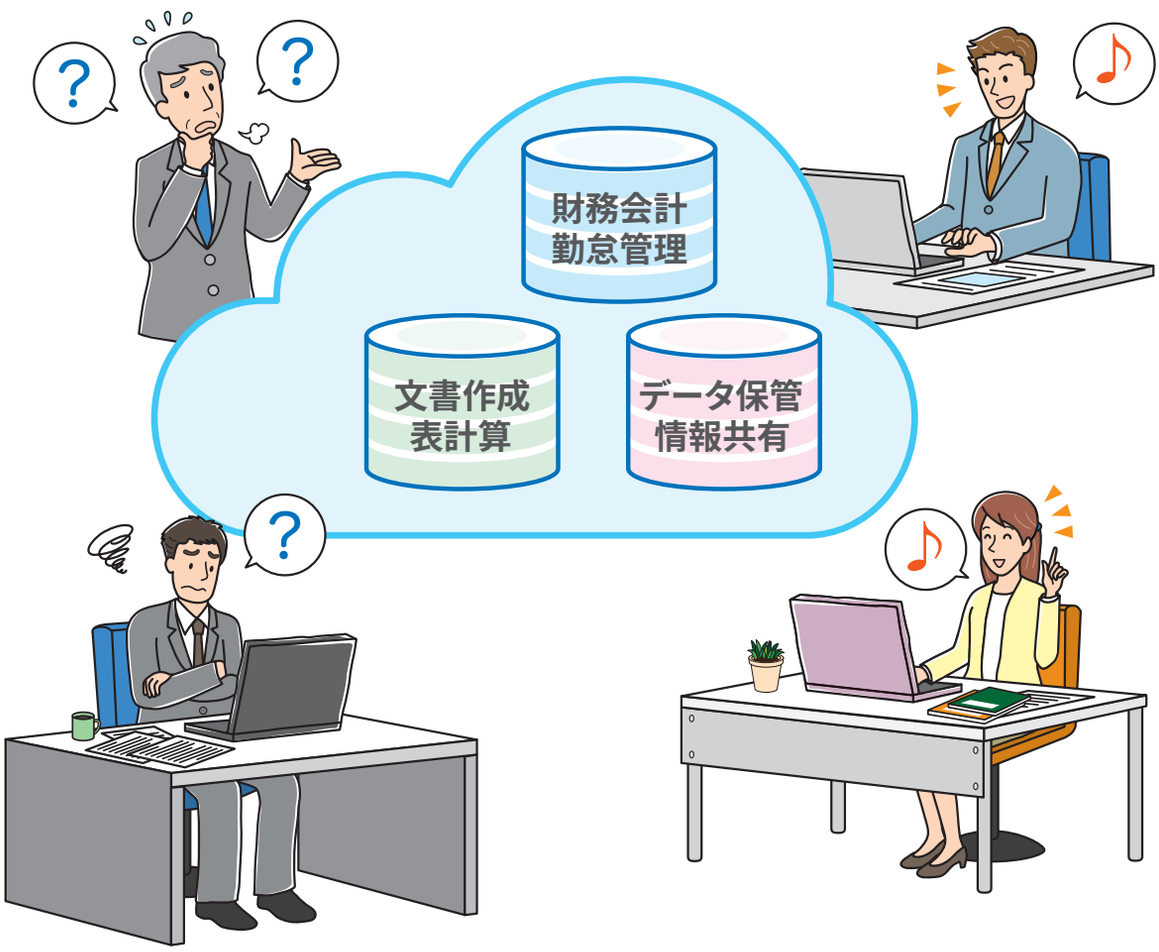
中小企業・小規模事業者の皆様へ

# 中小企業のための
# クラウドサービス
# 安全利用の手引き

## クラウドサービスの安全利用、できてますか？




取り返しのつかないことになる前に…
クラウドサービス
**安全利用チェックシート** で確認！

## クラウドサービスとは？

- インターネットを通じてソフトウェアやハードウェアを利用する情報システムサービスをクラウドサービスといいます。インターネットが普及し、コンピュータの仮想化技術※など、関連技術が進展したことで、身近になってきました。コンピュータが、雲の向こうのように、利用者から見えない所にあることから“クラウド”（cloud 雲）と呼ばれています。

