IPA Information-technology Promotion Agency, Japan

中小企業のための

クラウドサービス

安全利用の手引き

２０１１年４月

独立行政法人情報処理推進機構

中小企業のためのクラウドサービス安全利用の手引き

はじめに

クラウドコンピューティングが注目を集めています。クラウドコンピューティングをうまく活用すると、従来より少ない負担で IT を利用したり、IT のより高度な活用が図れる可能性があります。特に IT 利活用に十分に取組めていなかったり、IT の負担が重いと感じる中小企業にとっては、IT の利活用を進めるチャンスとなる可能性が大きくあります。

しかし、中小企業にとっては、クラウドとはどういうものか理解しにくかったり、どう使えばよいかわかりにくかったり、正しく使えないためにデメリットが勝ったりといったことも起こりえます。

そこでこの手引では、クラウドの利用についての判断やその条件の確認、注意点の点検等が、比較的容易にできるように、解説やチェック項目を整理しました。

本書を活用することで、多くの中小企業の方々が、クラウドを正しく安全に利用し、IT 利活用の効果を経営に活かし、また IT セキュリティのレベルアップを実現されることが期待されます。

なお、利用に際しては以下の点に留意してください。

- 利用企業はITをある程度活用しているレベル[1]であることを想定しています。
- クラウドサービスの種類として SaaS の利用を念頭に置いた確認項目を記しています。PaaS や IaaS の利用に際しては、別の確認項目や注意が必要になる場合があります。別途情報を確認するとか、詳しい人に相談することをお奨めします。（SaaS、PaaS、IaaS の意味については脚注 2 参照）
- 本書の利用主体は中小企業の経営層を想定しています。IT 担当部門の関与が必要な場合には、IT の管理責任者や担当者にも活用いただけます。軽微な案件は経営層の関与がなくても IT 担当部門で判断可能なケースもありえますが、原則として、クラウドの利用判断に当っては経営層の関与があることを前提としています。

[1] 経済産業省の定める IT 経営力指標において、ステージ２と定義されるレベル<末尾の参考情報参照>を基本とし、ステージ 1 の中で 2 に近いレベルの層も一部含む。

1．クラウドコンピューティングとは

● クラウドコンピューティング、クラウドサービスとは

クラウドコンピューティングとは、大規模データセンターにおいて仮想化等の技術を用いてコンピュータの機能[2]を用意し、それをインターネット経由で自由に柔軟に利用する仕組みの総称です。企業や個人が個別にコンピュータやアプリケーションを所有して利用するのに比べて、ITに関する開発や調達や運用･保守の負担が軽減され、コスト削減にもなる技術、サービスとして注目されています。

クラウドサービスとは、クラウドコンピューティングに基づいて、サービスの形で提供される IT の機能と言うことができます。本書では「クラウドコンピューティングによるサービス」を「クラウドサービス」と表記することとします。また、クラウドサービスを提供する事業者のことを「クラウド事業者」と表記します。

● 中小企業にとってのクラウドサービス活用の利点

クラウドサービスでは、「持つ IT」から「利用する IT」に転換できることから、以下のような利点があると考えられています。

（ア）IT の調達に関わる負担からの解放または負担の軽減

- サーバ、ストレージ、ネットワーク等の仕様決め、入手、設置、設定等
- アプリケーションソフトウェアの開発や調達
- 処理量の増大に対応した能力増強
- 設備やシステムの更新
- これらに伴う初期コスト、資本投下負担

（イ）IT の運用・保守の負荷からの解放または負荷の軽減

- IT 設備やシステムの運転、定期点検、トラブルシューティング等
- OS やアプリケーションのアップデート、パッチ適用、トラブルシューティング、バージョンアップ、ライセンス管理等
- 社内ユーザへのサポート、ヘルプデスク、アカウント管理等
- これらに伴うベンダとの連絡、折衝等

（ウ）IT 資源利用の柔軟性・拡張性の獲得

- 処理量、利用量の増減に対応して IT 使用量の増減が可能（持つ IT の場合はピーク量に合わせた容量が必要。減少に対応した対策は実質不可能）
- 急激な負荷変動にも柔軟に能力増強が可能（設備増強のリードタイムが不要）

---

[2] 「コンピュータの機能」は様々なレベル・形で提供される。ハードウェアやネットワーク、OS などの情報システム基盤を提供するサービスを IaaS（Infrastructure as a service）、アプリケーションの実行環境を提供するサービスを PaaS（Platform as a Service）、アプリケーションを提供するサービスを SaaS（Software as a Service）と呼ぶ。この他にもあるサービスをネットワークを通じて提供することを XaaS（X as a Service）と呼ぶことがある。

