「興味があり、情報を収集中」の回答が増加しました。このことは、クラウドの課題を理解した上で、情報を収集する企業が増加したことを表しています。

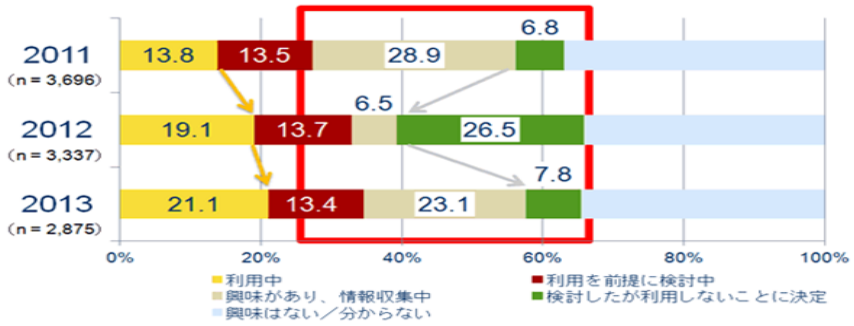


図 1-1　パブリッククラウド利用検討状況、2011 年～2013 年

資料：国内クラウド市場 ユーザー動向調査結果を発表（2013 年 7 月 8 日 IDC Japan）

次に、クラウドサービスの利用用途はどうでしょう。図 1-2 は、SaaS の導入状況を示しています。メールや掲示板といった周辺システムでの利用は進んでいますが、受発注、物流等の基幹システムでの利用はあまり進んでいないといえます。

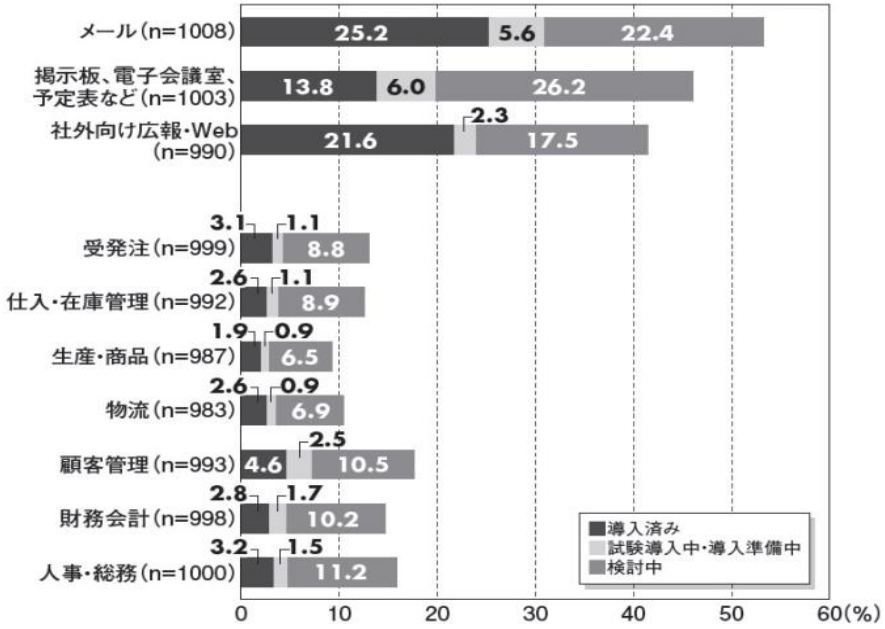


図 1-2　SaaS の導入状況

資料：早読み「企業 IT 動向調査」（2013/06/05　ITPRO/日経コンピュータ）

1.2.3 クラウドサービスのメリット

企業は、なぜクラウドサービスを利用するのでしょう。それは、クラウドサービスを利用することにメリットがあるからです。

クラウドサービスを利用するメリットとして、第一に「低価格」が挙げられます。自社でシステムを構築する場合は、機器の購入に加え運用保守に係る人件費等が必要となりますが、クラウドサービス利用では利用料金だけになるため、トータルコストを削減するこ

とができます。

第二に、「信頼性」が挙げられます。システム部門の要員不足、スキル不足は、多くの企業で課題となっており、運用負荷を低減したいというのは共通の悩みです。そのような企業の場合、信頼性の高いクラウドサービスを利用することにより、運用負荷を軽減できることは、「低価格」と同じくらい重要な要素となります。検討メンバーにおける利用事例の中でも、クラウドサービス利用のメリットとして、コストだけではなく、運用負荷の軽減やサービスレベルの向上を挙げる企業が複数ありました。

それ以外にも、すぐ使えるという「スピード」や必要な時に必要な分だけ使えるという「柔軟性」もメリットに挙げられます。

2. パブリッククラウドサービス利用者としてのリスク認識

本章では、クラウドサービスを利用するにあたり、懸念されるリスクとその対策について、検討メンバーの利用事例、クラウドセキュリティガイドライ及び活用ガイドブックより分析した結果を示します。

2.1 検討メンバーのクラウドサービス利用事例

2.1.1 検討メンバーの利用事例と想定リスク

検討メンバーのクラウドサービスの利用事例及び検討事例を元に、各サービスにおける想定リスクとその回避策について例示として表 2-1 にまとめました。

表 2-1　検討メンバーのクラウドサービス利用事例

サービス	想定されるリスク	リスクの分類	リスクの回避策
電子メールサービス	アクセス制御ができないことによる第三者からの不正アクセス 非暗号化による通信とデータ保存による情報漏えい	情報漏えい（パスワード情報を含む）	容易に推測されないパスワードの利用 運用による暗号化対策の実施
電子メール暗号化サービス	外部サービスとの連携による情報漏えいポイントの増加 サービス変更によるシステム障害や対応工数の増加	情報漏えい 事業継続	なし（サービスを容認）
電子メール一定期間保管・管理者閲覧サービス	外部サービスの連携による情報漏えいポイントの増加 メールデータの外部保存による情報漏えい	情報漏えい	なし（サービスを容認）
グループウェアサービス	社内機密情報の外部保存による情報漏えい サービスの終了	情報漏えい 情報消滅 事業継続	一部機能のオンプレミス化 他社サービスへの移行を事前検証
ファイルサーバサービス	社内機密情報の外部保存による情報漏えい 非暗号化による通信とデータ保存による情報漏えい	情報漏えい 情報消滅	アカウント認証によるアクセス制限 事前に暗号化してデータ保存
大容量ファイル送受信サービス	社内機密情報の外部保存による情報漏えい	情報漏えい 情報消滅 海外当局による検閲	セキュリティ要件を満たしたサービス事業者の選択 利用者の限定
モバイル端末からの印刷サービス	社内機密情報の外部保存による情報漏えい	情報漏えい 情報消滅 海外当局による検閲	なし（サービスの非採用）
SNS	メンバー公開による不特定の第三者への情報漏えい	情報漏えい	なし（サービスの非採用）
社内メール便追跡サービス	外部サーバへ社員の個人情報を保管することによる個人情報の漏えい	情報漏えい	契約書、覚書による情報の扱いに関する契約締結
e ラーニング	ラーニングデータの消失	情報消滅	なし（サービスを容認）
与信管理支援サービス	決算非公開企業の場合に与信不可	ー	なし（サービスを容認）
安否確認システム	緊急時のシステム障害によるサービス利用不可	ー	なし（サービスを容認）
電子契約サービス	障害発生によるシステム利用不可	契約遅延／情報消滅	なし（サービスを容認）

2.1.2 クラウドサービス利用事例から見る想定リスク

クラウドサービス利用時に想定されるリスクについては、情報漏えいや情報消滅といった企業情報の取扱いに関する内容が大半を占めました。しかしながら、この情報漏えいや情報消滅の対策についてはクラウドサービス事業者に委ねられる部分が多く、利用者側で根本的な対策を取ることは難しい場合がほとんどです。一方、クラウドサービス事業者がセキュリティに関する内容を開示することは、脆弱性を開示することとなる場合もあり、開示されることはあまりありません。また、事前にクラウドサービス事業者と交渉を行い、契約内容を変更して自社独自の内容の契約を締結できることも稀です。

利用者は、クラウドサービスの利用にあたって、クラウドサービス事業者から提供されるサービスを許容して利用することを前提に、サービス利用の可否及びクラウドサービス事業者の選択を検討する必要があります。

