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」対応

クラウド事業者による

情報開示の参照ガイド

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」対応

クラウド事業者による情報開示の参照ガイド

はじめに

IPA では、中小企業によるクラウドサービスの利用推進に向けて「中小企業のためのクラウドサービス安全利用の手引き」（以下、「安全利用の手引」）を作成しました。「安全利用の手引」では、クラウドサービスの解説と利点ならびに留意事項、そしてクラウドサービスの利用事例と期待効果を紹介し、利用に際して準備・確認すべき項目を示して解説しています。

利用に際して確認すべき項目の多くはクラウドサービスの提供事業者（以下、クラウド事業者）が開示する情報に関するものです。中小企業によるクラウドサービスの安全利用のためには、必要な情報が適時適切にクラウド事業者から提供されることが望まれます。

本書では、クラウド事業者による情報開示に関して、その項目や開示方法について、中小企業によるクラウドサービスの安全利用の視点から、期待される姿を示します。クラウドサービスの特徴である、オンデマンドセルフサービスを実現するためにも、クラウド事業者からの積極的な情報の提供が期待されるところです。

クラウド事業者の開示する情報について

「安全利用の手引」では、クラウド事業者の開示する情報について、以下のカテゴリを提示しています。

- 事業者の信頼性
- サービスの信頼性
- セキュリティ対策
- 利用者サポート
- 利用終了時のデータの確保
- 契約条件の確認

これらのカテゴリごとに、開示が望まれる情報項目を提示し、開示の方法についても案を示します。ここで提示する項目はすべてを公開しなければならないというものではありません。利用者が自らクラウドサービスの利用について判断する際に参照すべき情報として提示しており、必要に応じて限定された情報項目や開示方法（既存会員限定など）で提供するようなことも考えられます。利用者にとって必要な情報が、クラウド事業者に特段の負担となることなく提供され、中小企業によるクラウドサービスの利用が促進される状況が実現することが望まれます。

1. 「事業者の信頼性」に関する情報開示の項目とその方法

「安全利用の手引」における確認項目の記述

(9) 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。

事業者の信頼性とは

クラウドサービス利用者にとって、サービスの安定性と継続性は重大な関心事です。経営の財務上および事業運営上の持続性と安定性を示す情報が求められています。具体的には以下の項目がそのようなニーズを満たすものと考えられます。

事業者の信頼性に関する項目

- 企業名、企業の所在地、連絡先（電話、FAX、電子メール）等の企業の存在に関する情報
- 創業の時期、当該クラウドサービスの開始時期・利用実績等、サービスの継続性に関する情報
- 販売代理店、提携先等、サービスの購入や利用に関する参考情報
- 制度に基づいて開示される企業情報（株式公開、内部統制報告書、情報セキュリティ報告書、情報セキュリティ監査報告書、ASP・SaaS の情報開示指針に基づく開示　等）
- 「安全利用の手引」では、「以下のような項目が判断の参考になります」として示しています[1]。

  (ア) 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。

  (イ) 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。

  (ウ) 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。)

[1] 「安全利用の手引」では、(注) として「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。」と補足している。

(エ) 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。

(オ) 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。

情報の開示方法について

事業者の信頼性に関する情報は、ウェブサイトやサービスカタログに記載されていると良いでしょう。利用者はサービスの詳細を確認するとともに、サービスを提供する事業者を確認しますので、サービスを紹介したウェブサイトやカタログから直接確認できることが望ましいでしょう。

2. 「サービスの信頼性」に関する情報開示の項目とその方法

「安全利用の手引」における確認項目の記述

(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。

サービスの信頼性とは

クラウドサービス利用者は、事業者の信頼性に加えて、サービスそのものの信頼性についても確認したいと考えています。サービスの信頼性に関する情報としては、サービスの稼働率、計画的または偶発的停止の際の連絡や回復時間に関する情報、その間のサポート等に関する情報等が該当すると考えられます。運用面での情報を開示することで、利用者に安心感を持ってもらうことができます。