  ※物理的に少数のコンピュータを、論理的に多数のコンピュータのように使うことができる技術

- 情報システムを自社で所有・運用することなく、サービスとして利用するだけのクラウドサービスは、メリットも多く、企業の業務処理だけでなく、個人の生活にまで利用が広がっています。

**身近なクラウドサービスの例**

- **財務会計、税務申告、給与計算、労務管理** などの経営管理アプリケーション
- **顧客管理、販売管理、名刺管理、ホームページ作成、ECサイト** などの業務アプリケーション
- **ワープロ、表計算、グループウェア、電子メール、オンラインストレージ** などのオフィスアプリケーション

## クラウドサービスを利用する前に確認しましょう！

- 情報セキュリティ対策について、情報システムを所有する場合には、自社が対応すればよいのですが、“利用するだけ”のクラウドサービスではサービスを提供する事業者に委ねる部分が発生します。
- 事業者に委ねる部分については、利用者が直接管理することはできないので、サービスの機能だけではなく、サービスに付随するセキュリティ対策についても、きちんと確認したうえで利用する必要があります。
- クラウドサービスのセキュリティ対策は、自社で所有する場合との共通点もありますが、以下のようなクラウドサービス固有のリスクを考慮して検討します。

インターネットを使う ➡外部からの攻撃を受けやすい
1台のコンピュータを多数で共用する ➡1台のインシデントが多数に影響する
1つのサービスが複数事業者で構成される※ ➡すべての対策を把握することが難しい

※サービスを提供するための、データセンター・ネットワーク回線などの設備、サーバー・ルーターなどの機器、OSやアプリケーションなどのソフトウェアは、それぞれ別の事業者が運営していることがあります。

## 利用者がやるべきことを知っておきましょう！

- クラウドサービスのセキュリティはサービスを提供する事業者と利用者との両者が、それぞれの役割・責任を分担し、必要とされる対策を実施することで維持・向上します。
- 次ページ以降の「クラウドサービス安全利用チェックシート」と「解説編」を参考に、利用者としての役割・責任を認識して、今後ますます便利になる、クラウドサービスを活用してください。

# クラウドサービス安全利用チェックシート

| | | | ☑ |
|---|---|---|---|
| **I. 選択するときのポイント** | | | |
| 1 | **どの業務で利用するか明確にする** | どの業務をクラウドサービスで行い、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を明確にしましたか？ | □ |
| 2 | **クラウドサービスの種類を選ぶ** | 業務に適したクラウドサービスを選定し、どのようなメリットがあるか確認しましたか？ | □ |
| 3 | **取扱う情報の重要度を確認する** | クラウドサービスで取扱う情報が漏えい、改ざん、消失したり、サービスが停止した場合の影響を確認しましたか？ | □ |
| 4 | **セキュリティのルールと矛盾しないようにする** | 自社のルールとクラウドサービス活用との間に矛盾や不一致が生じませんか？ | □ |
| 5 | **クラウド事業者の信頼性を確認する** | 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？ | □ |
| 6 | **クラウドサービスの安全・信頼性を確認する** | 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品質保証は示されていますか？ | □ |
| **II. 運用するときのポイント** | | | |
| 7 | **管理担当者を決める** | クラウドサービスの特性を理解した管理担当者を社内に確保していますか？ | □ |
| 8 | **利用者の範囲を決める** | クラウドサービスを適切な利用者のみが利用可能となるように管理できていますか？ | □ |
| 9 | **利用者の認証を厳格に行う** | パスワードなどの認証機能について適切に設定・管理は実施できていますか？（共有しない、複雑にするなど） | □ |
| 10 | **バックアップに責任を持つ** | サービス停止やデータの消失・改ざんなどに備えて、重要情報を手元に確保して必要なときに使えるようにしていますか？ | □ |
| **III. セキュリティ管理のポイント** | | | |
| 11 | **付帯するセキュリティ対策を確認する** | サービスに付帯するセキュリティ対策が具体的に公開されていますか？ | □ |
| 12 | **利用者サポートの体制を確認する** | 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を確保する** | 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たか？ | □ |
| 14 | **適用法令や契約条件を確認する** | 個人情報保護などを想定し、一般的契約条件の各項目について確認しましたか？ | □ |
| 15 | **データ保存先の地理的所在地を確認する** | データがどの国や地域に設置されたサーバーに保存されているか確認しましたか？ | □ |

