

セキュリティマネジメント指導 (テーマ別) 実施要領

テーマ③ | クラウドサービスの安全利用

独立行政法人情報処理推進機構(IPA)
セキュリティセンター

本資料の位置づけ（指導の全体像）

本資料は、セキュリティ専門家が中小企業に対して行う訪問指導「**セキュリティマネジメント指導（テーマ別）**」の説明資料です。

訪問指導では、専門家が中小企業の特성에応じたセキュリティ対策を指導する際の基本的なフレームワークを提供することを目的としています。特に中小企業は、限られたリソースの中で情報セキュリティ対策を行う必要がありますが、どの部分に重点を置くべきかが明確でないケースが多々あります。

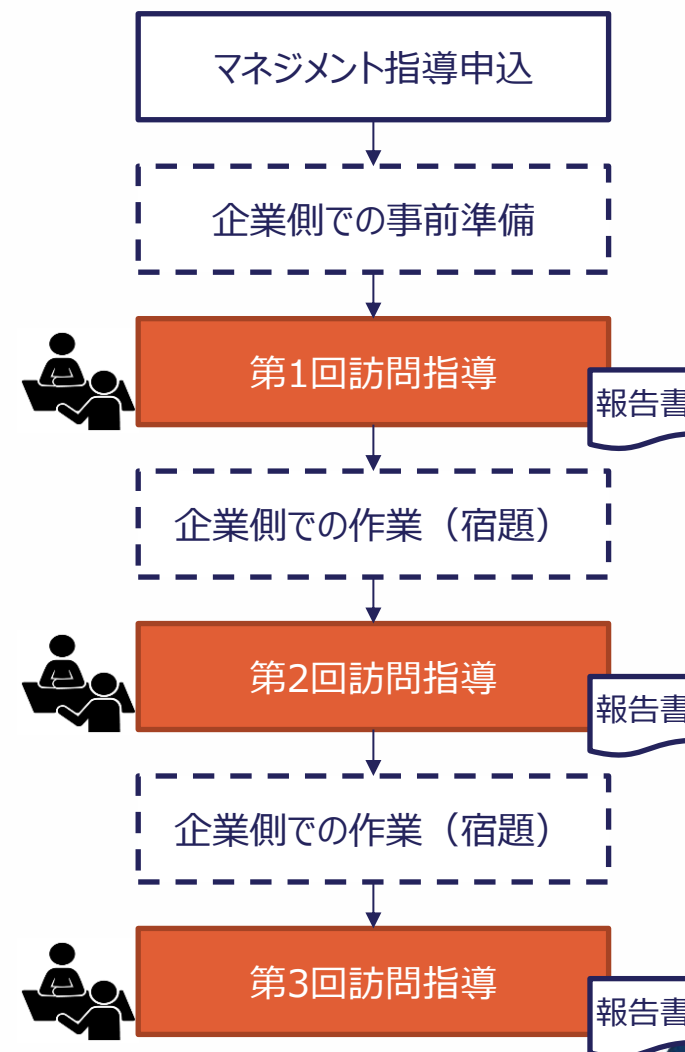
マネジメント指導（テーマ別）では、そのような中小企業に対して、**①情報セキュリティ規程の整備**、**②情報資産の洗い出しとリスク分析**、**③クラウドサービスの安全利用**、**④セキュリティインシデント対応**、そして**⑤従業員向けのセキュリティ教育**の5つの主要なテーマを指導するための具体的な方法と手順を提供しています。

各テーマにおいては、どのような企業がその指導を必要としているのか、指導によって達成されるべき目標、さらには具体的な作業内容や使用ツール、指導後の効果の考え方等を想定しています。これにより、専門家は訪問先の企業ごとに適切な指導計画を立て、効率的に支援を行うことができると考えています。

本資料では、専門家が現場で利用できる具体的なシラバスやチェックシート、ガイドラインも挙げております。実際には企業に訪問した際は、企業の実情に応じた柔軟な対応をお願いすることとなりますが、ツール活用によってある程度訪問指導の際の一貫性が確保され、企業においても自律的なセキュリティ対策の強化が期待できると考えます。