サービスの信頼性に関する項目

- サービスの稼働状況に関する情報
  - 通常運転時のサービスやシステムの稼働状況
  - 稼働状況を確認できる情報源の場所（ダッシュボード等）やその見方

- サービスの稼働率に関する情報
  - サービスのアップタイム率の見込みまたは保証値（計算単位含む）
  - 保証値が未達の場合の補償内容
- 計画的停止に関する情報
  - 事前通知のリードタイム
  - 停止の最大時間
- 障害時の復旧等に関する情報
  - 障害発生時の通知方法、通知のタイミング等
  - 障害復旧までの見込み時間等、復旧途中での情報提供の方法
  - 障害期間中のサポート体制等
- 「安全利用の手引」では、「以下のことを確認しましょう。」として示しています。

(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。

情報の開示方法について

サービスの信頼性に関する情報は、ウェブサイトやサービスカタログに記載されていると良いでしょう。利用者はサービスの詳細を確認すると共に、サービスに対する信頼性を確認しますので、サービスを紹介したウェブサイトやカタログから直接確認できることが望ましいでしょう。

また、サービスの信頼性においては、障害発生時の対応など、過去の実績についても情報を望む場合があります。障害対応の実績や事例を公開することは、利用者の信頼や安心を生むことにつながる場合も多くあります。事業に差し障りのない範囲で情報を開示することが望ましいでしょう。

3. 「セキュリティ対策」に関する情報開示の項目とその方法

「安全利用の手引」における確認項目の記述

(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を公表している場合もあります。

セキュリティ対策とは

クラウドサービス利用における懸念事項のひとつにセキュリティ対策があります。中小企業はクラウドサービスを提供するためのシステムの仕組みやその安全を確保する要素について十分な知識を持っていないため、セキュリティ上の安全性について自ら確認することができません。第三者が提供するサービスを利用することや社外にデータを置くことに漠然たる不安を抱くケースが多いと考えられます。システムやデータの安全性対策を示すことが安心につながります。

セキュリティ対策に関する項目

- 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）
- 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バックアップ（インターバル、世代、復旧方法、保存期間等）

- 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
- 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
- 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

情報の開示方法について

セキュリティ対策については、レベルなどの判断が難しいため、上記に例示した項目については、実施しているかどうかを明確にしておけば良いでしょう。詳細なセキュリティ対策を公開することは、攻撃を意図するものに情報を提供することになる可能性もあるため、そのような恐れのない範囲に限定するという判断も考えられます。

情報の開示については、ウェブサイトへの掲載や資料の作成･配布等が一般的方法と考えられます。利用者に限定して提供する情報であれば、利用者専用の提供方法による開示や問い合わせベースでの対応でも良いでしょう。ただし、これらの情報を利用者は自社内のセキュリティ管理に利用することがあるため、何らかの文書になっているとより利便性が高まるでしょう。

また、情報セキュリティ対策については、定期的な報告をすることも、利用者の安心を得るためのより良い手段だといえます。利用者が自社のセキュリティ監査を行う場合の情報源となるような、情報セキュリティに関する報告書やホワイトペーパーなどを提供することも役に立つと考えられます。

「安全利用の手引」には、次のような記述があります。これらに該当する情報開示を行っている場合は、セキュリティ対策に関する情報開示の補完として効果があります。

> *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。(*URLについては巻末を参照。)*
>
> - *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*
> - *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）の適合性評価制度*
- ✧ *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*

4. 「利用者サポート」に関する情報開示の項目とその方法

「安全利用の手引」における確認項目の記述

(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。

利用者サポートとは

中小企業にとっての良いサービスの条件として、サポートが充実していることがあります。利用方法がわからない時、トラブルが発生したときに、情報を入手できる場所や相談できる相手があることは安心感につながります。自社のサポート体制だけではなく、ユーザ用のコミュニティがある場合には、ユーザ同士の情報交換が役に立つことも考えられます。

サポート体制と内容に関する項目

- 利用方法の説明・解説文書の提供：オンラインヘルプ、ユーザマニュアル等
- よくある質問集(FAQ)：トップページからたどりやすいところにある、キーワード検索が充実している　等が望ましい
- サポート窓口の情報：連絡先（電話、FAX、メール、その他）、応対方法、受付時間、費用の有無や体系　等
- ユーザコミュニティに関する情報：サポート掲示板、ユーザグループ紹介など