※No15 クラウドサービスのサーバーは日本国外に設置されている場合もありますが、扱うデータによってサーバーの設置国・地域の法規制が適用されることがあります。
※No6,11,12,13はスマートSMEサポーター（認定情報処理支援機関）の開示情報で確認できます。

# Ⅰ．選択するときのポイント

クラウドサービスの機能や情報セキュリティ対策はサービスを提供する事業者の対応に依存する部分が多いため、必要な機能やセキュリティ対策を確認して選択します。


チェックシートNo.1

## どの業務で利用するか明確にする

クラウドサービスでどの業務を行い、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を明確にしましょう。

**例えば**

社内の情報共有のために、
- ●グループウェアを利用し、社員のスケジュール管理を行う
- ●オンラインストレージに製品カタログを保存して営業部門で共有する…など

チェックシートNo.2

## クラウドサービスの種類を選ぶ

業務に適したクラウドサービスを選び、メリットについて確認しましょう。

**例えば**

社外でも業務ができるようにして、コストを削減するために、
- ●経費精算にクラウドサービスを利用することで外出先や自宅などどこでも業務ができるようにする
- ●経費精算に関わる社内の作業時間を短縮し、サービス利用料を上回るコストを削減する…など

チェックシートNo.3

## 取扱う情報の重要度を確認する

クラウドサービスで取扱う情報が漏えい、改ざんされたり、消失、サービスが停止したときの影響を確認しましょう。

**例えば**

お客様の個人情報をクラウドサービスに保存していて、サイバー攻撃で個人情報が漏えいした場合の影響は、
- ●悪用などで本人に多大な迷惑がかかる
- ●本人への謝罪、補償や関係者への連絡が必要になる
- ●個人情報保護委員会に報告が必要になる
- ●被害拡大防止や再発防止のために多額の費用がかかる…など

チェックシートNo.4

## セキュリティのルールと矛盾しないようにする

セキュリティのルールとクラウドサービス活用との間に矛盾や不一致が生じないようにしましょう。

**例えば**

給与計算をクラウドサービスで行うにあたり、従業員のマイナンバーを登録する必要があるが、
- ●マイナンバーを記載した書類やデータを社外に保存することは社内ルールで禁止されている
- ●そこで暗号化登録ができるサービスを利用し、暗号化した場合のみ社外の保存を許可するルールに変更する…など

# 解説編

## チェックシートNo.5

### クラウド事業者の信頼性を確認する

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を選択しましょう。

**例えば**

**会計業務をクラウドサービスに移行するにあたり長期間利用できて、セキュリティ対策を常に改善しているサービスを選択するため、**
**●事業者が公表している財務情報を確認する**
**●利用者数などの実績を問い合わせる**
**●事業者の情報セキュリティ方針や関連した認証・認定制度※1の取得状況を確認する…など**

※1）以下のクラウドサービス選択時に参考となる制度等を参照してください。
ISMAP　政府情報システムのためのセキュリティ評価制度
https://www.ismap.go.jp/csm?id=csm_ismap_index
ISMAP（Information system Security Management and Assessment Program: 通称、ISMAP（イスマップ））は、政府が求めるセキュリティ要求を満たしているクラウドサービスを予め評価・登録することにより、政府のクラウドサービス調達におけるセキュリティ水準の確保を図り、もってクラウドサービスの円滑な導入に資することを目的とした制度です。