専門家のみなさまにおかれましては、本資料に記載された趣旨をご理解の上、中小企業へのセキュリティ個別指導にご対応ください。

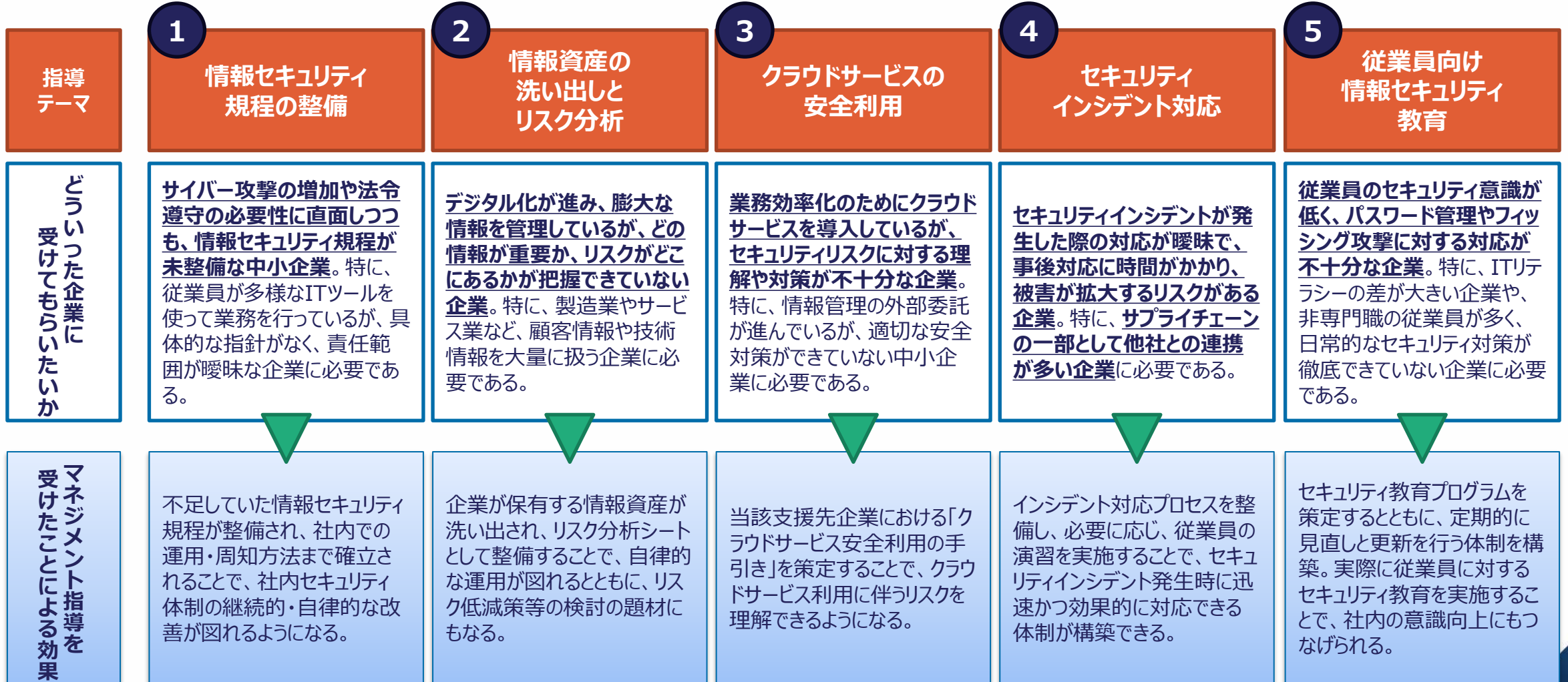
マネジメント指導の流れ



マネジメント指導のテーマと狙い

今回用意したマネジメント指導のテーマは以下の5テーマです。

企業の実情に即し、原則として以下のテーマから選定の上、企業への訪問指導を行っていただきます。



本書の構成

- 企業へのマネジメント指導を行うにあたり、5つの指導テーマについて、主にIPAのセキュリティ対策支援ツールを活用した3回の標準的な専門家の指導内容（標準シラバス）と、指導先企業の依頼・調整事項や指導にあたっての基本的な留意点を説明する「実施要領」を作成しました。
- 「実施要領」は、セキュリティの専門家による指導の下、今後も継続して活用できるものとなるよう、標準シラバスを示しつつ、指導先企業の個別事情に応じた指導に必要なツールの活用方法、経験者の体験による気付きや工夫など実践的なノウハウを提供する内容としています。

具体的支援 の進め方	標準シラバス	専門家指導全体の構成と留意事項 ・専門家指導の全体構成 ・各回ごとの指導の内容（標準的な進め方） ・指導に当たっての留意点
	ツール解説編	各種ツールの活用方法 ・使用するツール/資料 ・参考資料

テーマ③ | クラウドサービスの安全利用

【標準シラバス】
専門家指導全体の構成と留意事項

- ## マネジメント指導業務の達成目標と成果物

達成目標 3

達成目標 2

継続
実施

成果物

取組みスタート

達成目標 1

● 5分でできる！ 情報セキュリティ自社診断 (Excel版) による現状リ
スク洗い出し結果

- 社内におけるクラウドサービスの洗い出し

- クラウドサービス
に対する安全利
用チェック実施

[illegible]

「標準的な進め方」の全体構成

1～2
週間

事前準備#1

- *IPA自社診断(Excel版)の実施依頼
- *「クラウドサービス台帳」における既存/予定クラウドサービス洗い出し作業の実施依頼

第1回

既存及び検討中クラウドサービスの洗い出し

支援先企業のビジネス内容や組織概要等を聞き取った上で、企業側が作成したクラウドサービス台帳に基づきヒアリングを行い、必要に応じ加筆修正指示を行います。

1～2
週間

事前準備#2

- *前回の指導を通じて得た情報をもとにチェックを実施
- *特に「チェックが十分でない」と評価されたクラウドサービスに対するリスク低減策や回避策について検討
- *社内運用に向けて、当該企業用のクラウドサービス利用ガイドライン案及び安全利用チェックシートの案を作成

第2回

チェックシートに基づく、クラウドサービスのリスク評価

企業側が作成したチェックシート及びガイドライン案に基づきヒアリングを行い、必要に応じ加筆修正指示を行うとともに、企業側が示したリスク回避策や低減策についてアドバイスを行います。また、継続的な運用方法の考え方について指南します。

1～2
週間

事前準備#3

- *各サービスの安全利用チェックについて引き続き検討
- *社内運用に向けて、周知の方法や運用プランを策定

第3回

チェックシートに基づく、クラウドサービスのリスク評価（継続）

引き続き、企業側が作成したチェックシート及びガイドライン案に基づきヒアリングを行い、必要に応じ加筆修正指示を行うとともに、企業側が示したリスク回避策や低減策についてアドバイスを行います。また、継続的な運用方法の考え方について指南します。
また、以後の継続運用に際してのアドバイスも行います。

計1.5ヶ月
程度

「標準的な進め方」の詳細（1）

第1回 既存及び検討中クラウドサービスの洗い出し

		企業	専門家	成果物/提供ツールなど
事前準備	1	提供可能な社内資料の準備 (企業紹介のパンフレット等)	ホームページなどによる企業の情報収集とヒアリング シートの作成（企業・事業の理解）	【提供】指導講習コンテンツ
	2	「5分でできる！自社診断（Excel版）」による自己診断の実施	（事前配付）	【提供】5分でできる！自社診断チェックシート（Excel版）
	3	「クラウドサービス台帳兼チェックリスト」による 既存/予定クラウドサービスの洗い出し	クラウドサービス洗い出しの実施依頼	【提供】クラウドサービス台帳兼チェックリスト
	4	出席メンバー選定 (経営者/従業員等、半日x3回)	専門家指導の作業内容、全体スケジュール案の作成、初回訪問日程の事前確認	初回のスケジュール調整
当日	1	説明事項に対するディスカッション(確認・了解)	今回の訪問指導の目標、作業内容、全体スケジュール、成果物等の説明と合意	【提供】指導講習コンテンツ
	2	自社診断(Excel版)の結果の理解と課題認識についてのディスカッション	自社診断(Excel版)の結果についての説明と、改善領域に関する現状確認と要望の確認	【成果物】自社診断(Excel版)の結果のまとめ
	3	「クラウドサービス台帳兼チェックリスト」の結果と課題認識についてのディスカッション	「クラウドサービス台帳兼チェックリスト」結果を踏まえ、各クラウドサービスに対するリスク評価の考え方について指南（重要度が高いもの等）	【成果物】クラウドサービス台帳兼チェックリスト作成指示
	4	依頼事項についての確認と了解	シートにリストアップした各サービスについて、指導内容を踏まえ、次回までにリスク分析作業を実施	（終了後） 実施報告書の作成