クラウドサービス事業者の選択においては、一概にセキュリティの強固なクラウドサービス事業者を選択していては、クラウドサービスのメリットである「低価格」というメリットを十分に享受できなくなります。取り扱う情報やサービスのレベルによって、想定されるリスクに強弱を付けて最適なクラウドサービス事業者を選択しましょう。

2.2 マネジメントガイドライン／ガイドブックの想定リスク

2.2.1 マネジメントガイドライン及び活用ガイドブックにおける想定リスク

「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」の附属書A及び「クラウドセキュリティ活用ガイドブック」に例示されているリスク一覧より、サービス利用者や事業者の対応方法や検討タイミングを分類し、例示として表2-2にまとめました。

表 2-2　情報セキュリティガイドライン／ガイドブックにおける想定リスク

サービス利用要件	想定されるリスク	リスクの分類	サービス利用者や事業者の対応方法	検討タイミング		
				導入前（可否）	事業者選択	運用
DoS 攻撃	DoS 攻撃をされた場合に、全てのサービスが停止してしまう可能性	事業継続	リスクを許容		●	●
ID 管理	クラウド事業者の仕組みを利用することによる管理工数の増大 一貫したセキュリティ対策及び管理にミスが発生する確率増加	情報漏えい データ改ざん 情報消滅 管理コスト	サービスの選択 ID 管理が困難になるリスクを許容	●	●	●
アクセスポイント	ネットワーク上のアクセス制御が困難	情報漏えい データ改ざん 情報消滅	サービスの選択 アクセス管理が困難になるリスクを許容		●	●
アクセス制御	利用者が想定するアクセス制御が困難	情報漏えい データ改ざん 情報消滅 管理コスト	サービスの選択 サービスされる制御を受け入れてリスクを許容	●	●	●
アプリケーション	SaaS で提供されるアプリケーションの機能は限定的で、アプリケーション同士の互換性も不十分	事業継続	サービスの選択 互換性に制限があることを許容	●		●
インシデント管理	インシデントを管理するための情報が限定されるため、利用者が主体となった管理が困難となり、レベルの相違やビジネスへの影響が不明確	－	インシデントやイベントのレベルを合意 レベル相違によるリスクを許容	●		●
クラウド事業者の事業継続	クラウド事業者が事業を継続できなくなった時に、サービス上の情報が利用できなくなりデータが消失する可能性	事業継続	クラウド事業者の信頼性の確認 サービス提供の停止は事業者が決定するリスクを許容		●	●

サービス利用要件	想定されるリスク	リスクの分類	サービス利用者／事業者の対応	検討タイミング		
				導入前（可否）	事業者選択	運用
システム運用・保守	セキュリティに関する業務は委託できるが責任は委譲不可	ー	クラウドサービス利用前段階でのセキュリティ規定の整備	●		●
スケールアウト技術	スケールアウト技術（ハードウェアを仮想的に連携させた構成）は、物理的な検証が十分できないため、予知できない障害発生の可能性	ー	リスク移転（利用料の減額等）の実現 障害リスクを許容	●		●
データセンタの所在	様々な国のネットワーク技術の接続性による、サービスレベルの低下及び現地の法執行機関による情報差し押さえ	法令遵守	データセンタの所在地の法規適用によるリスクを許容		●	●
データセンタの物理環境	データセンタの新しい運用形態（コンテナ式等）により、事業者が経験したことのない障害が発生する可能性	ー	リスク移転（利用料の減額等）の実現 障害リスクを許容	●	●	●
ヘルプデスク	海外のクラウドサービス利用では、言語・時差・営業日の違いによる不便	利用者／事業者	リスクを許容		●	●
マルチテナント	一つのハードウェアに複数の契約者が同居することにより、ハードウェア攻撃が実施された場合、他の契約者にも影響が及ぶ可能性	情報漏えい データ改ざん 情報消滅 事業継続	他の契約者の管理不備による障害リスクを許容	●	●	●
メモリ管理	クラウド事業者は物理的なメモリ管理ができないため、メモリ保護に関するトラブル対処が困難	情報漏えい データ改ざん 情報消滅	技術的障害のリスク移転（利用料の減額等）の実現 障害リスクを許容	●		●
メンテナンスユーティリティ	システムの状況を知るためのユーティリティが提供されないことにより、情報不足による障害予兆の判断が困難	事業継続	情報が不足することのリスクを許容		●	●

サービス利用要件	想定されるリスク	リスクの分類	サービス利用者や事業者の対応	検討タイミング		
				導入前（可否）	事業者選択	運用
ライセンス管理	クラウドサービス上でソフトウェアの利用状況が把握できないことにより、ライセンス体系によってはソフトウェア監査におけるトラブルに発展	利用者／事業者	ライセンス（契約）の再確認	●		●
リカバリ	クラウドサービスを顧客向けに提供している場合は、正確な復旧計画を顧客に提示できない問題が発生	事業継続	SLA があれば復旧計画を顧客に通知 代替策を講じるかリスクを許容	●	●	●
ログ監視	アクセスログが提供されない場合に、利用者の資産の危機を知ることが難しく、事前に対策が講じられない	情報漏えい データ改ざん 情報消滅	サービスの選択 スキャンニング等の認知が困難であるというリスクを許容		●	●
暗号化	SSL/TLS の暗号化通信に対応していないサービスの場合に、自社の機密データ取扱いの規程に反する可能性	情報漏えい データ改ざん 情報消滅	暗号化されないリスクを許容		●	●
仮想化対応	仮想化環境を前提としないアプリケーションは、レスポンスの低下やコンピュータリソースの非効率な使用により、クラウドのメリットであるコスト削減に寄与しない可能性	ー	リスク移転（利用料の減額等）の実現 メリットが出ないことを許容	●		●
携帯電話・スマートフォン	スマートデバイスは、PC に比べてセキュリティ対策が弱く実績も少ないため、トラブル対策の情報が得られない	情報漏えい データ改ざん 情報消滅	サービスの選択 管理が弱くなるリスクを許容		●	●
最大許容停止時間	最大許容停止時間はクラウド事業者が定めるものであり、利用者は復旧を待つしか方法がない	事業継続	過去の障害対応状況や改善点の対応状況を確認		●	●
残存データ	メモリやハードディスクにデータが残った場合に、仮想化環境では制御できない	情報漏えい	クラウド事業者の技術的処理方法を確認 障害リスクを許容	●		●

サービス利用要件	想定されるリスク	リスクの分類	サービス利用者／事業者の対応	検討タイミング		
				導入前（可否）	事業者選択	運用
実行環境の制限	アプリケーションによっては、必要なライブラリが使えないことによる動作不能及び、PaaS ベンダーによっては独自の開発言語を使用することで他社のサービスが利用不可	ー	汎用性のある実行環境の事業者を選択 実行環境の制限を許容	●	●	●
従量課金を利用した攻撃	処理を必要以上に増加させる外部攻撃により、リソースの使用料が高額になり経済的に事業継続不可	事業継続	クラウド事業者と攻撃による損失に対して契約条項を設定	●		●
接続性	国内外を問わずデータセンタを展開して、ネットワークが複雑になり接続の信頼性を把握できない	情報漏えい 事業継続	接続性に係わるリスク移転（利用料の減額等）の実現 接続性リスクを許容	●		●
相互運用性	クラウドサービスに関する標準化が未整備のため、システム間の連携ができない可能性	ー	相互運用性の高いサービスの選択 相互運用ができないリスクを許容	●	●	●
中間者攻撃	データセンタが複数の場所で展開され、かつ連携していることにより、中間者攻撃を受けやすい	情報漏えい データ改ざん 情報消滅	攻撃による損失のリスク移転（使用料の減額等）の実現 攻撃損失リスクを許容	●		●
分散管理	冗長性・拡張性のメリットを出すために、分散管理の手法が使われ、情報の一元管理を妨げる	情報漏えい データ改ざん 情報消滅 法令遵守	データの所在を把握できないリスクを許容	●		●
ネットワーク	通信の傍受	情報漏えい	リージョン間の暗号化の確認または代替策の検討 データの暗号化の標準化及び実施			●