## チェックシートNo.6

### クラウドサービスの安全・信頼性を確認する

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品質保証を確認しましょう。

**例えば**

**店舗にクラウド型POSレジを導入するにあたりサービスが常に動いている必要があるため、**
**●事業者またはプラットフォーム事業者が公表している品質保証基準（SLA※2）を確認する**
**●システムの障害でデータ消失などの被害が発生したときに、どこまでが事業者の責任で、どこからが利用者の責任なのか利用規約で確認する…など**

※2）SLA Service Level Agreement サービスレベルに関する合意書「サービス及び合意されたサービスレベルを文書化した、サービスプロバイダと顧客間の書面による合意。(ISO/IEC20000-1)」

## ☛クラウドサービス選択時に参考となる制度等

クラウドサービス事業者が適切なデータ保護やセキュリティ対策を実施していることをマークとして表示する制度があります。いずれもURL記載のページ内でそれぞれの条件を満たすサービスが紹介されており、選定時の参考として利用することができます。

**ISMSクラウドセキュリティ認証**（一般社団法人情報マネジメントシステム認定センター）
**https://isms.jp/isms-cls.html**
通常のISMS(JIS Q 27001)認証に加えて、クラウドサービス固有の管理策(ISO/IEC 27017)が適切に導入、実施されていることを認証するものです。

**クラウド情報セキュリティ監査制度**（特定非営利活動法人日本セキュリティ監査協会）
**http://jasa.jp/jcispa/cloud_security/**
クラウドサービス事業者が基本的な要件を満たす情報セキュリティ対策を実施していることを監査し、その結果をCSマークの表示許諾を通じて利用者に対し、安全性が確保されていることを公開する制度です。外部監査と内部監査で「ゴールド」と「シルバー」の２種類があります。

**ASP・SaaS情報開示認定制度**（一般社団法人日本クラウド産業協会）
**https://www.aspicjapan.org/nintei/asp-nintei/index.html**
安全・信頼性に係る比較・評価・選択を行うために必要な情報を、クラウドサービス事業者が開示をしていることを認定する制度です。クラウドで扱う情報や環境の種類に応じて、「医療情報」「特定個人情報」「IoTクラウド」「データセンター」など合計７種類の認定マークが定められています。

**ISMAP　政府情報システムのためのセキュリティ評価制度**
**https://www.ismap.go.jp/**
ISMAP（Information system Security Management and Assessment Program: 通称、ISMAP（イスマップ））は、政府が求めるセキュリティ要求を満たしているクラウドサービスを予め評価・登録することにより、政府のクラウドサービス調達におけるセキュリティ水準の確保を図り、もってクラウドサービスの円滑な導入に資することを目的とした制度です。

## ☛ IT活用を支援する情報処理支援機関

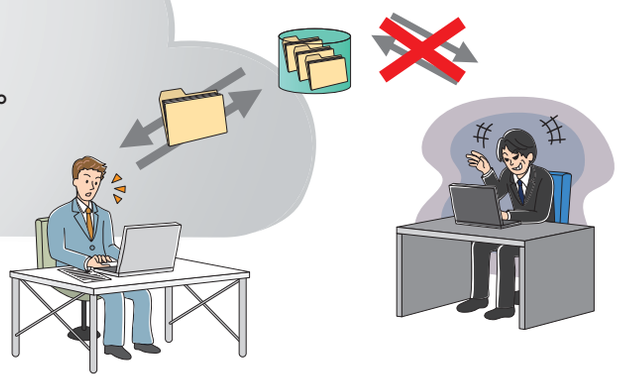
中小企業者等の生産性向上に資するITツールや中小企業のIT活用を支援するITベンダーを法令に基づいて認定し、中小企業者がITツール選定するために必要となる情報を開示しています。