＜実施のポイント＞

- 第1回の指導では、ヒアリングによって、企業側で現在活用している／今後活用予定のクラウドサービス洗い出し状況について把握します。
- 「5分でできる！情報セキュリティ自社診断」は、経営者だけではなく従業員にも実施してもらうことで、実態をより明確にできます。
- 自社診断結果が高得点で、リスクが見えない場合には、本当に対応できているのか、例外的に見逃していることは無いかなど、突っ込んだ質問を行って課題を洗い出し、重点改善領域についてディスカッションします。

「標準的な進め方」の詳細（2）

第2回 チェックシートに基づく、クラウドサービスのリスク評価

		企業	専門家	成果物/提供ツールなど
事前準備	1	依頼された必要情報の準備	前回訪問で得た情報の整理・分析 (理解に齟齬が無いが訪問時に確認する)	-
	2	リストの見直しを行うとともに、支援先企業においてリストアップしたクラウドサービスについて安全利用チェックを実施	第2回の資料作成 ・安全利用チェック状況について整理 ・重点改善領域の見極め	【提供】クラウドサービス台帳兼チェックリスト
当日	1	依頼された必要情報の提供・説明	提供された情報の確認・質疑応答	-
	2	各クラウドサービスに対する安全利用チェック結果と、考えられるリスク回避・低減策について説明・ディスカッション	安全利用チェック結果に対しアドバイス・ディスカッション (*安全利用チェックの考え方について指南する。特にクラウドサービスの「導入時」「運用時」「セキュリティ管理」の観点から、チェック項目として重視すべきポイント等について伝える。企業側からの疑問や質問に答える。)	【成果物】クラウドサービス台帳兼チェックリスト
	3	必要な追加情報の提供了解	改善領域の対策検討に必要な追加情報の提供依頼	(終了後) 実施報告書の作成

<実施のポイント>

- 「クラウドサービス台帳兼チェックリスト」の結果を改めて事前に分析し、リスク大と評価されうる項目を指摘して、緊急度、重要度、難易度などの視点から、対策の優先順位についてディスカッションを行います。
- リスク回避・低減策の考え方は、各企業の状況によって異なります。ビジネスの内容や取り扱う情報の性質、社外関係先の状況も踏まえ、過度にハードルを上げることにならないよう、実効性を高めるようガイドしていきます。

「標準的な進め方」の詳細（3）

第3回 チェックシートに基づく、クラウドサービスのリスク評価（継続）

		企業	専門家	成果物/提供ツールなど
事前準備	1	急がれる改善施策の実現性の検討 (実現のための課題や対策の事前検討)	前回訪問結果の整理と、絞り込んだ具体的対策の実施計画案の作成	-
	2	クラウドサービス安全利用チェック結果を踏まえ、対応不十分なサービスへの対応方法を検討し、情報セキュリティ対策を検討する	適宜アドバイス	【提供】クラウドサービス台帳兼チェックリスト 【提供】付録6「中小企業のためのクラウドサービス安全利用の手引き」
当日	1	「中小企業のためのクラウドサービス安全利用の手引き」を活用した情報セキュリティ対策案について説明	クラウドサービス安全利用策に対しアドバイス・ディスカッション	【成果物】クラウドサービス台帳兼チェックリスト
	2	専門家指導についての評価	指導結果のまとめと評価	(終了後) 指導結果のまとめと評価を行う 【成果物】最終報告書

<実施のポイント>

- 第3回までの面談・ディスカッションを経て、クラウドサービス台帳兼チェックリストを完成させます。当日は全体の成果物について、レビューと合意を行います。
- 可能であれば、引き続き社内での情報セキュリティ対策の実効性を高めるため、数ヶ月後にチェックポイントを設けるなど、継続した支援活動(有料)の提案を行い、専門家としての次のステップとなる自走化を目指します。
- 計画される情報セキュリティ対策は、経営者が自分事として取り組める実効性と納得感のあるものとします。

指導先企業への依頼や調整事項

確認・調整事項	依頼・調整のポイント
1 企業様の検討体制(参加メンバー)等の調整	✓ 経営層に加え、以下の現場のリーダー層～課長クラスに参加いただくことを推奨します。 ・事業や業務のプロセスに詳しい方 ・ITシステムの運用管理を担っている方
2 打ち合わせ場所や環境の確認/準備	✓ 会議室/プロジェクター等の環境確認/準備をお願いします。 ・映像コンテンツの投影や、ディスカッションの効率に大きな影響があります。 ✓ 検討方法は、各専門家のやり方(経験)を踏まえ実施します。 ・原因を掘り下げ、メンバーの納得感と実効性のある対策に結びつけます。(企業によって、検討方法が異なる場合があります)
3 指導環境の調整 (コミュニケーション環境)	✓ 原則として訪問による現地指導を行いますが、初回を除く2回目以降で訪問と同等の指導がオンラインでも可能であることが見込まれ、かつ指導企業が合意した場合に、オンラインによる指導を行う場合もあります。
4 提供を受ける情報の取り扱い	✓ 指導企業にいただいた情報は、専門家において取り扱いに留意します。

【ツール解説編】 各種ツールの活用方法

使用するツール/資料の内容（自社診断結果）

- IPAが提供する「5分でできる！情報セキュリティ自社診断」を使用します。
- Excelファイルをそのまま、または印刷して実施してください。Excelファイルは、IPA Webサイトからダウンロードが可能です。
<https://www.ipa.go.jp/security/guide/sme/5minutes.html>



自社診断のための25項目

- **基本的対策（5項目）**
脆弱性対策、ウイルス対策、パスワード強化など
- **従業員としての対策（13項目）**
標的型攻撃メール、電子メール、ウェブ利用、持ち出し、廃棄など
- **組織としての対策（7項目）**
守秘義務、教育、委託先管理、ルール化など

- 第1回目の事前準備として、指導先企業へ自社診断の実施を依頼の上、診断結果を共有します。
- 第1回目の指導後にヒアリング情報や診断結果をもとに、現状の対策や取り組み状況についての分析を改めて行います。
- 第2回目の指導時には、診断項目について「なぜそのように評価したか」、「例外はないか」などを掘り下げ、課題の抽出を進めます。重点改善領域と思われる項目を提示し、緊急度・重要度・難易度などの視点から、対策の優先順位付けについてディスカッションを行います。