サービス利用要件	想定されるリスク	リスクの分類	サービス利用者／事業者の対応	検討タイミング		
				導入前（可否）	事業者選択	運用
ネットワーク	中間者攻撃やなりすましによる攻撃	情報漏えい データ改ざん	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かの理解 サーバや端末間の相互認証（必要に応じて証明書の活用）			●
	内部ネットワーク管理の不備（ネットワークダウン）	事業継続	機器の構成管理や容量管理 ネットワークが切断されないような物理的な保護			●
	VLAN 上の障害（仮想ネットワーク容量）	事業継続	必要に応じて最適化された機器の導入を検討（プライベートクラウド） 通信量だけでなく機器の数などのキャパシティに配慮した管理			●
データセンタ	データセンタへの不正な入退館（管理コンソールの悪用）	情報漏えい データ改ざん	建物及び敷地への不正侵入を管理することが重要			●
	機器への直接的な攻撃（機器・電源の防御）	情報消滅	多層防御（5 層が理想）			●
	意図しない操作ミス	情報消滅 データ改ざん	操作手順書の作成及び訓練の実施 事業者は操作手順書作成の支援			●
	内部関係者による意図的な攻撃	情報漏えい 情報消滅	認可レベルの明確化（誰が、どこで、どの機器を、どのように操作できるのかを定義）			●
	電源喪失のよるサービス停止	事業継続	バックアップ電源の確保及び定期的な切替テストの実施			●

サービス利用要件	想定されるリスク	リスクの分類	サービス利用者／事業者の対応	検討タイミング		
				導入前（可否）	事業者選択	運用
仮想化基盤	事故対応の不備（サービス再開時間の延滞、再発可能性）	事業継続	インスタンスのバックアップ及びテンプレートの準備 バックアップのリストアサービスの契約			●
サービス基盤	単一障害点となるサービスに関する脅威	事業継続	サービス構成図の作成及び冗長化の検討			●
	共有サービス（他社の同居）に関する脅威	ー	データの所在を確認する方法とサービス継続性のトレードオフにて選択			●
統合管理環境	統合管理環境に関する脅威（コントロールパネルへの攻撃）	ー	アクセス管理の徹底			●
	監視環境に関する脅威	ー	なし（リスクを許容）			●
データ管理方針	データ管理のガバナンスの喪失	情報漏えい 情報消失 データ改ざん	情報資産の分類方針を明確化し、その中で、クラウド上で取り扱うことのできるものを分類し、そのデータへのアクセス権を設定			●
	不正なデータの取得によるウイルス感染	情報漏えい 情報消失 データ改ざん	ダウンロード及びアップロードした際のウイルススキャンの実行			●
データ分類	適切なアクセス権の設定不能（ユーザ権限 vs 管理者権限）	ー	利用者組織のポリシをベースに権限設定			●
データのライフサイクル管理	データ管理におけるライフサイクル管理の欠如	ー	クラウド上での適切な削除方法を理解し、その手順を明確化			●
	データ漏えい・流出（下書きデータ・送信済みデータの漏れ）	情報漏えい	不用意なコピーやローカル PC への保存を行わないように管理 情報資産を増やさない			●

サービス利用要件	想定されるリスク	リスクの分類	サービス利用者／事業者の対応	検討タイミング		
				導入前（可否）	事業者選択	運用
ID 管理	クラウドにおける ID 管理	ー	二要素認証や二段階認証 多様な認証機能サービスの提供			●
	ID フェデレーション	ー	取り扱うサービスよって ID 管理レベルを決定			●
人員	クラウド利用者のリテラシー	ー	サービスの内容や機能を理解するため、注意喚起の資料や研修を実施			●
	クラウド構築・運用・管理に関するリテラシー	ー	手順などの文書化と研修の実施 予兆管理などのための監視環境を構築			●

コラム　クラウド利用の落とし穴

実際にクラウドサービスの利用を開始して、こんなはずではなかったと思うこともあるかもしれません。以下にクラウドサービスを利用するにあたっての注意点を記述します。

(1)サービスレベルについて

例えばサービスレベルが 99.9%と定義されていた場合、ほとんど業務影響が発生しないような感覚に囚われがちですが、そこに落とし穴があります。サービスレベルの算出方法はクラウドサービスによって異なりますが、以下の例で考えてみましょう。

表 2-3　サービスレベル契約の例

月間稼働率	サービス クレジット（請求可能）
99.9%未満	25%
99.0%未満	50%
95.0%未満	100%

$$\text{月間稼働率} = \frac{\text{ユーザ時間（分）} - \text{ダウンタイム}}{\text{ユーザ時間（分）}} \times 100$$

※ユーザ時間　：月の総時間にユーザの総数を乗じた時間（分）
※ダウンタイム:当該サービスを利用できない月の総時間に、影響を受けたユーザの総数を乗じた時間(分)

上記のサービスを、100 人で 31 日間利用した場合、8 時間ダウンタイムがあったとしも、月間稼働率は 99.99%となります（サービスレベルは守られている)。つまり、サービス稼働率が高ければ“ほとんど業務に影響しないであろう“という思い込みは危険です。サービスを利用できなくなる場合があることを想定し、その場合のアクション（例：利用者への周知方法や代替手段など）を事前に準備しておきましょう。

(2) 仕様変更、軽微な問題、共用サービスのリスクについて

Web ブラウザを利用するクラウドサービスの場合、随時、対応ブラウザバージョンへの追従が必要となりますので、他の業務システム等で Web ブラウザを利用している場合には注意が必要です。また、サービスとしては継続利用できる範囲で操作画面の大規模な仕様変更や、軽微な問題（例：日本語表記が英語表記になるなど）も起こり得ます。

また、複数社が共用で利用するサービスの場合、他社の利用状況による一時的なパフォーマンスの低下や、ディスク容量が当初想定していた分を確保できないなどの問題も起こり得ます。

「こんなはずではなかった！」とならないように、どのようなリスクがあるのか事前にできる限り確認しておきたいところですが、実際に使ってみないと気付けないことの方が多いかもしれません。よって、クラウドサービスを本格的に導入する前に、一部のユーザ限定で試験的に導入してみるなどのステップを踏むのも有効な手段となります。

3. パブリッククラウド利用者の情報活用と意識改革

本章では、クラウドサービス利用者がサービスの提供を受ける際に、そのリスクを回避する対策や、そのリスクを受け入れる準備をするために必要な情報にどのようなものがあるかを整理し、さらに利用者としての意識の転換の必要性についてまとめました。

3.1 クラウドの利用ステージと活用する情報

3.1.1 クラウドの利用ステージ

クラウドを利用するための手順の中には、いくつかのステージがあり、その中で様々な判断や決定が行われています。

最初のステージでは、自社システムの新規構築　または再構築において、その方法を検討します。ここでは、自社構築（オンプレミス）するのか、あるいはクラウドサービスを採用するかどうかを判断する場面が出てきます。

クラウドサービスを利用することが決定されると、次のステージでは、クラウドサービス事業者をどこにするかを検討します。ここでは、必要となる処理機能に対して、どのようなサービスが提供されるのか、あるいは事業者の実績などから信用できるかどうかを確認して判断する場面が出てきます。

また、クラウドサービス稼働後のステージでは、運用上の課題を解決するためにどのような手段を取るかを判断する場面が出てきます。

一方、導入しようとするクラウドサービスの種類も様々で、IaaS や SaaS、基幹システムや周辺システムなど　サービス範囲や対応策も異なったものになっています。自社にとってのシステムの重要度によって、要求されるサービス品質は変わってきますが、判断をするために利用する情報は概ね同じものとなります。

3.1.2 クラウド導入の判断で活用する情報

(1)必要となる情報とは

システムの自社構築　または外部システムの導入の方針決定は、経営層の判断を仰ぐことになりますが、クラウドサービス利用の可否判断においては、自社環境での構築との比較を行い、コスト、セキュリティの両面での説明が必要となります。

表 3-1 は、自社構築とクラウドサービス利用において、コスト面、セキュリティ面の要件の違いを表したものです。

表 3-1　自社構築とクラウドサービス導入との比較

判断項目	自社構築（オンプレミス）	クラウドサービス導入
初期コスト	必要	不要
利用コスト	システム全体に係るコスト	利用分のみのコスト
災害対策コスト	高い	低い
調達期間	長い	短い
セキュリティ管理	自社の設計による	事業者のサービスによる
バックアップ	自社の設計による	オプションサービス

資料：Amazon Web Service のホームページから引用

(2) 情報活用のポイント

クラウドサービス導入に向けた経営層への説明には、以下の事項を折り込むことが重要です。

●低価格でクラウドが利用できること。

但し、必要とする処理機能が、自社構築のように痒いところに手が届くものではないこと、またデータのバックアップ処理などサービスの範囲外の項目があることは、前提として伝えておく必要があります。