情報の開示方法について

サポート窓口については事業者のホームページやサービスごとのウェブサイト、サービス約款や契約書などに記載しておくと良いでしょう。サポートが有償の場合

や登録制度がある場合には、その旨をあらかじめ伝えて理解しておいてもらうことも大事です。

5. 「利用終了時のデータの確保」に関する情報開示の項目とその方法

「安全利用の手引」における確認項目の記述

(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。

利用終了時のデータの確保とは

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、クラウドサービス上に作成、保管されたデータを、サービス利用終了時に引き上げたいという要望が利用者にはあります。作成したデータをどのようにローカルに保存し、再利用できるのかについての情報を提供することで、利用者の安心感を得、また利用についての判断を促すことになります。

また、サービス利用終了時のクラウド上のデータの抹消方法についても、個人情報や機密情報だけではなく、企業のすべての情報において気になるところです。利用が終了した後は、クラウドにあったデータは確実に消去され、復元されたり再利用されたり流出したりということが起らないことを保証し、説明することが重要です。

利用終了時のデータの確保に関する項目

- 利用終了時のデータのローカルへの落し込み・保存方法
- 保存できるデータ形式
- 利用終了後のユーザデータのクラウド上からの抹消についての保証
- 「安全利用の手引」では「次の事項について確認が必要です。」として以下の項目を示しています。

    - ✧ *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。*

情報の開示方法について

利用終了時のデータの確保に関する情報は、ウェブサイト上で事前に提供されていることが望ましいでしょう。また、必要に応じてツールを提供し、安全にデータをダウンロードできるようにすると良いでしょう。

6. 「契約条件の確認」に関する情報開示の項目とその方法

「安全利用の手引」における確認項目の記述

(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。

契約条件の確認とは

クラウドサービスの利用も一般の商取引であり、契約条項は相互に確認の上契約されるべきものですが、ウェブサイト上の約款を利用者に読んでもらって、利用者が確認のボタンをクリックすることで契約が成立するパターンが一般的であり、内容を十分に確認せずに利用を開始してしまう利用者もいます。

特にいくつかの項目は万が一のときに紛糾する恐れがあるので、契約時にきちんと認識されているようにすることが望まれます。また、サービス利用中も必要に応じてこれらの契約条件がいつでも参照できるように提供することが望ましいでしょう。

契約条件の確認に関する項目

「安全利用の手引」では「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。」として以下の項目を示しています。

- *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）*

情報の開示方法について

サービスの利用における契約条項は、利用者が同意するときにその内容を十分確認できるよう、明確にわかりやすく示す必要があります。また、利用者が同意したそのままの内容を保存して将来相互に確認できる状態を保持することが望まれます。

契約期間中はいつでも参照できるように、ウェブサイトにわかりやすく掲載しておきましょう。利用途中で条件を変更する場合に利用者からの確認を得て記録を残すことにも留意しましょう。

以上

＜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の URL＞

- ✧ 経済産業省：SaaS 向け SLA ガイドライン
  http://www.meti.go.jp/press/20080121004/20080121004.html
- ✧ 経済産業省：情報セキュリティ報告書モデル
  http://www.meti.go.jp/policy/netsecurity/downloadfiles/5_sec_report.pdf
- ✧ 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
  http://www.meti.go.jp/press/2011/04/20110401001/20110401001.html
- ✧ 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
  http://www.soumu.go.jp/menu_news/s-news/2008/080130_3.html
- ✧ 総務省：ASP・SaaS の安全・信頼性に係る情報開示指針
  http://www.soumu.go.jp/menu_news/s-news/2007/071127_3.html
- ✧ 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
  http://www.soumu.go.jp/menu_news/s-news/090226_5.html
- ✧ 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
  http://www.isms.jipdec.or.jp/isms.html
- ✧ ITSMS(IT サービスマネジメントシステム)適合性評価制度
  http://www.isms.jipdec.or.jp/itsms.html
- ✧ 日本情報経済社会推進協会：プライバシーマーク制度
  http://privacymark.jp/
- ✧ 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

http://www.fmmc.or.jp/asp-nintei/

✧ 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）

https://www.pcisecuritystandards.org/

✧ 米国会計監査基準における SAS70 TypeII 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

http://www.aicpa.org/Research/Standards/AuditAttest/Pages/SAS.aspx

http://www.hp.jicpa.or.jp/specialized_field/pdf/00534-001629.pdf