（エ） セキュリティ対策の負担と負荷からの解放または負担軽減

- ファイアウォールの設定や変更、不正アクセス監視の負担の軽減
- サーバのマルウェア対策や OS のアップデート、セキュリティパッチの適時適用などの負担の軽減
- スパムメールやウイルスつきメール等のフィルタリング負担の軽減

● クラウドサービス利用上留意すべき事項

クラウドサービスの利用には、いくつかの懸念材料も指摘されています。

（ア） コンピュータシステムを自ら管理しないことによる制約

- メンテナンス時期の選択
- 障害時の復旧のコントロール
- 機能の選択肢の限定　等

（イ） データを自らの管理範囲外に置く、あるいは社外に預ける不安や制約

- 万一の障害時のデータの完全性・可用性の確保がコントロール困難
- 委託先管理要求に対応したコントロール実現が困難　等

（ウ） 利用量・処理量の異常な増加や意図せぬ増大に伴う使用料の急増のリスク

（エ） 利用できるアプリケーションのカスタマイズの制約

（オ） アプリケーション間のデータ連携実現への制約やコスト増の可能性

これらの懸念材料については、自社の状況やクラウド事業者の情報を総合的に判断して、リスクを見極め、対策を施した上でクラウドサービスを利用する必要があります。

2. クラウドサービスはこんな形で活用されています

クラウドサービスは、パソコンやスマートフォンなどの高機能端末から、インターネット経由で利用できます。様々なサービスが数多くのクラウド事業者から提供されているので、自社のニーズに合ったサービスの選択やクラウドサービスを活用して業務改善を図るといった利用が可能です。料金は利用時間や利用量に比例する形が一般的で、月額固定方式や年額制の場合もあります。

実際に使ってみることがクラウドサービスを知るための近道です。クラウド事業者の中には、試用期間を設けていたり、少人数の利用について無料提供を行っていたり、機能限定版を無料提供している場合があります。業務アプリケーションは、実際に使ってみないとわからないことがありますので、試用について積極的にクラウド事業者に問い合せてみることをお奨めします。

クラウドサービスの活用例として、いくつかのサービスの事例を紹介します。

2.1. 活用事例：電子メール

比較的容易に導入できるクラウドサービスとして、電子メールサービスが挙げられます。自社でメールサーバを持たないことで機器の費用を軽減することができますし、サービスの管理・運用を外部に委ねることで、自社のシステム管理負担を軽減することができます。スパムフィルタリングやウイルスチェックなどのセキュリティ対策もクラウドサービス側で提供される場合が多く、自社での対策負担が軽減されます。

また、世界中どこからでも、インターネットアクセスさえ可能なら、同じメール環境を利用できるので、仕事の機動性が高まります。手元のパソコン等にコピーを残さなければ、情報の紛失・漏洩リスクも軽減できます。

2.2. 活用事例：経営管理アプリケーション

財務会計、税務計算、給与計算、人事管理、顧客管理などの経営管理のためのアプリケーションを、クラウドサービスとして利用することもできます。専用のサーバや端末が不要、ソフトウェアのインストールやアップデートが不要なので、それらのための初期投資や維持管理の負荷も不要となります。ウェブブラウザから簡単な設定で利用できるため、使用可能な端末や場所が増えて、業務効率が上がります。

従来、IT システムを自前で持つことやその管理運用の負荷から、経営管理の種々の業務を IT 化できなかった中小企業でも、IT 経営の敷居が大幅に下がることが期待されます。

2.3. 活用事例：事務処理系ソフトウェア

事務処理系ソフトウェア（オフィスアプリケーション、デスクトップアプリケーション等の言い方もあります）の機能を提供するクラウドサービスがあります。電子メール、ワードプロセッサ、表計算といった一般的な事務処理アプリケーションや、グループウェア、

営業管理ツールのようなオフィスでの情報共有や連絡調整を自動化するアプリケーション等を、手元のパソコンにインストールしなくても、機能だけを利用できます。

個別のパソコンにアプリケーションソフトウェアをインストールしたり、情報共有のためのサーバを立てたりといった手間やコストが削減され、ライセンス料の節約につながる可能性もあります。

アップデートやセキュリティパッチの適用も、クラウドサービスの側で実施されるので、安心して手軽にこれらアプリケーションを利用できます。

事務処理ソフトで作成したファイルをクラウド上に保存すれば、複数担当者や部署間での共有や共同作業も容易に実現することができます。

３．あなたの会社のITに、こんな期待や課題はありませんか？

IT を経営に活かす、あるいは IT 経営を促進する上で、以下のような期待や課題をお持ちではありませんか。いくつか思い当たるふしがあるなら、クラウドサービスを活用することで実現したり解決したりできるかもしれません。