●セキュリティ面で安心であること。

但し、現段階では、クラウドサービス事業者に関する監査制度は始まったばかりで、セキュリティレベルを同じ基準で判断することは難しいですが、主要なクラウドサービス事業者であれば事業者自らの事業を継続していくための必要最低限の要件は準備されていると考えられます。

表 3-2　情報セキュリティの要件

セキュリティ要件	内容
機密性 Confidentiality	その情報へのアクセスを許可された者だけが、その情報を閲覧できること。 ID やパスワードによる認証機能などを用いる。
完全性 Integrity	情報や情報の処理方法が正確かつ完全（改ざんされていない）であること。 デジタル署名機能などを用いる。
可用性 Availability	許可された利用者が、必要な時に確実にアクセスできる環境であること。 回線二重化やバックアップシステムの機能などを用いる。

表 3-2 は、情報システム監査等において定義されている情報セキュリティの 3 つの要件となります。

3.1.3 クラウドサービス事業者の選択で活用する情報

(1)必要となる情報とは

クラウドサービス事業者の選択では、自社が必要とする処理機能への対応面、及び保守・運用への対応面について、クラウドサービス事業者のサービスレベルや技術レベルの比較を行う必要があります。

(2)情報活用のポイント

経済産業省　情報セキュリティ政策室（平成２６年）の**「クラウドセキュリティガイドライン活用ガイドブック」**「4.3 クラウドサービス事業者の選択」では、

●経済産業省の**「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」**に従って情報を提供している事業者を、まず候補業者の対象にし

●事業者が第三者認証を取得しているか。

●事業者がホワイトペーパーなどを開示しているか。

などを調査し、選択要件の補完情報とすることが推奨されています。

また、

●事業者に預けるデータの種類・範囲が明確になれば、リスクが絞られ、それにより情報の重要性に見合ったセキュリティレベルや対応策が明らかになります。

表 3-3 は、JASA（平成２４年５月）**「クラウド情報セキュリティ管理基準利用ガイド」**の中で、検討すべき基本的なリスク（21 項目）を一覧にしたものです。

表 3-3　クラウドサービスに係わる基本的リスク

【リスク高】

H01	リソース・インフラの高集約によるインシデントの影響の拡大
H02	仮想／物理の設計・運用の不整合
H03	他の共同利用者の行為による信頼の喪失
H04	リソースの枯渇（リソース割り当ての過不足）
H05	隔離の失敗
H06	サービスエンジンの侵害

【リスク中】

M07	クラウドプロバイダでの内部不正－特権の悪用
M08	管理用インターフェースの悪用（操作、アクセス）
M09	データ転送途上における攻撃、データ漏えい （アップ／ダウンロード時、クラウド間転送時）
M10	セキュリティが確保されていない、または　不完全なデータ削除
M11	クラウド内 DDoS／DoS 攻撃

【リスク低】

L12	ロックインによるユーザ忌避
L13	ガバナンスの喪失
L14	サプライチェーンにおける障害
L15	EDoS 攻撃（経済的な損失を狙った DoS 攻撃）
L16	事業者が管理すべき暗号鍵の喪失
L17	不正な探査・スキャンの実施の回避
L18	証拠提出命令と電子的証拠開示
L19	司法権の違い
L20	個人データ保護の失敗
L21	ライセンス管理の失敗

一方、クラウドサービスでは、

●「フリーミアム」（Free：無料　Premium：有償からの造語）を活用し、正式採用の前に「実際に使ってみる」ことも選択要件としては効果的と思われます。

3.1.4 運用上の課題解決で活用する情報

(1)必要となる情報とは

運用上の課題は、主にシステム障害への対応や稼働状況の分析、及び稼働予測、システムの改善など、サービス利用者では管理できない事項に関してコミュニケーションを取ることが必要となります。

(2)情報活用のポイント

サービス利用者は、運用契約、SLA（Service Level Agreement）などの締結条項として記載した内容が、齟齬なく実行されているかを管理することが必要となります。

2010 年の資料になりますが、クラウドコンピューティング　ユースケース　ディスカッショングループがまとめた**「ホワイト・ペーパー（第 4.0 版）」**の「8.4　SLA に関する考慮事項」「8.5　SLA の要件」に締結の要件が記載されています。

また、前出の「活用ガイドブック」でも、

●システム／データのバックアップを定期的に取得するサービスが実行されているか、

●システム運用でのアクセス制御として、多要素認証（二段階認証、二要素認証）に対応されているか。

●管理者用ネットワークの制限ができるか

などのアドバイスが記載されています。

クラウドサービス事業者の基本サービス、またはオプションサービスとして十分な要件が揃うことが必要となります。

企業においては、自社構築（オンプレミス）からクラウドへとシステムの利用形態が移りつつあり、利用する側の意識も変えていく時期が到来しています。

今までは、ものを「所有」して、自社構築（オンプレミス）として運用・管理を行ってきましたが、クラウド環境が普及しているとはいえ、セキュリティやガバナンスの観点から、パブリッククラウドに完全移行することは、現実的に難しいものです。

そこで、利用者は、様々なクラウドサービスを適切に選択し、既存システムと連携を取りながら、ユーザ満足を図りつつ、グループ企業の全体最適化を進めていくことが必要になってきます。（図 3-1）

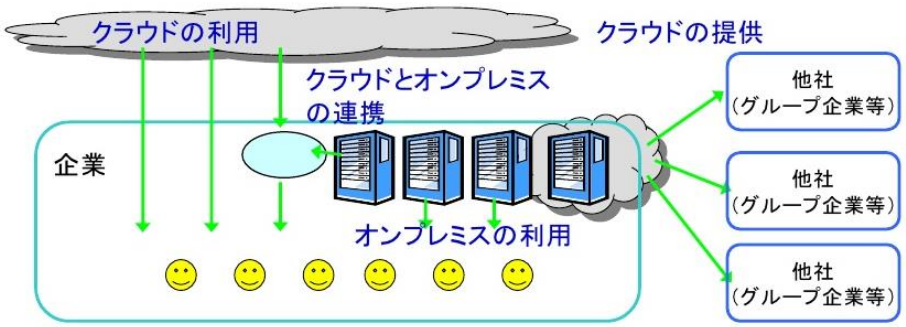


図 3-1　オンプレミスとクラウド概要

資料：http://www.slideshare.net/kurikiyo/it-presentation-792809

(1) ブラックボックス化への課題認識

自社システム（外部委託を含む）の場合、サービス品質（仕様変更）をコントロールでき、障害発生時も、原因の究明や復旧に迅速な対応を取ることができでいましたが、クラウドサービスの場合、メンテナンスなどの手間がかからず、利用が簡単になる反面、基本的に内部構成はブラックボックス化されているため、障害発生時の原因と復旧の目途も立ちにくいという懸念があります。

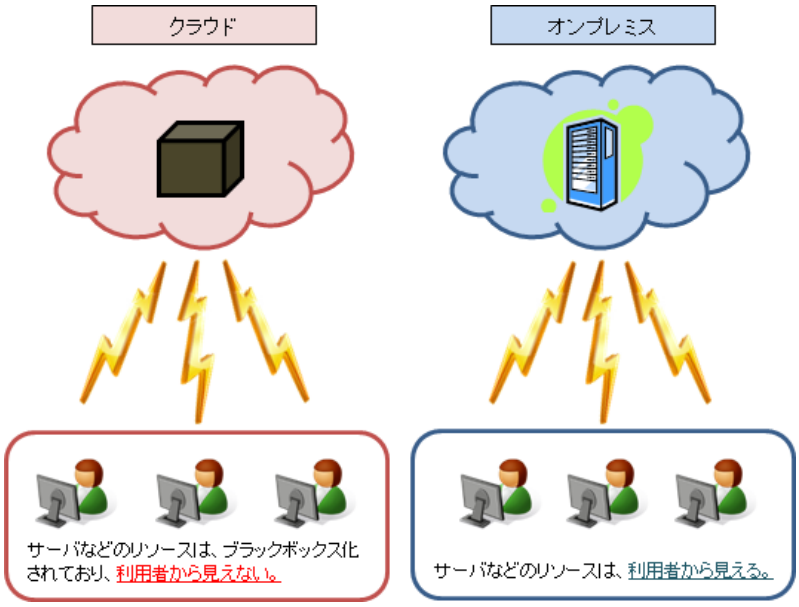


図 3-2　システムのブラックボックス化

特にパフォーマンスに関して、適切に管理（パフォーマンス問題の有無、責任範囲等）するために、サービスレベルを明確にする必要があります。

利用者として重要なのは、「エンドユーザとして、快適にサービスが利用できているかどうか」という観点で把握することが必要です。

(2) 情報（データ）に対する利用者責任の認識

クラウドサービスは、様々な情報（データ）保管を外部委託する仕組みであるが、最終的に情報（データ）に対して責任を負うのは、今までと同様、利用者側にあることを認識しておく必要があります。