自社診断実施の留意点（自社診断結果）

項目No.	診断内容	掘り下げるチェックポイント（例）
基本的対策	1 パソコンやスマホなど、情報機器のOSやソフトウェアは常に最新の状態にしていますか？	①. 状況を管理する担当者は決まっているか ②. 業務外のソフトウェアが勝手に導入されていないか ③. 従業員に、どのように徹底できているか
	2 パソコンやスマホなどにはウイルス対策ソフトを導入し、ウイルス定義ファイル※1 は最新の状態にしていますか？	①. すべてのパソコンの更新レベルが把握できているか ②. 「社長、役員は別」などの例外的な取り扱いはないか ③. 管理者/使用者がはっきりしないパソコンは無い
	3 パスワードは破られにくい「長く」「複雑な」パスワードを設定していますか？	①. 従業員に、どのように徹底できているか ②. 例外的に認められていることは無い
	4 重要情報※2 に対する適切なアクセス制限を行っていますか？	①. 初期設定のままになっている機器はないか ②. 設定内容を定期的にチェックしているか ③. 例外的に認められていることは無い
	5 新たな脅威や攻撃の手口を知り対策を社内共有する仕組みはできていますか？	①. 利用中のウェブサービスの棚卸しができているか ②. 注意喚起が迅速にできる仕組みが整っているか ③. セミナーなどの外部の情報も共有できているか

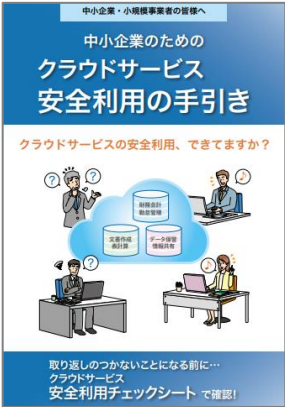
※1 コンピュータウイルスを検出するためのデータベースファイル「パターンファイル」とも呼ばれます。

※2 重要情報とは営業秘密など事業に必要で組織にとって価値のある情報や、従業員の個人情報など管理責任を伴う情報のことです。

チェックの判断根拠を十分に掘り下げることで、身の丈に合った有効な対策に絞り込みます

使用するツール/資料の内容（クラウドサービスチェックリスト）

- 「中小企業の情報セキュリティ対策ガイドライン 第3.1版」の付録6「クラウドサービス安全利用の手引き」の考え方をもとに、「クラウドサービス台帳兼安全利用チェックリスト」を作成します。
- チェックリストをもとに、今後の社内でのクラウドサービス安全利用策を検討します。



クラウドサービスの選定

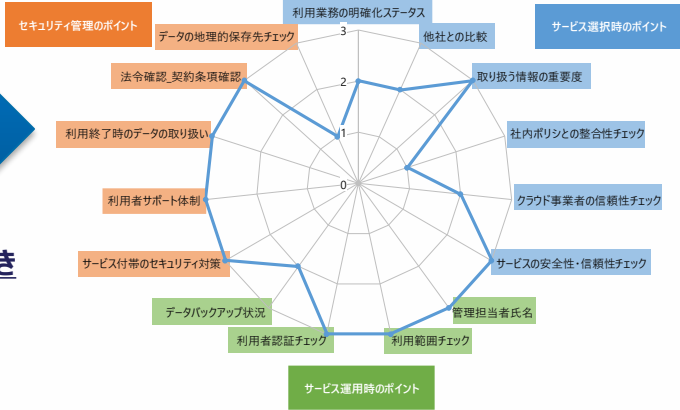
クラウド化する業務によって重視すべきセキュリティ対策は異なるため、**業務のセキュリティ要件に見合ったサービスを**選定しましょう。

クラウドサービスの運用

クラウドサービスは**提供者と利用者が連携して運用**するため、その特性を理解して運用しましょう。

クラウドサービスのセキュリティ対策

クラウドサービス利用者が**対応すべきセキュリティ対策**を理解して実施しましょう。



<クラウドサービス台帳兼安全利用チェックシート>

管理番号	サービス名	所管部署	サービスの概要	ステータス	サービス利用開始日	サービス利用終了（予定）日	Ⅰ. サービス選択時のポイント					Ⅱ. サービス運用時のポイント				Ⅲ. セキュリティ管理のポイント					総合評価	
							利用業務の明確化ステータス	他社との比較	取り扱う情報の重要度	社内ポリシーとの整合性チェック	クラウド事業者の信頼性チェック	サービスの安全性・信頼性チェック	管理担当者氏名	利用範囲チェック	利用者認証チェック	データバックアップ状況	サービス付帯のセキュリティ対策	利用者サポート体制	利用終了時のデータの取り扱い	法令確認、契約条項確認		データの地理的保存先チェック
S0001	〇〇オンラインストレージサービス	営業部	外部顧客との営業関係書類受け渡し用	利用中	2024/4/1	未定	一部明確化できている	確認中	確認した	問題があるが対処方法なし	確認中	すべて確認済（約款添付）	担当者アサイン済	すべて管理できている	すべて管理できている	一部管理できている	すべて具体的に公開されている	ヘルプデスクあり	確認した	確認した	未確認	37
S0002	△△クラウド財務会計v2	財務部	所内財務会計、税務申告、給与計算	利用中	2023/4/1	未定	一部明確化できている	確認中	確認した	問題があるが対処方法なし	わからない	わからない	担当者アサイン済	すべて管理できている	すべて管理できている	一部管理できている	わからない	ヘルプデスクあり	確認した	わからない	未確認	26
S0003	××勤怠管理WEBシステム	総務部	所内労務管理	利用中	2023/4/1	未定	一部明確化できている	確認中	確認した	問題があるが対処方法なし	わからない	わからない	担当者アサイン済	すべて管理できている	すべて管理できている	一部管理できている	わからない	ヘルプデスクあり	確認した	確認した	未確認	29
S0004	□□ECプラットフォーム	営業部	オンライン通販システム	調査中	未定	未定	一部明確化できている	確認中	確認した	問題があるが対処方法なし	わからない	わからない	担当者アサイン済	一部管理できている	一部管理できている	未確認	わからない	わからない	わからない	わからない	未確認	17
S0005	△△クラウド財務会計v1	財務部	所内財務会計、税務申告、給与計算	利用終了	2020/4/1	2024/3/31	一部明確化できている	確認中	確認した	わからない	わからない	わからない	未了	未確認	未確認	未確認	わからない	わからない	わからない	わからない	わからない	11