クラウドサービスにはどんなものがあり、どんなことができるのか、検討してみましょう。お知り合いのコンサルタント、IT コーディネータ、システムインテグレータ等、専門家の方に相談するのもよいでしょう。その際には、期待や課題を具体的に説明することが重要です。

＜業務効率について＞

- IT で行う業務の効率を上げて間接コストを圧縮したい
- 社内でバラバラに保有されている情報を集約して有効活用したい
- 管理業務や間接業務の IT 化率を上げて業務効率を改善したい
- 社外からでも、電子メールやスケジューラーなどを使いたい

＜IT の負担について＞

- IT の運用や維持管理のコスト（人手や手間）を削減したい
- 自社で運用しているサーバの運用負担を軽くしたい
- 専門要員を雇わずに最新の IT を活用したい
- 手間をかけずに情報セキュリティを維持・向上したい
- 最新の機能を持つソフトウェアを使いたいが、更新するのが面倒だ
- バックアップの作業負担やコストを軽減したい

＜IT を活用したビジネスについて＞

- IT を活かした新規サービスビジネスを迅速かつ安価に開始したい
- IT をベースに今展開している事業を、少ない投資で充実・拡大したい
- 経営管理や業務処理を IT 化したい
- 受発注処理、顧客管理、商談管理等にITを導入したい（SCM[3]、CRM[4]、SFA[5]等）
- 連携する企業間で情報共有を図り、新しい付加価値やサービスを開拓したい

---

[3] Supply Chain Management（サプライチェーン管理）
[4] Customer Relationship Management （顧客管理）
[5] Sales Force Automation （営業管理支援）

４．クラウドサービスを導入するにあたってチェックしましょう！

クラウドサービスの導入は、あなたの会社における IT の利用のしかたを変化させることになる可能性があります。その結果、職場での IT の利用のしかた、データの持ち方や保管の方法、業務間のデータ連携の方法などが影響を受ける可能性があります。

クラウドサービスの導入の前には、このような面に関してあらかじめ検討し、クラウドを効果的に利用できる条件を整えて、安全かつ有効にクラウドサービスを利用しましょう。

クラウドサービスの導入を検討する際には、経営者や経営管理に携わる立場と、クラウド利用を実際に所管する IT 担当の立場の両面から検討する必要があります。ここでは、少なくともこれだけは確認しておくことが望ましいと思われる項目を、３つの領域に分けて整理しました。

［A］クラウドサービスの利用範囲についての確認項目（４項目）

［B］クラウドサービスの利用準備についての確認項目（４項目）

［C］クラウドサービスの提供条件等についての確認項目（６項目）

以下の解説を参考に、付録のチェックシートで確認することをお奨めします。

チェックシートでチェックがつかなかった項目に関しては、クラウドサービスの導入・利用に際して、セキュリティ等に関するリスクが発生する可能性があります。そういった項目から生じるリスクについて、許容可能か（経営上、業務上、大きな支障が発生する恐れがないか）どうかを改めて検討してみてください。

［A］クラウドサービスの利用範囲についての確認項目

No.	項目	内容
(1)	利用範囲の明確化	クラウドサービスでどの業務、どの情報を扱うかを検討し、業務の切り分けや運用ルールの設定を行いましたか？
(2)	サービスの種類とコスト	業務に合うクラウドサービスを選定し、コストについて確認しましたか？
(3)	扱う情報の重要度	クラウドサービスで取扱う情報の管理レベルについて確認しましたか？
(4)	ポリシーやルールとの整合性	セキュリティ上のルールとクラウドサービスの活用の間に矛盾や不一致が生じませんか？

(1) クラウドサービスでどの業務、どの情報を扱うかを検討し、業務の切り分けや運用ルールの設定を行いましたか？

社内のどんな業務のどの範囲をクラウドサービスに移行すべきかを、まず判断する必要があります。どのような業務でどんな負荷・負担が発生しているかを整理し、(2)項で確認

する、どんなサービスがどんなコストで利用できるかと照らし合わせながら、クラウドサービスに移行する業務範囲と、そこで取扱う情報の種類・範囲を決定します。

その際、クラウドサービス導入に伴って発生する問題を明確にしておく必要があります。IT で処理している業務の特定部分を取り出して、別のシステムに移せるでしょうか。その場合に、他の既存のシステムや処理との連携は問題ないでしょうか。クラウドサービスの導入が既存の業務やシステムに与える影響を検討しましょう。