**情報処理支援機関（スマートSMEサポーター）制度**（中小企業庁）
**https://www.smartsme.go.jp/**
中小企業が使いやすいITツールの開発促進や中小企業のIT導入を通じた生産性向上を図ります。
認定を受けたITベンダーの情報セキュリティ対策の実施状況を確認できます。

Smart SME Supporter

# Ⅱ．運用するときのポイント

**クラウドサービスを安全に利用するために、**
**利用者側の体制やセキュリティ対策を決めます。**



## チェックシートNo.7

### 管理担当者を決める

クラウドサービスの技術的な側面などの特性を理解したうえで、業務に適した運用や設定・操作・ヘルプデスクを行うことができる、管理担当者を社内に確保しましょう。

**例えば**

**クラウド型顧客管理システムの運用にあたり、**
**●入力項目やその活用については営業部長が担当する**
**●技術的な設定や社内のヘルプデスクはシステム管理者が担当する…など**

## チェックシートNo.8

### 利用者の範囲を決める

クラウドサービスを利用する人の範囲を決め、どのような権限を与えるか適切に管理しましょう。

**例えば**

**販売管理をクラウドサービスで行うにあたり、**
**●社長と販売部門従業員だけに利用者アカウントを作成する**
**●承認権限は従業員の上司に付与する…など**

## チェックシートNo.9

### 利用者の認証を厳格に行う

パスワードなどの認証機能を適切に設定・管理しましょう。

**例えば**

**なりすましや不正ログインを防ぐために、**
**●パスワードは破られにくい安全なパスワードを利用する**
**●ID・パスワードの共有はしない**
**●サービスで以下の認証方式が提供されている場合は利用する**
**➢特定のパソコンでしか利用できないように電子証明書※3をインストールする**
**➢パスワードを不正利用されてもログインはできないように「2段階認証」※4を用いる…など**

※3）電子証明書インターネットでクラウドサービスを利用するときに特定のPCからしかアクセスできないように制限するための「身分証明書」です。
※4）複数の要素（記憶、所持、生体情報）を用いた認証方式である「多要素認証」や、同じ要素の認証を多段で実施する認証方式である「多段階認証」などがあります。

## チェックシートNo.10

### バックアップに責任を持つ

サービス停止やデータの消失・改ざん等に備えて、重要情報を手元に確保して、必要なときに使えるようにしましょう。

**例えば**

**会計データやホームページなど、消失や改ざんの影響が大きいものは、**
**●クラウドサービスの拡張機能にバックアップがある場合は利用する。**
**●定期的に社内の専用ハードディスクなどにもバックアップを取得する**
**●直前のバックアップよりもさらに過去の状態に遡って復元できるように複数世代※5のバックアップを取得する…など**

※5）毎月バックアップを取得する場合に前月だけでなく2ヶ月前、３ヶ月前のように複数のバックアップを取得しておくことです。

# III. セキュリティ管理のポイント

**クラウドサービス特有のリスクや関連する法令について対応できているか確認します。**


チェックシートNo.11

## 付帯するセキュリティ対策を確認する

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るか確認しましょう。

**例えば**

**サイバー攻撃や通信傍受に対する対策が十分されているか、**
- **通信の暗号化**
- **ファイアウォールや侵入検知**
- **ウイルス対策**
- **サービスで使っているOSやソフトウェアの脆弱性対応・セキュリティパッチの適用について公開されているか確認する…など**

チェックシートNo.12

## 利用者サポートの体制を確認する

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）が提供されているか確認しましょう。

**例えば**

**クラウドサービスを社内のシステム担当者不在の週末も利用するため、**
- **サポートの受付時間（週末夜間も受付可能か）**
- **連絡方法（メール、電話、チャット、オンライン、のうちパソコンがない事務所から週末も電話連絡可能か）**
- **料金（頻繁に問い合わせた場合に料金はどのぐらいか）を確認する…など**