成果物作成の留意点（クラウドサービスチェックリスト）

- **選択**するときの確認ポイント（6 項目）
 - ・ 何に使うか、どんな情報を扱うか？
 - ・ サービス事業者は信頼できるか？
- **運用**するときの確認ポイント（4 項目）
 - ・ 誰が使うのか、どう管理するか？
 - ・ 誰が責任を持つか？
- **セキュリティ管理**のポイント（5 項目）
 - ・ 事業者のセキュリティ対策は、サポートは？
 - ・ データ保存先は何処の地域か？

使用するツール/資料の内容（クラウドサービスチェックリスト）



- 「クラウドサービス台帳兼安全利用チェックリスト」作成に際しては、「クラウドサービスの選択」「クラウドサービスの運用」「セキュリティ管理」の3つのフェーズにおける確認ポイントに留意し、それぞれの水準まで安全利用チェックが進められているかを記載します。
- リストアップの対象としては、すでに社内で活用しているクラウドサービスに加え、今後利用を検討しているサービスも含めます。
- まずは、「クラウドサービス台帳兼チェックリスト」シートのA列～I列に、導入済み及び今後導入予定のクラウドサービスを列挙してください。
- システムごとに個票を作成し、そのデータを一覧表に転記することもできます。

クラウドサービス台帳兼安全利用チェックシート								
管理番号	サービス名	作成日	記入担当者氏名	所管部署	サービスの概要	ステータス	サービス利用開始（予定）日	サービス利用終了（予定）日
記入例01	〇〇オンラインストレージサービス	2024/11/01	山田 一郎	営業部	外部顧客との営業関係書類受け渡し用	利用中	2024/4/1	未定
記入例02	△△クラウド財務会計v2	2024/11/02	吉田 太郎	財務部	所内財務会計、税務申告、給与計算	利用中	2023/4/1	未定
S0001	××勤怠管理WEBシステム	2024/11/03	鈴木 花子	総務部	所内労務管理	利用中	2023/4/1	未定
S0002	□□ECプラットフォーム	2024/11/04	山田 一郎	営業部	オンライン通販システム	調査中	未定	未定
S0003	△△クラウド財務会計v1	2024/11/05	吉田 太郎	財務部	所内財務会計、税務申告、給与計算	利用終了	2020/4/1	2024/3/31
S0004	クラウド顧客管理システムZZZ	2024/11/06	山田 一郎	営業部	顧客管理、営業管理、広報PRメールマガ管理等	調査中	未定	未定
S0005	WEBメール「Aメール」	2024/11/07	山田 一郎	営業部	■■プロジェクトにおけるJV関係者間共通メール	調査中	未定	未定

クラウドサービス安全利用チェックシート（個票）

管理番号：	S0005
対象サービス名：	WEBメール「Aメール」
作成日：	2024/11/07
記入担当者氏名：	山田 一郎
所管部署：	営業部
サービスの概要：	■■プロジェクトにおけるJV関係者間共通メール
ステータス：	調査中
サービス利用開始（予定）日：	未定
サービス利用終了（予定）日：	未定

分類	No	チェック項目	ポイント	チェック
Ⅰ. 選択するもののポイント	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？	明確化できていない
	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？	確認中
	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、クラウドサービスが停止した場合の影響を確認しましたか？	確認中
	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？	問題があるが対処方法なし
	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？	確認した
	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？	一部確認済（約款添付）
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？	担当者アサイン中
	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？	一部管理できている
	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？（共有しなし、複雑にするなど）	未確認
	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ときに使えるようにしていますか？	一部管理できている
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？	一部公開されている
	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？	ヘルプデスクなし
	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？	確認中
	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？	確認中
	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に保存されているか確認しましたか？	未確認

使用するツール/資料の内容（クラウドサービスチェックリスト）



クラウドサービス安全利用チェックシート（個票）

管理番号：	S0005
対象サービス名：	WEBメール「Aメール」
作成日：	2024/11/07
記入担当者氏名：	山田 一郎
所管部署：	営業部
サービスの概要：	■■プロジェクトにおけるJV関係者間共通メール
ステータス：	調査中
サービス利用開始（予定）日：	未定
サービス利用終了（予定）日：	未定

<個票からの転記手順>

- ① 「個票」ファイルの「クラウドサービス安全利用チェックシート | 記入用個票」シートに必要事項を記入します。
- ② 「貼り付けデータ生成」シートのA2～X2セルの値をコピーします。
- ③ コピーした情報を、「クラウドサービス台帳兼チェックリスト」ファイルの「一覧表」シートで、既存データの続きに「値貼り付け」します。
「形式を選択して貼り付け」→「値」

分類	No	チェック項目	ポイント	チェック
I. 選択するサービスのポイント	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、どのリソースや運用ルールを明確にしたか	
	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の漏えい、漏えい防止が停止した場合の影響を確認したか	
	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、障害発生時の対応体制が適切に示されているか	
II. 選択するサービスの運用のポイント	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決めるか	担当者アサイン中
	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範囲に限定できるように管理できているか	一部管理できている
	9	利用者の認証を厳格に行う	パスワードの認証機能にロックアウト機能（共有できない、復旧するなど）が実装されているか	未確認
	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、重要情報を手元で保管し、必要に応じて使えるようにしていますか	一部管理できている
III. サービス利用時のポイント	11	付帯するセキュリティ対策を確認する	サービス利用に伴うセキュリティ対策が具体的に公開されていますか	一部公開されている
	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	ヘルプデスクなし
	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、データの取り扱い条件について確認しましたか	確認中
	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	確認中
	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ビスに保存されているか確認しましたか	未確認

以下の1行をコピーし、一覧表の最下部に付け足して「値貼り付け」してください。

S0005	WEBメール「Aメール」	45603	山田 一郎	営業部	■■プロジェクトにおけるJV関係者間共通メール	調査中	未定	未定	明確化できていない	確認中	問題があるが対処方法なし	確認した	一部確認済（約款添付）	担当者アサイン中	一部管理できている	未確認	一部管理できている	一部公開されている	ヘルプデスクなし	確認中	確認中	未確認
-------	--------------	-------	-------	-----	-------------------------	-----	----	----	-----------	-----	--------------	------	-------------	----------	-----------	-----	-----------	-----------	----------	-----	-----	-----