最初は電子メール、セキュアストレージなどに対象範囲を限ってクラウドサービスの利用を始めてみてもよいでしょう。重要な情報（個人情報や機密情報）を外部に預けないように範囲を区切ってクラウドサービスを活用することも検討に値します。

(2) 業務に合うクラウドサービスを選定し、コストについて確認しましたか？

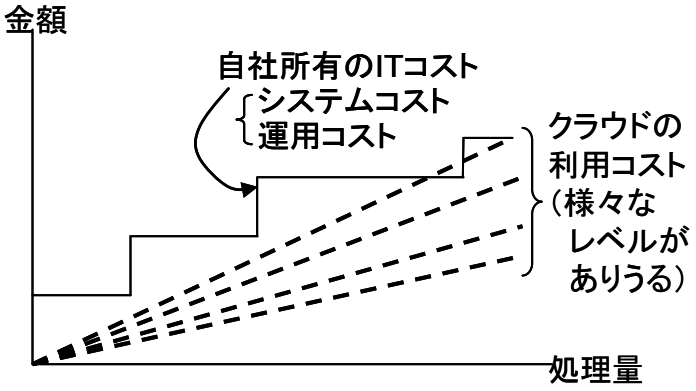
様々なクラウドサービスが、様々なクラウド事業者から提供されています。サービス内容や特徴を調べて比較して理解を深め、自社の業務に適したサービスを選択しましょう。

さまざまなクラウドサービスの例

財務会計、経理、人事管理、給与計算、税務申告、グループウェア、セキュリティ対策、販売管理、プロジェクト管理、インターネットバンキング、社会保険手続き、顧客商談管理、仕入れ・在庫管理、CAD、データ配信、データ管理、省エネ管理、電子メール、事務処理系アプリケーション　等

クラウドサービスの導入と運用に関するコストを試算してメリットを確認しましょう。同条件で必要なコストを比べてみてもよいでしょう。これまで必要であった専任または兼務の IT 管理・運用要員が不要になる場合や、IT 資産が不要になる場合にはコスト面の利点が大きくなります。サーバの更新時期に合わせてクラウドサービスに切り替えるといった方法も効果的です。

導入コストだけでなく、間接費も含めた月々の運用コストについても調べてみましょう。



クラウドサービスのコストのシミュレーションの例

将来、利用の規模を拡大した場合にどの程度のコスト増となるかについてもシミュレーションを行って検討しておきましょう。

概ね、自社所有の IT コストとクラウドの利用コストの関係は、上図のようなモデルで表現することができます。

⑶ クラウドサービスで取扱う情報の管理レベルについて確認しましたか？

プライバシーや企業秘密に係る情報をクラウドサービスで取扱う場合には適切な管理が必要です。情報の性質や重要度を考慮して、クラウドサービスで取扱って問題がないかを検討しましょう。

情報が外部預託可能なものであるかを検討しましょう。例えば個人情報をクラウドサービスで取扱うためには、個人情報保護法に基づき、委託先の適切な監督義務が生じる場合があります。

情報の重要度については、その情報が失われた場合の、経営にとってのダメージを評価しておきましょう。競争力の喪失、顧客の喪失、信用の失墜、預金等の不正引出し、経営管理情報の紛失等、経営に重大な影響を及ぼす結果につながる場合があります。

⑷ セキュリティ上のルールとクラウドサービスの活用の間に矛盾や不一致が生じませんか？

会社のセキュリティポリシーやルールで、社外に情報を置くことを禁止していたり、外部委託に関する制限をしていたりすると、クラウドサービスの利用が難しくなる場合もあります。現在このようなポリシーやルールがあなたの会社にある状態で、それらを変更してでもクラウドを利用する価値が大きいと判断できる場合には、情報をクラウド事業者に預けられるようにこれらの規則を見直し、IT の利活用の実態に整合させることが望ましいでしょう。

そのような判断をする場合には、クラウドサービス使用時に起きうるトラブルに伴って想定される不都合が、業務の上で許容される範囲内に抑えられることを確認しましょう。情報や情報処理プロセスを外部に預けることに伴うメリットと、利用に伴うリスクの許容可能な範囲とを理解した上で、クラウドサービスを活用してください。

［B］クラウドサービスの利用準備についての確認項目

No.	項目	内容
(5)	利用管理担当者	クラウドサービスの特性を理解した利用管理担当者を社内に確保しましたか？
(6)	ユーザ管理	クラウドサービスのユーザについて適切に管理できますか？
(7)	パスワード	パスワードの適切な設定・管理は実施できますか？
(8)	データの複製	サービス停止等に備えて、重要情報を手元に確保して必要なときに使えるための備えはありますか？