チェックシートNo.13

## 利用終了時のデータを確保する

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。

**例えば**

**利用中のクラウド型会計システムを他のクラウドサービスに変更するにあたり、**
- **過年度データを含む全データを返却または社内のパソコンなどにダウンロードできるか**
- **データのフォーマットは他のサービスと互換性があるか**
- **移行先のサービスは返却されたデータを一括して取り込む機能があるか**
- **返却後にシステム上に残るデータは完全に消去または再利用されないことが保証されているかを確認する…など**

チェックシートNo.14

## 適用法令や契約条件を確認する

個人情報保護など関連法規制の遵守などを規定した利用規約等について確認しましょう。

**例えば**

**クラウドサービスに秘密情報や個人情報を保存するため、**
- **利用者が入力したデータにサービス事業者がアクセスする場合の条件や責任について明記されているか**
- **設備の保守等を再委託している場合の再委託先の管理監督責任について明記されているか**
- **利用者が入力した個人情報に関して個人情報保護法に準拠することが明記されているか（安全管理措置、委託先の監督）を確認する…など**

# 解説編

**チェックシートNo.15**

## データ保存先の地理的所在地を確認する

データがどの国や地域に設置されたサーバーに保存されているか確認しましょう。

**例えば**

**インターネットを通じて商品やサービスを海外に販売する越境ECを開店するにあたり、**
**●プラットフォームを構築するデータセンターの所在国・地域と現地の個人情報保護に係わる法律・規制※6を確認する**
**●現地の法律・規制に基づきプライバシーポリシー制定や個人情報の取り扱いについて事前に承諾を得るためのオプトインシステムを導入する…など**

※6）以下のような法律・規制があります。
・個人情報保護法第24条外国第三者提供個人データを外国にある第三者に提供する場合は、あらかじめ本人の同意を得なければならないことがあります。
・EU一般データ保護規則（General Data Protection Regulation：GDPR）日本国内の企業でも欧州経済領域（European Economic Area：EEA、EU加盟国28カ国、ノルウェー、アイスランド、リヒテンシュタイン）と個人データをやり取りする場合に適用対象となります。
・アメリカ・カリフォルニア州　消費者プライバシー法（California Consumer Privacy Act：CCPA）アメリカ カリフォルニア州民の個人データを守るための法律です。
・中国・個人情報保護法（Personal Information Protection Law：PIPL）中華人民共和国におけるデータのプライバシーと保護に関し詳細な規則を定めた法律です。

# 情報セキュリティ対策に役立つ情報

### 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（経済産業省）

クラウドサービスの利用にかかわるリスク対応のために JIS Q 27002（実践のための規範）から適切な管理策を選択し，導入するための助言とその最適な実施のための手引を提供している

**https://www.meti.go.jp/policy/netsecurity/downloadfiles/cloudsec2013fy.pdf**

### クラウドセキュリティガイドライン活用ガイドブック（経済産業省）

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ている

**http://www.meti.go.jp/policy/netsecurity/downloadfiles/cloudseckatsuyou2013fy.pdf**

### クラウドサービスの安全・信頼性に係る情報開示指針（総務省）

クラウドサービスの安全・信頼性を向上させることを目的として、利用者のサービス選定における情報収集の負担を軽減する観点から、クラウドサービス事業者によるクラウドサービスに係る情報開示のあり方を示した指針

**http://www.soumu.go.jp/main_content/000477838.pdf**

### SECURITY ACTION セキュリティ対策自己宣言（独立行政法人情報処理推進機構）

中小企業自らが情報セキュリティ対策に取組むことを自己宣言する制度で、自社の状況に応じて「一つ星」と「二つ星」の2段階の取組み目標を用意している

**https://www.ipa.go.jp/security/security-action/**

IPA 独立行政法人 情報処理推進機構

〒113-6591 東京都文京区本駒込2丁目28番8号
文京グリーンコートセンターオフィス
TEL 03-5978-7530　FAX 03-5978-7513
E-mail isec-pr-cssp@ipa.go.jp　URL https://www.ipa.go.jp

2026.3.27 Version2.2