この範囲をコピー

「貼り付けデータ生成」シート

クラウドサービス台帳兼安全利用チェック								Ⅰ. サービス選択時のポイント							Ⅱ. サービス運用時のポイント				Ⅲ. セキュリティ管理のポイント				
管理番号	サービス名	担当者氏名	所管部署	サービスの概要	ステータス	サービス利用開始 (予定) 日	サービス利用終了 (予定) 日	利用業務の明確化 ステータス	他社との比較	取扱い情報の 重要度	社内ポリシーとの 整合性チェック	クラウド事業者の 信頼性 チェック	サービスの安全性・ 信頼性 チェック	管理担当者氏名	利用範囲 チェック	利用者認証 チェック	データバックアップ 状況	サービス付帯の セキュリティ対策	利用終了時の データ処理	利用終了時の データの取り扱い	法令確認、契約 条件確認	データの地理 的保存先 チェック	
記入例01	〇〇オンラインストレージサービス	2024/11/01	営業部	外部顧客との営業関係書類受け渡し用	利用中	2024/4/1	未定	すべて明確化できている	確認した	確認した	問題がないことを確認済	確認した	すべて確認済(約款添付)	担当者アサイン済	すべて管理できている	すべて管理できている	すべて管理できている	すべて具体的に公開されている	ヘルプデスクあり	確認した	確認した	確認した	
記入例02	△△クラウド財務会計v2	2024/11/01	財務部	所内財務会計、税務申告、給与計算	利用中	2023/4/1	未定	一部明確化できている	確認中	確認した	問題があるが対処方法なし	わからない	わからない	担当者アサイン済	すべて管理できている	すべて管理できている	一部管理できている	わからない	ヘルプデスクあり	確認した	わからない	未確認	
S0001	××勤怠管理WEBシステム	2024/11/03 鈴木 花子	総務部	所内労務管理	利用中	2023/4/1	未定	一部明確化できている	確認中	確認した	問題があるが対処方法なし	わからない	わからない	担当者アサイン済	すべて管理できている	すべて管理できている	一部管理できている	わからない	ヘルプデスクあり	確認した	確認した	未確認	
S0002	□□ECプラットフォーム	2024/11/04 山田 一郎	営業部	オンライン通販システム	調査中	未定	未定	一部明確化できている	確認中	確認した	問題があるが対処方法なし	わからない	わからない	担当者アサイン済	一部管理できている	一部管理できている	一部管理できている	わからない	わからない	わからない	わからない	未確認	
S0003	△△クラウド財務会計v1	2024/11/05 吉田 太郎	財務部	所内財務会計、税務申告、給与計算	利用終了	2020/4/1	2024/3/31	一部明確化できている	確認中	確認した	わからない	わからない	わからない	未了	未確認	未確認	未確認	わからない	わからない	わからない	わからない	未確認	
S0004	クラウド顧客管理システムZZZ	2024/11/06 山田 一郎	営業部	顧客管理、営業管理、広報PRメール管理等	調査中	未定	未定	すべて明確化できている	確認中	確認した	問題がないことを確認済	確認中	すべて確認済(約款添付)	担当者アサイン済	すべて管理できている	一部管理できている	未確認	すべて具体的に公開されている	ヘルプデスクあり	確認中	確認した	確認中	
S0005	WEBメール「Aメール」	2024/11/07 山田 一郎	営業部	■■プロジェクトにおけるJV関係者間共通メール	調査中	未定	未定	明確化できていない	確認中	確認中	問題があるが対処方法なし	確認した	一部確認済(約款添付)	担当者アサイン中	一部管理できている	未確認	一部管理できている	一部公開されている	ヘルプデスクなし	確認中	確認中	未確認	

ここに「値」で貼り付け

「クラウドサービス安全利用チェックシート | 記入用個票」シート

使用するツール/資料の内容（クラウドサービスチェックリスト）



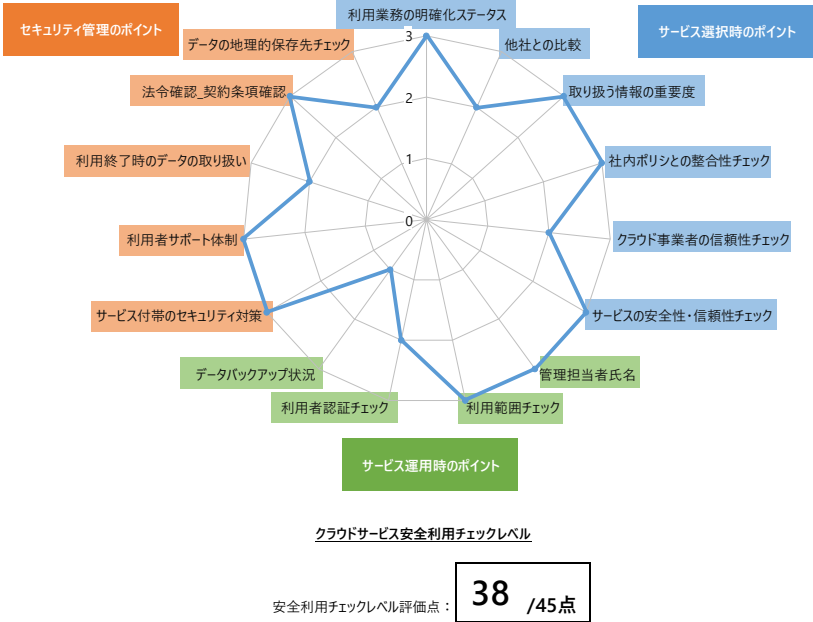
- 一覧表に記載されたサービスは、別シートで個票として分析結果を表示することができます。
- 個票では、「対象サービス名」の欄を選択することで、各サービスの安全利用チェックレベルに応じたレーダーチャートを表示します。
- レーダーチャートのへこみ部分等をもとに、安全利用チェックの方法や水準について検討してください。

クラウドサービス安全利用チェックシート（個票）

管理番号：	S0004
対象サービス名：	クラウド顧客管理システムZZZ
作成日：	2024/11/06
記入担当者氏名：	山田 一郎

分類	No	チェック項目	ポイント	チェック
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？	すべて明確化できている
	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？	確認中
	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、クラウドサービスが停止した場合の影響を確認しましたか？	確認した
	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？	問題がないことを確認済
	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？	確認中
	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？	すべて確認済（約款添付）
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？	担当者アサイン済
	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？	すべて管理できている
	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）	一部管理できている
	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ときに使えるようにしていますか？	未確認
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？	すべて具体的に公開されている
	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？	ヘルプデスクあり
	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、データの取り扱い条件について確認しましたか？	確認中
	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？	確認した
	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に保存されているか確認しましたか？	確認中