(5) クラウドサービスの特性を理解した利用管理担当者を社内に確保しましたか？

クラウドサービスに関する業務を行う利用管理担当者が最低 1 人は必要です（専任でなく兼務でも構いません)。社内にクラウドサービスの利用管理担当者を確保しましょう。(ITの利用に詳しい人であれば適任の可能性が高いです。)

クラウドサービスの利用管理担当者は、IT 管理責任者の指示と監督の下、クラウドの利用に際しての各種設定を行う等、IT 担当者と同等の業務を行います。その役割としては、次のようなことが考えられます。

(ア) ユーザアカウントの登録や抹消の処理（誰にどこまでの処理をさせるかを会社の方針に基づいてクラウドサービス上で設定する）
(イ) クラウドサービスの利用マニュアルの整備や利用方法の指導
(ウ) クラウドサービスの利用者に対するヘルプデスク
(エ) クラウドサービスに置くデータの定期的な複製
(オ) クラウドサービスに障害が生じた場合のクラウド事業者との連絡調整や、必要に応じて迂回処置等の検討・実施
(カ) クラウドサービスでの処理量の増減に応じたサービス利用量の調整

また、クラウドサービスの利用に際して、自社だけで判断が困難な事項が生じた際に、相談できる先[6]を社外に確保しておくとよいでしょう。

(6) クラウドサービスのユーザについて適切に管理できますか？

クラウドサービスの利用の際には適切なユーザ管理が必要です。ユーザ管理とは、実際に業務のためにクラウドを利用する人について、その権限等を定めて管理することです。以下のことを実施しましょう。

(ア) クラウドサービスの業務ごとに、利用する従業者を登録し、他の者はアクセスできないようにする。（アクセス管理）
(イ) クラウドサービスの利用者について、どの業務・どの情報についてどのような操

[6] IT コーディネータなどのコンサルタントや税理士等の専門家、日頃付き合いのある IT 機器や事務機の販売店などが、相談相手として考えられます。

作・処理を許可するのかを決定する。（権限管理）

(ウ) クラウドサービスの利用者一人一人について、ID とパスワードの対（ユーザアカウント）を用意する。（複数人でアカウントを共有することは、権限外の処理を誘発したり、責任をあいまいにしたりします。）

ルール通りに利用・運用ができているかを定期的に管理するために、管理者用のアカウントも用意しましょう。管理者の権限は必要な人に限って与えるようにしましょう。

(7) パスワードの適切な設定・管理は実施できますか？

クラウドサービス利用者のパスワードは他人に推測されにくいものを設定し、他人に見破られないようにしましょう。また、パスワードは定期的に変更するなど、他人のなりすましによる悪用を防ぐように管理する必要があります。

もし、パスワードを忘れてクラウドサービスにアクセスできなくなると、業務に支障をきたしたり、必要なデータを使えなくなったりします。パスワードを忘れることがないよう管理する[7]、パスワードを復元する方法を用意する[8]等の措置も必要です。

万一パスワードがわからなくなったときのために、クラウドサービス事業者はパスワードリセットの仕組みを提供している場合が多いと考えられます。そのようなサービスが提供されているかあらかじめ確認しましょう。提供されている場合は、リセット要求を誰が出して誰が受け付けるのか、要求者の本人確認の仕組みはどうか、あらかじめ登録した特定の人からしか要求できないようになっているか、等を確認しましょう。誰でも勝手にリセットできる状態では、権限違反やなりすましのリスクがあります。また例えば手続が郵送ベースだけだったりするとリードタイムが長くなるので、その間に支障をきたさない備えも必要になります。

(8) サービス停止等に備えて、重要情報を手元に確保して必要なときに使えるための備えはありますか？

クラウドに置いた重要なデータの複製を定期的に取りましょう。「アーカイブ」と呼ばれる作業です。万が一、クラウドサービス上に置いたデータが失われたときでも事業の継続・再開が可能なように、適切な間隔でクラウドサービスの外にデータの複製を作ることをお奨めします。例えば売上処理が終わったら、売上台帳のデータのコピーを自社内のサーバに取るとか、テープや DVD に落として倉庫に保管するなどです。複製作業を適切に実行・運用できる体制を整えておくとよいでしょう。

なお、クラウドサービス事業者は、通常、自動バックアップを標準機能として提供しています。日常業務の中では、ユーザが頻繁なバックアップを実施する必要がない場合が多いと考えられます。クラウド事業者の実施内容を確認のうえ、万が一に備えるレベルでの