また、日本以外の国や場所にデータセンタが設置されることで、情報の取扱いの違いや現地の規制当局による情報の差し押さえなどのリスクがあることを認識しておく必要があります。そこで、第 4 章の契約書等を活用したリスクコントロールが重要となります。

コラム　「ガイドライン」の活用

クラウドサービス関連のガイドライン等は、表 3-5 のような構成で、多種多様となっており、利用者は利用分野によって、使い分けていく必要があります。

ここでは、表 3-5 の中から、分野共通に利用できる（利用者だけでなく、事業者にも利用できる）ものとして、経済産業省から 2014 年 3 月 14 日に公表されているガイドライン・ガイドブックの概要について示しました（表 3-4）。

表 3-4　経済産業省ガイドライン・ガイドブック概要

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（2013 年度版）	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）
情報セキュリティマネジメントのベストプラクティスをまとめた国際規格（ISO/IEC27002：2005）を参照して、情報セキュリティ確保のため、以下の内容が解説されている。 ① クラウド利用者自ら行うべきこと ② クラウド事業者に対して求める必要のあること	以下の内容が具体的に解説され、ガイドラインの参照先が示されている。 (1) クラウドサービスの構造 (2) クラウドセキュリティの考え方 (3) ガイドラインを利用したリスク分析手法 (4) クラウド利用者のためのガイドライン活用 (5) クラウド事業者のためのガイドライン活用 (6) クラウド契約時の契約書やサービスレベル合意書（SLA）

資料：http://www.meti.go.jp/press/2013/03/20140314004/20140314004.html

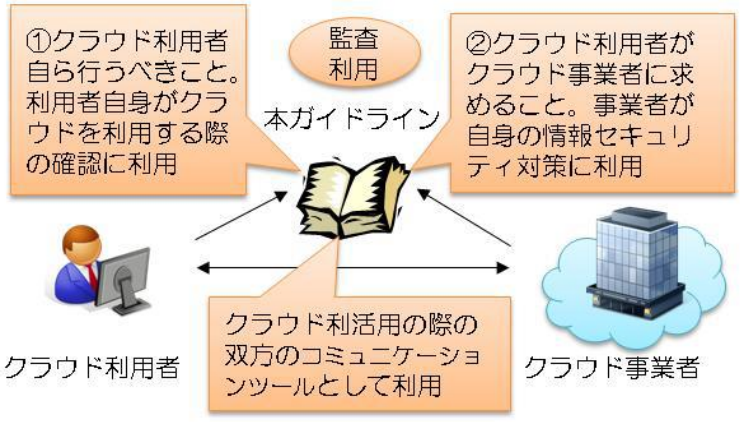
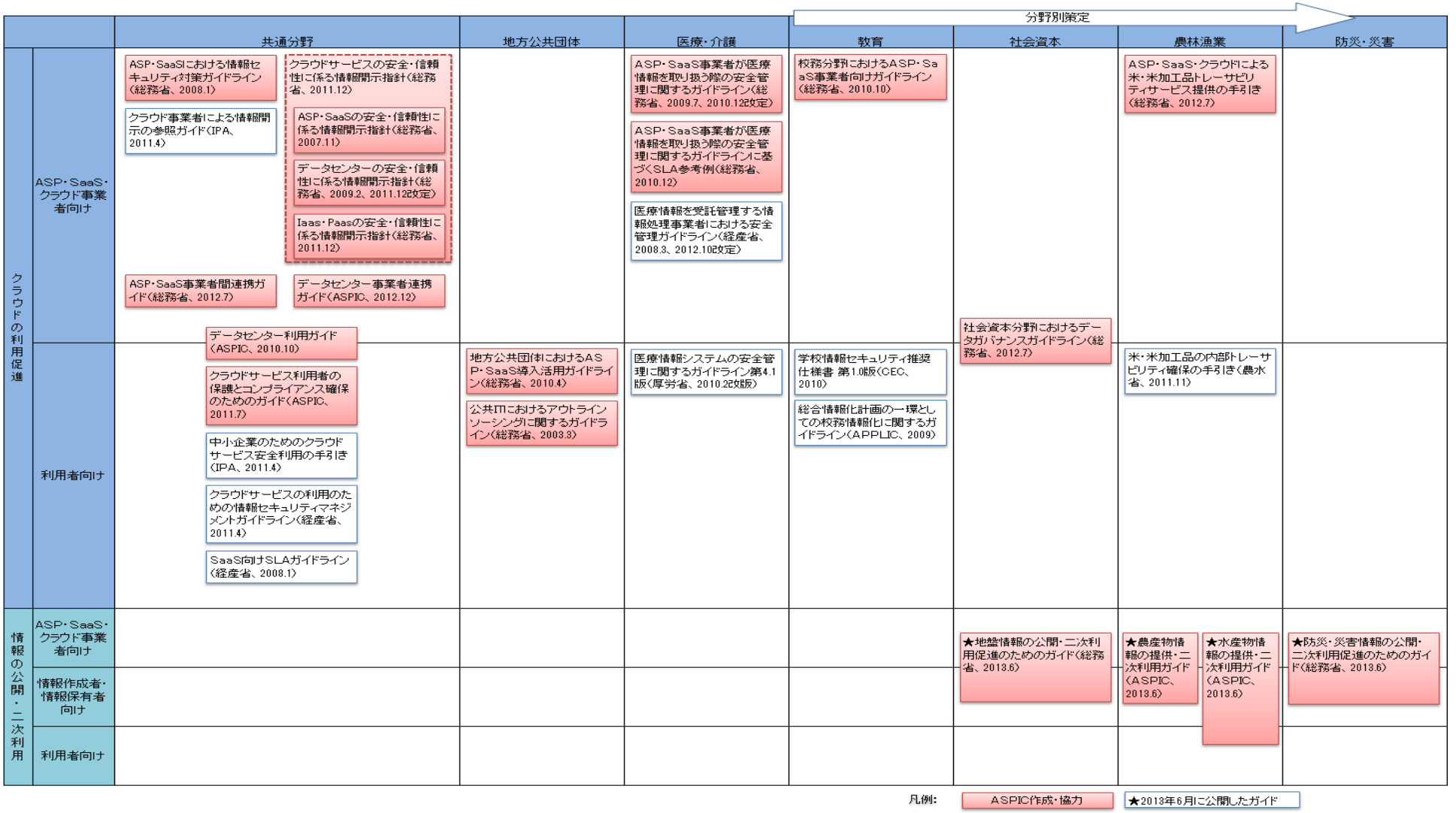


図 3-3　ガイドラインの利用方法の例

資料：http://www.meti.go.jp/press/2011/04/20110401001/20110401001.html

表 3-5　ASP・SaaS・クラウド関連のガイドライン・指針等（全体像）



資料：http://www.aspicjapan.org/event/forum/2013/file/aspic01.pdf

4. クラウドサービス契約

本章ではクラウドサービス契約についての考慮点を示します。第 2 章ではクラウドサービス利用に係わるリスクについて述べました。クラウドサービス利用に関わるリスクをコントロールする手段の一つにクラウドサービス事業者とのクラウドサービス契約があり、サービス利用者は第 3 章の各種情報収集・評価と併せて検討する必要があります。

オンプレミスの場合は、組織的安全管理措置、人的安全管理措置、物理的安全管理措置、技術的安全管理措置の対応状況は、自社の管理基準に基づき網羅的に正確かつ詳細に把握できます。したがって、一部の安全管理措置が対応できていなくても他の安全管理措置の実施によるリスク軽減策等でリスクをコントロールでき残存するリスクも正確に把握できます。

クラウドサービス利用の場合は、各種安全管理措置の対応状況は、クラウドサービス事業者からの収集した情報に基づきサービス利用者の各種安全管理基準に基づき自己評価しリスクを評価する必要があります。リスクがあると評価した場合は、リスクを許容してクラウドサービスを利用するか、クラウドサービス事業者にリスク軽減策の実施を依頼することになります。このように、クラウドサービス利用者との取り決め事項は契約で明記してリスクをコントロールしていく必要があります。