所管部署：	営業部
サービスの概要：	顧客管理、営業管理、広報PRメルマガ管理等
ステータス：	調査中
サービス利用開始（予定）日：	未定
サービス利用終了（予定）日：	未定



使用するツール/資料の内容（クラウドサービスチェックリスト）

- 各チェック項目は、安全性確認の度合いごとに4段階（3点・2点・1点・0点）のポイントが付しています。
- 各項目の取り組み状況とポイントの関係は以下の通りです。

項目	3点	2点	1点	0点
利用業務の明確化ステータス	すべて明確化できている	一部明確化できている	明確化できていない	わからない
他社との比較	確認した	確認中	まだ確認していない	わからない
取り扱う情報の重要度	確認した	確認中	まだ確認していない	わからない
社内ポリシーとの整合性チェック	問題がないことを確認済	一部不整合があるが修正対応中	問題があるが対処方法なし	わからない
クラウド事業者の信頼性チェック	確認した	確認中	まだ確認していない	わからない
サービスの安全性・信頼性チェック	すべて確認済（約款添付）	一部確認済（約款添付）	まだ確認していない	わからない
管理担当者氏名	担当者アサイン済	担当者アサイン中	未了	わからない
利用範囲チェック	すべて管理できている	一部管理できている	まだ確認していない	わからない
利用者認証チェック	すべて管理できている	一部管理できている	まだ確認していない	わからない
データバックアップ状況	すべて管理できている	一部管理できている	まだ確認していない	わからない
サービス付帯のセキュリティ対策	すべて具体的に公開されている	一部公開されている	公開されていない	わからない
利用者サポート体制	ヘルプデスクあり	ヘルプデスクなし	まだ確認していない	わからない
利用終了時のデータの取り扱い	確認した	確認中	まだ確認していない	わからない
法令確認_契約条項確認	確認した	確認中	まだ確認していない	わからない
データの地理的保存先チェック	確認した	確認中	まだ確認していない	わからない

中小企業のためのクラウドサービス安全利用の手引き

- 中小企業がクラウドサービスを安全に利用するための確認事項や注意点をまとめた手引き
 - ・ **クラウドサービス安全利用チェックシート**で確認すべきことが分かる
 - ・ 身近なサービスを例に、何を確認し、どうしたら安全に利用することができるか分かる

クラウドサービスの 選定

クラウド化する業務によって重視すべきセキュリティ対策は異なるため、**業務のセキュリティ要件に見合ったサービス**を選定しましょう。

クラウドサービスの 運用

クラウドサービスは**提供者と利用者が連携して運用**するため、その特性を理解して運用しましょう。

クラウドサービスの セキュリティ対策

クラウドサービス利用者が対応すべきセキュリティ対策を理解して実施しましょう。



クラウドサービス安全利用に関するポイント

クラウドサービスとは？

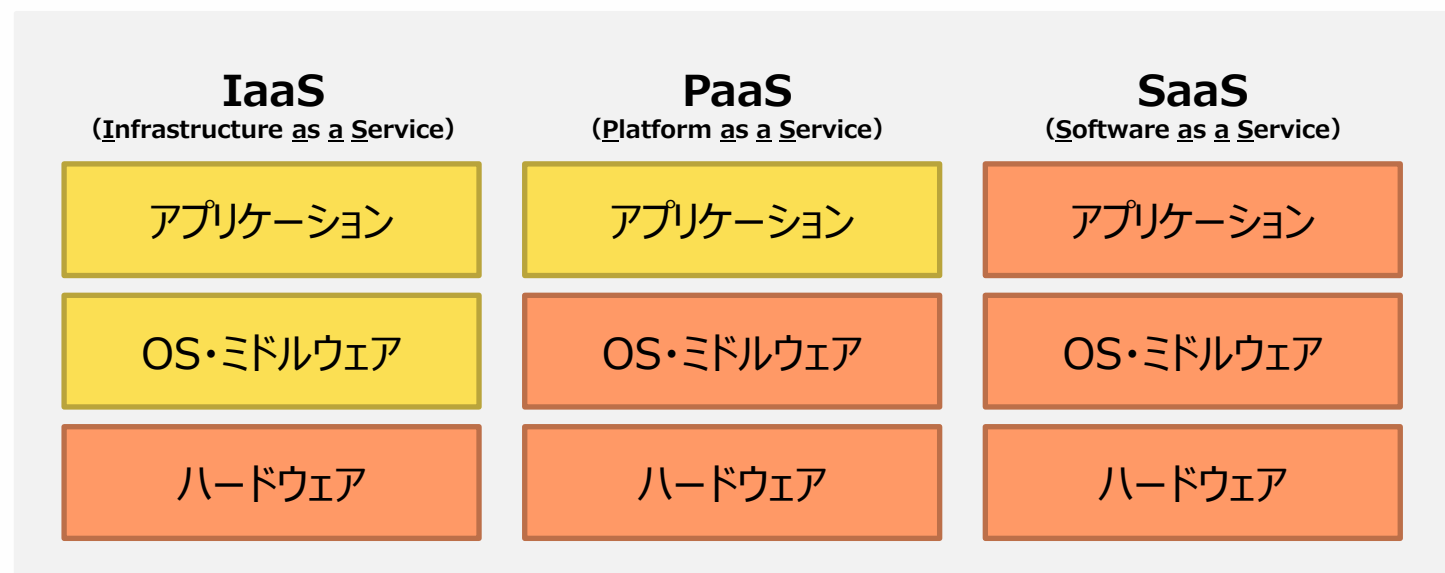
- インターネットを通じてソフトウェアやハードウェアを利用する情報システムサービス
- インターネットの普及、仮想化技術など、関連技術の進展で、身近になった
- 情報システムは、雲（クラウド）の向こうのように、利用者から見えない

自社保有

オンプレミス



クラウドサービス



自社が
調達・運用・保守

クラウド事業者が
調達・運用・保守

クラウドサービス安全利用に関するポイント

身近なクラウドサービスの例

- 経営管理アプリケーション
 - ・ 財務会計、税務申告、給与計算、労務管理など
- 業務アプリケーション
 - ・ 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
- オフィスアプリケーション
 - ・ ワードプロ、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

クラウドサービス活用の利点

- ITの調達に関わる負担からの解放または負担の軽減
- ITの運用・保守の負荷からの解放または負荷の軽減
- IT資源利用の柔軟性・拡張性の獲得
- 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