---

[7] 一定のルールで記録し、利用者以外のものが別の場所でルールに基づいて保管する等

[8] パスワードを、ある方法と特定のパラメータ（特定の数字の組み合わせ等）によって生成することとし、方法とパラメータを別々に管理する等

データの複製（ローカルコピー、アーカイブ）で十分と考えられます。

［C］クラウドサービスの提供条件についての確認項目

No.	項目	内容
⑼	事業者の信頼性	クラウドサービスを提供する事業者は信頼できる事業者ですか？
⑽	サービスの信頼性	サービスの稼働率、障害発生頻度、障害時の回復目標時間などのサービスレベルは示されていますか？
⑾	セキュリティ対策	クラウドサービスにおけるセキュリティ対策が具体的に公開されていますか？
⑿	利用者サポート	サービスの使い方がわからないときの支援（ヘルプデスクやFAQ）は提供されていますか？
⒀	利用終了時のデータの確保	サービスの利用が終了したときの、データの取扱い条件について確認しましょう。
⒁	契約条件の確認	一般的契約条件の各項目について確認しましょう。

⑼ クラウドサービスを提供する事業者は信頼できる事業者ですか？

そのサービスを提供するクラウド事業者の経営が安定して信頼できるか、サービスの提供が長期間安定して行われるかを確認しましょう。経営の評価は難しいですが、以下のような項目が判断の参考になります。

（注）これらはあくまで参考情報であり、これらを満たしていることは必須でなく、また、これらの項目に適合しているからといってそれだけで信頼できるとは限らないことに留意してください。一方、新規参入だけど利用価値の高い新事業者・サービスも登場してくるので、それらをうまく安全に活用する視点も大事です。

⑺ 株式公開企業であるか。株式公開企業は経営状況について審査を受け、定期的に情報を公開しています。

⑴ 何年業務を続けているか。長年事業が継続していれば、安定性、継続性の指標になります。

⑼ 利用者の数が多いか。多くの人が利用していることは、信頼性が高い結果である可能性が高いです。どんなユーザがいるかが判れば、より参考になります。（クラウドサービスを実際に利用しているユーザと話すことができるなら、使い勝手、投資効果、障害の有無や対応等について悪い評価はないか確認してみましょう。）

⑽ 事故の情報がたびたび聞かれたりしないか、万一の障害対応がきちんと行われているか。

⑾ そのサービスを、事業実績のあるシステムインテグレータや IT の販売店が代理販売しているケースもありえます。信用や実績のある事業者が推奨、再販してい

るサービスは、ある程度安心して使うことができるでしょう。

(カ) 対象のクラウドサービスが、大手クラウド事業者（コンピュータメーカや通信事業者もクラウドサービスを提供しています）が提供するプラットフォーム上で提供されている場合もあります。その場合には、基盤となっているクラウドサービス部分のセキュリティや信頼性、つまり可用性や攻撃等への耐性は高いものと考えられるでしょう。

(10) サービスの稼働率、障害発生頻度、障害時の回復目標時間などのサービスレベルは示されていますか？

クラウドサービスは、メンテナンスや障害のために、予告して、あるいは突然止まることがあります。その対策方針等は、SLA（サービスレベルアグリーメント、またはサービスレベル契約書）等の文書で示されている場合が多いです。以下のことを確認しましょう。

(ア) 予告して停止する場合は、予告のリードタイムが十分であるか、予告の方法として、確実に事前に知ることができる方法が示されているか、不都合が生じる恐れがないかを確認しましょう。

(イ) 突然の障害等については、予告や予測は困難ですが、クラウドサービス側でトラブルが発生した際に、クラウド事業者側からどのような方法で連絡をしてくるかを確認しましょう。トラブルが生じた場合には、速やかに通知が来るようになっていることも大事です。

(ウ) 突然の障害等について、その発生頻度の理論値や経験値、障害でサービスが止まった場合の、復旧に要する見込み時間などが示されていることがあります。それらを総合して、稼働率保証として示されることもあります。

稼働率保証の場合は、率の計算単位が何か（通常、月単位）を確認しましょう。年単位の場合は、0.1%の停止でも理論的には 8 時間 45 分連続して停止する可能性もあることになります。

なお、この稼働率保証のことを簡略化してSLAと呼び習わしていることもあります。

(エ) また、稼働率保証は、通常、それ以上のサービス停止があった場合には何らかの補償をしますという条件で示されることが一般的です。必ずしも示された稼働時間が保障されている訳ではないことに注意しましょう。想定外の長時間の停止に備えて、(8)で確認したようなローカルバックアップ、アーカイブによる備えをすることが望まれます。