オンプレミスに情報システムを構築する場合は、自社の開発・運用管理基準（ガイドライン）に従い、業務システムの機能要件、非機能要件をシステム設計書として定義します。クラウドサービスの利用に際しても、「設計書」を代替する何らかの文書でサービス利用者側の要件等を確認する必要があり、その一部に「契約書・SLA」等があるという考え方です。

4.1 契約書

4.1.1 クラウドサービス利用時の契約書

クラウドサービス利用時は、外部委託でオンプレミスにシステムを構築し運用する場合の契約条項の他、クラウドサービスの特性に応じた契約条項を追加する必要があります。

(1) クラウドサービスの機能要件

クラウドサービスの利用は既に出来上がっている情報システムの利用であり、サービス利用者は、機能要件の根幹部分が満たされているか事前に十分確認する必要があります。オンプレミスの場合はオーダーメードシステム構築の場合はもちろんのこと、ASP の利用

であってもカスタマイズ等である程度柔軟に対応できます。クラウドサービスはマルチテナントが前提のサービスですので、機能要件を満たさない場合は自社向けの個別対応はできないことを前提とすべきです。言い換えればクラウドサービスの機能をそのまま利用し、サービス利用者側の業務をクラウドサービス機能に合わせて利用するというスタンスが必要です。仮に、クラウドサービス事業者との交渉過程で、業務機能の追加、変更を実施するという取り決めが成立するのであれば、この取り決めは契約書・SLA で明確にすることを推奨します。

(2) クラウドサービスの非機能要件

クラウドサービス利用に際し、機能要件の事前検討は当然のこととして実施されます。しかし、非機能要件の検討は、後回しになったり、十分な検討がなされないまま導入後にこんなはずではなかったとトラブルになったりすることがあります。クラウドサービスの利用では、システム運用をクラウドサービス事業者に任せることになりますので、以下の基本的な非機能要件は事前に検討し、契約書や SLA に明記する必要があります。

- 性能、キャパシティ要件
- セキュリティ要件
- サイバー攻撃対策要件（含むコンピュータウイルス対策要件）
- 運用要件
- 障害対策要件
- 災害対策要件

(3) コンピュータセンタ

クラウドサービスは、クラウドサービス事業者のコンピュータセンタで運用されます。国内法が適用できる日本国内に存在するか等基本的な確認の他、可用性の高い業務でクラウドサービスを利用する場合は、災害対策としてのバックアップセンタの有無、耐震強度、津波等による水害対策、自家発電装置等電源喪失時の設備、液状化対策、システム運用要員確保等の確認の他、実際にコンピュータセンタを見学することを推奨します。

4.1.2 契約条項

契約書は、クラウドサービス事業者が作成した契約書を利用することになります。クラウドサービスの契約書に限らず、契約書を作成する側に有利な内容の契約書になっていると思われるので、特に損害賠償、準拠法等の内容は十分確認する必要があります。

表 4-1　契約条項(例示)

項番	契約条項	備考:サービス利用者側の確認事項等
1	契約の成立	契約の自動継続条件等の確認
2	本サービスの利用料	利用料の他、各種コスト等の確認
3	本サービスの利用方法	アカウント情報(ユーザ ID、パスワード)の適切な管理・使用。特に共用 ID の管理状況確認。
4	サービス利用者データの取扱い	機密性の高い情報の情報漏えい対策は、詳しく確認
5	バックアップ	役割・作業分担、追加費用の有無確認
6	禁止事項	事業者のデータアクセスについて禁止等、事業者側の禁止事項についての網羅性確認
7	譲渡禁止	クラウドサービス事業者側の業務継続(譲渡禁止)も必要に応じて取り決めが必要
8	本サービスの一時的な提供停止	SLA で具体的に定義必要
9	本サービスの廃止	クラウドサービス事業者側の業務継続も必要に応じて取り決めが必要(項番 7 と同様)
10	本契約終了後の処理	情報漏えい対策が必要
11	損害賠償の制限	損害賠償金額等の妥当性について確認
12	免責	免責となる損害の内容について確認
13	本利用規約の変更	クラウドサービス事業者が一方的に有利な内容になっていないか確認(利用料金の変更等)
14	輸出法の遵守	データセンタ等の所在地確認が必要(国内、国外)
15	合意管轄	クラウド事業者の所在地確認が必要
16	準拠法	個人情報保護法等国内法の適用対象か確認が必要(データセンタの所在等確認)
17	再委託	再委託は原則禁止、再委託時は事前承認する契約を推奨
18	監査	必要に応じてサービス利用者が監査できる内容の条項追加を推奨

資料:「クラウドセキュリティガイドライン活用ガイドブック」の項目に必要と判断された「再委託」「監査」を追加。

4.2 SLA

4.2.1 SLA の構成要素

SLA はクラウド利用契約書の補足事項として作成され、契約書の付属書類として添付されます。SLA を添付しないクラウドサービス事業者が散見されますが、サービス利用者としてはクラウドのサービスレベルは SLA に基づき確認することを推奨します。

なお、SLA は契約書の付属書類であるにもかかわらず「努力目標」としての規定に留めた項目がありますので、内容は十分確認する必要があります。

表 4-2　SLA(例示)

項番	SLA 項目		備考:サービス利用者側の確認事項等
1	アプリケーション運用	サービス提供時間	業務要件を満たすか確認
2		オンライン応答時間	マルチテナント要因等による応答時間の劣化を許容できるか確認
3		バッチ処理時間	同上
4		カスタマイズ性	定期的、定型的な変更は、サービス利用者自身で可能か確認
5		外部接続性	他のアプリケーションとの連携が可能か確認(API の提供有無を確認)
6		同時接続利用者数	業務要件を満たすか確認
7		利用者への通知	障害発生時のサービス利用者への通知対象内容、通知方法が妥当か確認
8		ディザスターリカバリ	バックアップセンタ、データの隔地保管の有無。サービス再開までに要する時間、どの時点まで回復可能か等を確認
9		重大障害時の代替手段	CP、業務 CP(BCP)の内容を確認
10	サポート	サポート窓口	連絡先が具体的に定義されているか確認
11		サポート緊急窓口	同上。特に、夜間、休祭日の窓口が定義されているか確認
12		サービス提供状況の報告方法	月次報告等、定期的な報告の有無を確認
13	データの管理	バックアップの方法	データ保全方法を具体的に確認
14		ログの取得	個人情報等機密性の高いデータを取り扱う場合は、取得するログの種類、保管期間、保全手段等の確認
15	セキュリティ	情報取扱者の制限(サービス利用者)	自社のセキュリティ管理基準で定めているアクセスコントロール要件を満たすか確認
16		情報取扱環境(クラウドサービス事業者)	クラウドサービス事業者は、システム的に情報にアクセスできないこと、物理的にもアクセスできない環境であることを確認
17		通信の暗号化レベル	公衆回線を利用する場合は、暗号化しているか確認
18		ウイルス対策管理	既知のウイルス対策はもちろん、未知のウイルス対策状況も確認
19		公的認証取得	ISMS、プライバシーマークの取得状況を確認。なお、ISMS の場合は利用するクラウドサービスが取得対象であることを確認
20		サービスに関する第三者評価	Web アプリケーション診断、ペネトレーションテスト、ネットワーク・サーバの脆弱性診断等の脆弱性診断を定期的に実施していることを確認

資料：経済産業省「クラウドセキュリティガイドライン活用ガイドブック」

4.3 チェックリスト

クラウドサービスの評価を行う場合、自社の開発管理基準、セキュリティ管理基準等に基づく各社固有の「チェックリスト」を利用して、クラウドサービス事業者に各種基準の実施状況を確認するケースが多いと思います。

また、クラウドサービス事業者がホームページ等で公開している情報、クラウドサービス事業者から提供されるサービス仕様書、パンフレット、概要書等でクラウドサービスを評価することもあると思います。

事業者との約束事、事業者から収集した情報、及び事業者が公開している情報は、当事者間での合意事項として契約書・SLA に記載することを推奨します。クラウドサービス事業者との関係で契約書・SLA に記載できない事項は、サービス利用者が自らの責任で情報を整理し、契約書・SLA とは別に文書化して当事者間で確認することを推奨します。契約書・SLA 以外の文書は法的な効力はないかもしれませんが、口頭での確認とは異なり、クラウドサービス事業者の各種管理基準の確認結果が文書で残りますので、各種管理基準、セキュリティ管理基準について、一定水準以上の実効性が確保できると思われるからです。

4.3.1 チェックリストの活用事例

(1) クラウドサービス利用時の基本的なチェック項目

経済産業省の「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」末尾付録に「クラウド利用における実施の手引き一覧」があり、チェックリストとして活用することが可能です。この手引きは同一のチェック項目に対して、クラウド利用者の立場で自らが実施すべき事項とクラウドサービス事業者が実施すべき事項とが併記され、それぞれの立場で確認できる内容ですので、双方のコミュニケーションツールとして有効活用できる内容となっています。

また、この一覧は ISO27002 を基準に作成されていますので、情報セキュリティ管理基準を網羅的に確認できるものです。

(2) システムの特性に応じた追加チェック項目

クラウドサービス利用に関わるリスクの中で、情報漏えいリスクは最もリスクの高いリスク項目の一つです。「クラウドサービスの利用者の範囲」や「クラウドサービスで取り扱う情報」等クラウドサービスの特性に応じて、情報漏えいのリスク度は異なりますが、クラウドサービスは、インターネットに公開されるシステムですので、特にサイバー攻撃による情報漏えいリスクについて評価することを推奨します。

① クラウドサービスの「利用者」による分類

・利用者を特定しないクラウドサービス

インターネットに公開するホームページ、オンラインショッピング、インターネットバンキング等が該当します。サイバー攻撃を受けるリスクが高く、サイバー攻撃対策について一歩踏み込んだ確認が必要です。

・取引先が利用するクラウドサービス

EDI 等特定の取引先が利用するシステムで、VPN 等専用ネットワークで接続したり、アカウント（ユーザ ID,パスワード）等によりアクセスを制限したりして利用するため、利用者は限定されます。上記の利用者を特定しないクラウドサービスと異なり利用者が限定されますが、機密性の高いデータを取り扱うことが多いと思われますので、サイバー攻撃対策について評価することを推奨します。

・社内で利用するクラウドサービス

業務系基幹システム、商品・顧客管理システム等分析系システム等社内での利用に限定されるシステムで、利用者が従業員に限定されるシステムです。機密性の高いデータを取り扱うことが多いと思われますので、サイバー攻撃対策について評価することを推奨します。

② クラウドサービスで「取り扱うデータ」による分類

・機密性の高いデータを取り扱うクラウドサービス。

経営情報、取引先の信用情報、顧客の個人情報、社員の人事情報等、機密性の高いデータを取り扱うクラウドサービスは、サイバー攻撃対策について一歩踏み込んだ確認が必要です。

・・・社内基幹系システムの他電子メール、社内掲示板、ファイルサーバ、Web 会議システム、大容量ファイル転送システム等の周辺システム

・公開情報等情報を取り扱うクラウドサービス。

機密性の高いデータは取り扱いませんが、情報の改ざん、ウイルスを埋め込まれるリスクがありサイバー攻撃対策について評価することを推奨します。

・・・ホームページ等

⑶ システムの特性に応じた追加チェック事項の例示

チェックリストとして活用できるものを例示します。

① サイバー攻撃対策

IPA からサイバー攻撃対策のチェックリストが公開されていますので、以下にチェッ

クリストとして例示します。

表 4-3　サイバー攻撃対策「チェックリスト」　（例示）

技術的　対策事項	
（1） システムへの入口と経路での防御	
	□　ファイアウォール
	□　最新のウイルス対策ソフト（ネットワーク、サ
	□　侵入検知システム／防止システム
	□　通信路の暗号化（Virtual Private Net
	□　ネットワーク構造／設計（重要なサーバーにトからの隔離）
（2） 脆弱性対策	
	□　OS やサーバーソフトウェアの定期的な脆弱
	□　ウェブサイトで使用しているOS やサーバーソ性情報の、時期を
	逸しない収集とパッチの反映　3）
	□　ウェブアプリケーションへの脆弱性の作り込み
	□　ウェブアプリケーションファイアウォール（WA
（3） 標的型攻撃ルート対策	
	□　スパムフィルター
	□　URL フィルター
	□　外部メディア利用規則、強制利用抑止
（4） ウイルス活動の阻害および抑止（出口対策）	
	□　端末間、他部署間のネットワーク通信の制限抑止）
	□　組織の端末からの外部通信はプロキシを経由
	□　組織内ネットワーク量の監視（異常さを早期に を早期に発見）
	□　知財等のある重要なサーバーはインターネッ
（5） アクセス制御	
	□　ユーザ認証
	□　アクセスするプログラムの特定（ホワイトリス
（6） 情報の暗号化	
	□　暗号
	□　暗号鍵管理
（7） システム監視、ログ分析	
	□　ネットワークログ取得・分析
	□　サーバログ取得・分析
	□　アクセスログの監査（DB 監査ツールなど含
（8） 管理統制およびコンテンジェンシープラン（事前準	
	□　セキュリティポリシー
	□　海外を含むグループ会社間でのセキュリティ
	□　危機対応体制の整備

資料：IPA「セキュリティ対策状況チェックリスト」http://www.ipa.go.jp/files/000008962.pdf

③ 個人情報保護対策

個人情報保護法に係わる各種管理策を具体化したものに、経済産業省の「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」があります。

経済産業省の「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」末尾付録の「クラウド利用における実施の手引き一覧」と重複するチェック項目が多いですが、クラウドサービスで個人情報を取り扱う場合は、個人情報保護法の法令遵守という観点でチェックリストとしての活用を推奨します。

4.4 監査

4.4.1 監査制度の活用

クラウドサービスに関わる契約書・SLA の内容確認、及びチェックリスク等による情報収集、分析、評価には、相応のスキルと時間を要しますし、100%正しい情報収集や評価ができるとは思えません。一歩踏み込んで自らがクラウドサービスを監査するという方法がありますが、監査の実施は相応の費用等が必要になりますので現実的な対応ではありません。

サービス利用者は、利害関係のない第三者による客観的な評価結果を得ることができれば、安心してクラウドを利用することができます。クラウドサービス事業者自らが、第三者による監査を受け、監査結果を広く利用者に開示する制度の整備が望まれます。具体的には、クラウド情報セキュリティ監査制度として JASA 監査制度等が制度として定着が望まれます。

サービス利用者としては制度の整備を待つだけではなく、開示された監査結果を評価するスキルが必要ですので、自らが情報セキュリティ管理体制の整備、ノウハウの蓄積が必要となります。

5. クラウドサービス事業者への提言

本章では、企業がクラウドサービスを導入（もしくは導入の検討）をするにあたり、クラウドサービス事業者へ期待することを取りまとめます。これは、クラウドサービス事業者が、数ある競合事業者の中から自社を“選んでもらえる”ための提言ともなります。クラウドサービス事業者が本章の提言を取り入れることにより、企業がクラウドサービスを導入するか決断する際、及び、事業者選定をする際の一助となることを期待します。

5.1 情報開示について

企業がクラウドサービスの導入を判断するにあたっては、第 2.1.2 章に記載したとおり、コストの他に、情報漏えいや情報消滅といったセキュリティ面や事業継続性についてのリスクを考慮する必要があります。しかし、特にセキュリティに関してはクラウドサービス事業者から得られる情報は十分といえないのが実情です。

5.1.1 統一的な開示項目と開示基準の策定

利用者側として知りたいのは、安全かどうかということ、利用者が受ける制約（あるいは許容すべきリスク）は何かということであり、セキュリティ対策内容の仔細について評価することは稀です（クラウドサービスで実現しようとする業務内容によっては、仔細な情報が必要となる場合もあります)。

例えば、利用者のデータを扱うクラウドサービスについて、データの保管場所はどこか、どのように守られているか（概要)、破損や消滅する可能性はあるのか、破損や消滅した時の復旧手段はあるのかなど、利用者が気にするポイントはある程度絞られるものと思います。クラウドサービスの導入を検討している企業は、上記のような事項を複数のクラウドサービス事業者に問い合わせますが、クラウドサービス事業者側も積極的には情報開示をしていないため、一度で満足できる回答を得られることは稀です。よって企業側は情報収集の段階において、多大な時間と労力を要することが多いのが実情です。

クラウドサービス事業者が、利用者が気にするポイントを想定し、ある程度統一的な開示項目と基準を策定して積極的に公開（または、すぐに開示できる準備）することが、クラウドサービスの導入促進につながるものと期待されます。