(オ) クラウド事業者によっては、ダッシュボードと呼ばれる画面等で、現在のクラウドの運転状況やトラブルの状況などの情報を常時提供している場合があります。そのような事業者はサービス稼動についての管理が充実していると期待できますし、また必要なときに随時運転状況を確認できるので安心です。

（11）クラウドサービスにおけるセキュリティ対策の具体的内容は公開されていますか？

多くの場合、クラウド事業者は自社のセキュリティ対策に関する解説をウェブサイトで公開しています。年次報告書（情報セキュリティ報告書やCSR報告書の形を取るケースも多い）やセキュリティに関するホワイトペーパー（レポート）を公表している場合もあります。

以下のセキュリティ対策に関する項目について、クラウド事業者のウェブサイト等で説明されているかを確認しましょう。

(ア) システムに関するセキュリティ対策項目
- OS やアプリケーションのアップデート、セキュリティ修正パッチやサービスパックの適時適用等
- システムの可用性・信頼性を確保するための対策（サーバやストレージやネットワークの多重化・冗長化、自動バックアップ等）

(イ) データ管理に関するセキュリティ対策項目
- 暗号化の自動実施、または暗号化機能の提供
- クラウド事業者側での自動バックアップ（インターバル、世代、復旧方法、保存期間等）

(ウ) ネットワークと通信に関するセキュリティ対策項目
- ウイルス・マルウェア感染への対策、不正アクセスへの対策、ネットワーク障害対策等
- 障害や攻撃に対する監視、検知、解析、防御対策等

(エ) データセンターに関するセキュリティ対策項目
- 防犯設備、入退室管理、災害対応、監視体制等
- 電源や冷却設備の二重化、予備電源の確保等

(オ) データセンターの運用に関するセキュリティ管理項目
- 運転要員の信頼性確認、勤務状況・作業内容のモニタリング等
- システムへのアクセス権限や管理者特権の管理、操作ログの管理等

公的機関が定めている情報開示指針やサービスに関するガイドラインがあります。また情報セキュリティやデータの保護管理に関する基準類も、民間のものも含めて数多くあります。それらに基づいた運用管理、情報開示、認定や認証が行われていれば、その事業者の信頼性やセキュリティ管理についても安心できる可能性が高いです。これら指針等の例としては、次のようなものがあります。

- 経済産業省：SaaS向けSLAガイドライン
- 経済産業省：情報セキュリティ報告書モデル
- 経済産業省：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
- 総務省：ASP・SaaSにおける情報セキュリティ対策ガイドライン
- 総務省：データセンターの安全・信頼性に係る情報開示指針
- ISMS（情報セキュリティマネジメントシステム）適合性評価制度

- ITSMS(IT サービスマネジメントシステム)適合性評価制度
- 日本情報経済社会推進協会：プライバシーマーク制度
- マルチメディア振興センター：ASP・SaaS 安全・信頼性に係る情報開示認定制度
- PCI DSS（クレジットカード業界の定めるデータセキュリティ基準）
- 米国会計監査基準における SAS70 Typell 監査（日本においては日本公認会計士協会の定める 18 号監査）による、内部統制に関わる監査報告

(12) サービスの使い方がわからないときの支援（ヘルプデスクや FAQ）は提供されていますか？

ユーザ支援のための施策として、ウェブサイトに公開されたよくある質問集（FAQ）、動画等を用いた取扱説明、使い方に関する質問を受け付けてくれるヘルプデスク（カスタマー窓口）等があります。

これらのユーザサポート施策が充実していて安心できるか確認しましょう。

ユーザサポート窓口については、以下を確認しましょう。

- 連絡方法・連絡先（電話、メール、その他の手段が提供されています）
- 受付時間（自社の利用パターンと合致するか、業務時間外に連絡が必要となるかを検討しましょう）
- 料金（問合せが月額料金に含まれているか、追加で料金が必要かを確認しましょう）

一度ためしに連絡して対応を確認してみてもよいでしょう。

(13) サービスの利用が終了したときの、データの取扱い条件について確認しましょう。

クラウドサービスの利用を何らかの理由で終了する場合には、クラウドに預けてあったデータを自社内のシステムに戻したり、他のサービス事業者に預け直したりすることが必要になります。

この作業がスムーズに支障なく行われるためには、次の事項について確認が必要です。

- データが必要なタイミングで返却されるか（あるいは随時ローカルコピーが可能か。そのスピードはデータ量に比して十分高速か）
- データが返却される場合のデータのフォーマットは、他のシステムとの互換性が確保されているか
- 利用が終了し、データが返却された後で、クラウドのシステム上に残るデータは確実に消去され、第三者による再利用や悪用が起こらないよう対策されているか。