5.1.2 わかりやすい説明（情報開示）

わかりやすい説明を心がけることも必要です。例えば、重要なデータを扱う業務について、オンプレミスとするのかクラウドサービスを利用するのか検討する場合、セキュリティ面は大きな判断要素となります。クラウドサービス事業者は、細かなセキュリティ対策を説明するよりも、どうして安全なのかをわかりやすく説明できることも必要です。もち

ろん仔細な情報を公開できるに越したことはありませんが、公開できる範囲に制約がある場合には、制約がある中でいかに安心してもらえる説明ができるかが鍵です。

例えば、企業はお金や証券類はどこに保管するでしょうか。一般的には、銀行に預けることが多いかと思います。その際、保管場所、その場所へのアクセス制御方法、金庫のロック解除の仕組みなどを気にすることはほとんどありません。セキュアな場所に保管されているということ、預貯金が失われるリスクもあるものの、ある一定額は保障されるという対策が明らかになっているため、利用者は安心して利用することができます。一方で、企業保有の金庫等に保管する場合もありますが、手元にあるという安心感やすぐに取り出せるという利便性と引き換えに、盗難にあうというリスク対策にコストと労力をかける必要があります。

極端な例を紹介しましたが、クラウドサービスについても同様、利用者が安心できる情報を、要点を押さえていかにわかりやすく提供できるか、が導入促進につながります。

但し、利用者にとって不利となるような情報（リスク）を包み隠してはいけません。リスクがあるならば開示し、許容できるかできないかを企業側に問うことも、信頼を得ることにつながります。

コラム　クラウドサービス事業者認定制度

現在のクラウドサービス事業者は、認定制度や監査制度がないために、利用者が事業者の選択を間違うと大きな痛手を受けることがあります。情報漏えいやデータ消滅、最悪の場合は、事業継続が困難になる可能性も否定できません。

この問題を改善すべく、JASA のクラウドセキュリティ推進協議会では、クラウドサービス事業者を認定する「クラウド情報セキュリティ監査制度」の準備を進めているそうです。

「クラウド情報セキュリティ監査制度」とは、どのようなものかをレストラン（飲食店）と比較して考えてみましょう。

日本の飲食店では、「調理師法」「食品衛生法」「公衆衛生法」の 3 つの法律により必要な資格や管理が行える店（人）のみ営業が許可されます。これにより、日本の飲食店では「味」はさておき、衛生面ではどこに行っても安心して食事をすることができます。

クラウドサービス事業者認定制度では、「資格認定制度」「管理基準と監査」「審査制度」の 3 つの制度を整備し事業者を認定します。

まず、資格認定制度でクラウドのセキュリティを正しく評価できる監査人を認定します。次に、クラウドに適した情報セキュリティの管理基準を規定して内部監査を行います。そして、この制度が適切に運営されるように、JASA の審査制度で公正な監査が行えるようにします。

これにより利用者が安心してクラウドサービスを利用できるというものです。
クラウドサービス利用者の「何がセキュアかわからない？」「説明も理解できない？」といった声に対して、認定されたクラウドサービス事業者は監査を正しく受けていることを言明（情報セキュリティ宣言）することで、細かな要件を見なくてもサービスの信頼性を確保することができようになります。

この制度が浸透してクラウドサービスが安心して利用できる環境が整えば、飲食店の検索サービスにあるような、利用者の「味」や「サービス」に関する評価がクラウドサービスにもあればと切に願うばかりです。

いずれにせよ、利用者である情報システム部門は、これまでの「システムを作るスキル」から「利用するスキル」へとスキル転換を求められそうです。

コラム　クラウドサービスに関する経営層への説明・説得ポイント

経営層への説明・説得に必要となる要素は概ね、コストと信頼性に関する優位性です。オンプレミスで実現する場合との比較にて、クラウドサービスのメリットを示します。

(1) システム見直しに至った経緯

現状の課題（機器の老朽化、運用コストや運用負荷の増大など）を含め、まずは経緯を説明します。

(2) オンプレミスとの比較

機能面、運用・保守面、信頼性、拡張性・柔軟性、コスト（大小レベル）等について、クラウドの優位性を簡潔に説明します。（一覧表などにまとめると良い）

(3) コストメリットの説明

初期コストと数年間の運用コストの合計について、オンプレミスとの比較を行います。現状からどれだけ（何%程度）コストダウンできるかについても言及すると効果的です。

(4) 信頼性の説明（安全・安心であるということ）

最終的に経営層が導入を決断するためには「本当にその外部サービスを使って大丈夫なのか？」という漠然とした懸念（心配）を払拭する必要があります。（クラウドサービスの導入を躊躇する一つの大きな要因として、不安を払拭するに至らないことが挙げられます）

セキュリティに関してはクラウドサービス事業者から得られる情報は限られることが多いですが、クラウドサービス事業者にも協力を仰ぎ、簡潔かつ説得力のある説明を記述するようします。

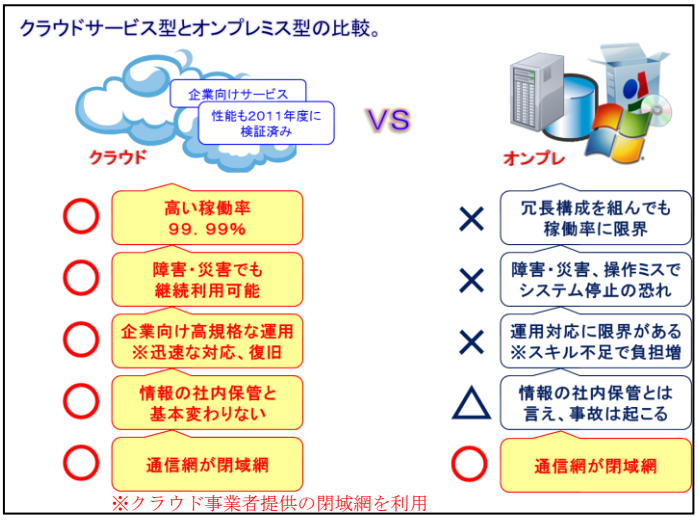


図 5-1　信頼性の比較説明例

なお、いかにも日本的な慣例ではありますが、当該クラウドサービスの他社導入実績や導入事例を示すことも、安心感を得てもらうための有効な手段となります。

まとめ

この報告書では、クラウドサービスの現状、想定されるリスクとその対策の考え方をまとめてきましたが、作業の中でさらに実情の認識を持つため、協議会メンバーの自社事例を開示して頂き参考情報と致しました。

しかし、クラウドサービスを本格的に導入している会社が少なく、サンプル事例も限定的なものとなりました。

そこで、より実態を把握するため、JASA のご担当者との意見交換を行い、クラウドサービス事業者の監査制度について説明を頂き、クラウドサービスの信頼性や、事業者の選択、また契約締結について具体的なお話を聞かせて頂きました。

また、独立行政法人　情報処理推進機構（IPA）のご担当者から、「ガイドラインとガイドブック」と題して、サービス利用者としての利活用の解説頂きました。

報告書作成に向けては、テーマを絞って集中討議を開催するなど、課題に対して十分な検討が行われ、またお互いの気付きの機会ともなり、成果が得られたと思います。

今後、クラウドサービスの導入は急速に展開されると推測されますが、事業者と利用者がお互いの役割を認識し、締結された契約に基づき実行されることが重要となります。

この報告書が、読者の皆さまの良きヒントになればと思います。

最後に、ワーキンググループ２の皆さん、外部の講師としてご協力頂いた方々、本年度の作業ありがとうございました。

事務局　　川口　修司

用語集

クラウド

情報システム（アプリケーション、ミドルウェア、OS、ハードウェア等）を、ネットワークを通じ、サービスの形で必要に応じて利用すること。

オンプレミス

情報システムを自社の設備に導入・設置し、運用すること。

SaaS (Software as a Service)

ユーザが必要とするソフトウェアの機能だけをサービスとして配布し､利用できるようにした形態。

検討メンバー

■メンバー

グローバルセキュリティエキスパート株式会社	多山　信彦
株式会社京王 IT ソリューションズ	古宮　敏雄
住友商事株式会社	北方　孝好
積水化学工業株式会社	平尾　安明
株式会社高島屋	上原　佳都雄
デロイトトーマツリスクサービス株式会社	丸山　満彦
日本コムシス株式会社	杉本　博之

（社名五十音順）

（事務局）

株式会社三菱総合研究所	川口　修司
株式会社三菱総合研究所	江連　三香