(14)一般的契約条件の各項目について確認しましょう。

クラウドサービスの利用に際しては、通常、サービスを提供するウェブサイトに利用のための契約約款が表示され、「同意します」ボタンをクリックすることで契約が成立する構造になっています。書面による契約と同じ効力を持ちますので、「同意します」ボタンをクリックする前に、契約条件を確認しておきましょう。

一般に、その取引の内容を規定する部分以外にも、以下のような注意すべき項目があります。

- 利用価格の体系や適用条件
- 価格の変更に関する規定（通知期間、通知方法、不同意の場合の処理等）
- サービスの変更に関する規定（内容、方法、通知期間、通知方法、不同意の場合の処理等）
- 守秘義務（ベンダ側、ユーザ側、双方同等。ベンダ側のユーザ情報に関する守秘義務やユーザ側の義務について注意が必要）
- 損害賠償規定（ベンダ側の原因でデータが失われた場合やサービス障害の波及損害に対する賠償規定があるか、それは十分かの確認）
- 契約の満期終了と更新に関する規定（契約期間は、自動更新規定があるか、更新しない（する）場合の通知期間・通知方法等）
- 契約の解除に関する規定（ベンダ側が一方的に解除できる条件でないか、ユーザ側が解除する場合のペナルティ等はないか、等）
- 契約の終了・解除に伴う処理等の規定（終了時のベンダの義務、ユーザの権利が規定されているか、それは妥当か。終了時のデータの返還や、返還後にクラウド上のデータを完全消去すること等が明記されているか　等）

以上

[P1]　経済産業省「IT 経営力指標　ステージ２」の定義

ステージ２

◆概ね経営課題は把握できている　◆経営戦略の周知が不十分　◆IT の活用が組織単位.

◆業務プロセスが可視化されているが、組織ごとの改善に留まる

◆職務権限と職務分掌が定められている.

◆システム基盤がアプリケーションごとにバラバラに構築.

◆IT 戦略の立案に経営層が関与している.

◆IT 投資の効果予測は投資前に行うが、投資後の評価は行っていない.

◆経営層や社員の IT 活用能力を向上させるために、マニュアルの整備、研修会や啓蒙活動を行っている.

◆経営層は IT に関連起因する情報漏洩・ウイルス・不正アクセス等の脅威を認識している.

*経済産業省「IT 経営ポータル IT 経営力指標」

http://www.meti.go.jp/policy/it_policy/it_keiei/about/idea/management.html

中小企業のためのクラウドサービス安全利用チェックシート

No.	項目	内容	チェック	メモ／摘要
［A］クラウドサービスの利用範囲についての確認項目				
(1)	利用範囲の明確化	クラウドサービスでどの業務、どの情報を扱うかを検討し、業務の切り分けや運用ルールの設定を行いましたか？	□	
(2)	サービスの種類とコスト	業務に合うクラウドサービスを選定し、コストについて確認しましたか？	□	
(3)	扱う情報の重要度	クラウドサービスで取扱う情報の管理レベルについて確認しましたか？	□	
(4)	ポリシーやルールとの整合性	セキュリティ上のルールとクラウドサービスの活用の間に矛盾や不一致が生じませんか？	□	
［B］クラウドサービスの利用準備についての確認項目				
(5)	担当者	クラウドサービスの特徴を理解した担当者を社内に確保しましたか？	□	
(6)	ユーザ管理	クラウドサービスのユーザについて適切に管理できますか？	□	
(7)	パスワード	パスワードの適切な設定・管理は実施できますか？	□	
(8)	データの複製	サービス停止等に備えて、重要情報を手元に確保して必要なときに使えるための備えはありますか？	□	
［C］クラウドサービス提供条件等についての確認				
(9)	事業者の信頼性	クラウドサービスを提供する事業者は信頼できる事業者ですか？	□	
(10)	サービスの信頼性	サービスの稼働率、障害発生頻度、障害時の回復目標時間などのサービスレベルは示されていますか？	□	
(11)	セキュリティ対策	クラウドサービスにおけるセキュリティ対策が具体的に公開されていますか？	□	
(12)	利用者サポート	サービスの使い方がわからないときの支援（ヘルプデスクやFAQ）は提供されていますか？	□	
(13)	利用終了時のデータの確保	サービスの利用が終了したときの、データの取扱い条件について確認しましょう。	□	
(14)	契約条件の確認	一般的契約条件の各項目について確認しましょう。	□	