クラウドサービス安全利用に関するポイント

クラウドサービス利用上留意すべき事項

- コンピュータを自ら管理しないことによる制約
- 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
- 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
- 利用できるアプリケーションのカスタマイズの制約
- 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

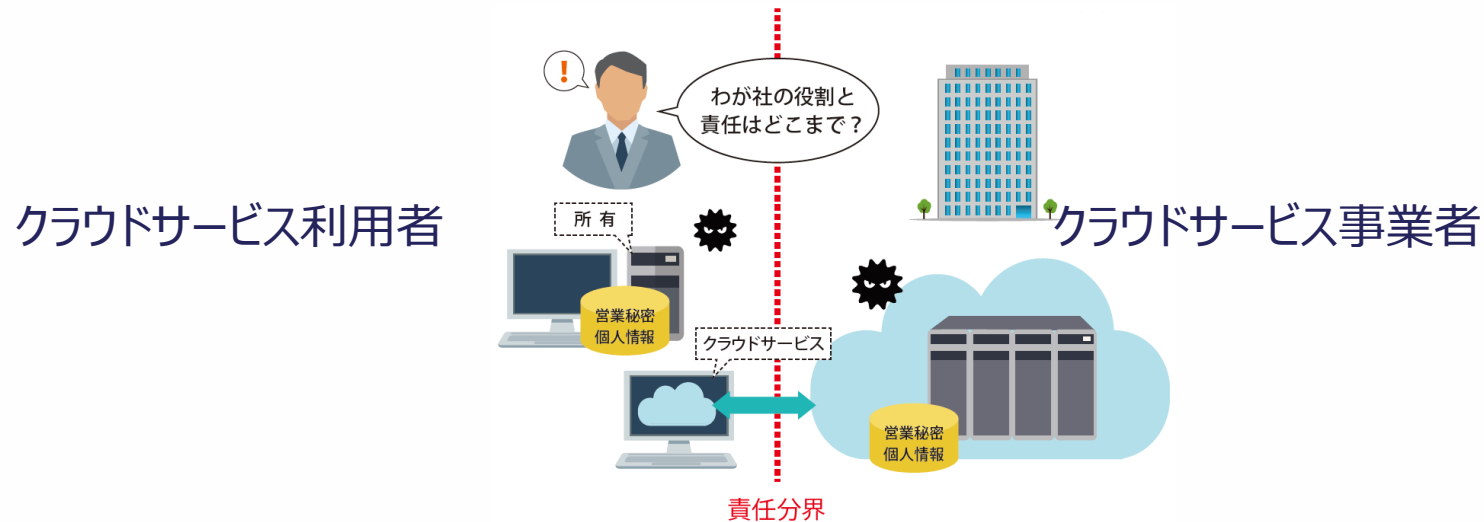
クラウドサービスの事故事例

- 国立研究開発法人
 - ・ 5,000件を超える個人情報や未公表の研究情報がクラウドサービス（メールシステム）と内部システムから漏えい
 - ・ クラウドサービスへの不正アクセスを契機としたサイバー攻撃が原因
- レンタルサーバー・クラウドサービス事業者
 - ・ 5,000件を超える顧客データが消失
 - ・ 事業者側のシステムメンテナンスの作業ミスが原因
- ファイル転送サービス事業者
 - ・ 480万件を超える利用者の個人情報とログイン情報が漏えい
 - ・ サーバーの脆弱性に対するサイバー攻撃が原因

クラウドサービス安全利用に関するポイント

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事業者と利用者が、役割・責任を分担し、対策を実施することで維持・向上
- **クラウドサービス安全利用チェックシート**と**解説編**で利用者の役割・責任を認識して、サービスを活用



1. どの業務で利用するか明確にする

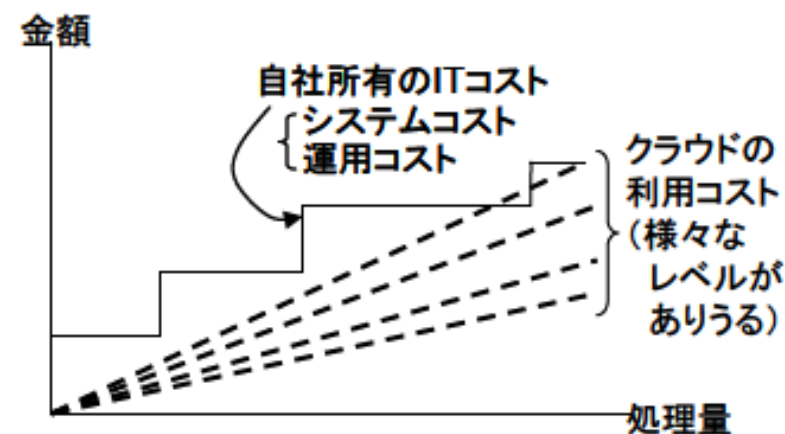
**どの業務をクラウドサービスで行い、
どの情報を扱うかを検討し、業務の切り分けや
運用ルールを明確にしましたか？**

- クラウドを利用する業務の選定
 - (例) 社内の情報共有のために
 - グループウェアを利用し、従業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
- 運用ルールの検討

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？

- 業務に最適のサービスを選定
- メリットの確認
 - ・ 業務品質は？
 - ・ 業務コストは？
 - ・ 業務時間短縮は？
 - ・ その他…



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？

- 取り扱うデータの重要性を確認
(例) 個人情報、営業秘密、カタログ情報
- 漏えい、改ざん、消失、停止の影響
(例) お客様情報の漏えい
 - 謝罪、補償
 - 個人情報保護委員会へ報告
 - 被害拡大防止、再発防止のための費用 ...など

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？**

- 社外に置くことを禁止しているデータ
（例）マイナンバー、お客様から預かった情報
- ルール変更とセキュリティ対策の検討 ...など

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？

● クラウド事業者の信頼性の確認

(例) 確認方法

- 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・認定制度の取得状況を確認する ...など

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？**

- サービスの安定性、信頼性の確認
- 稼働率、障害発生頻度、障害時の回復目標時間等
- 計画的サービス停止の事前通知
- 障害発生時の通知、ユーザ対応、情報提供等
- SLA（サービスレベル合意書）の意味するもの
- サービス状態のリアルタイム情報表示 ...など

【参考】クラウドサービス選択時に参考となる制度等

● ISMAP（政府情報システムのためのセキュリティ評価制度）

- 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

● ISMSクラウドセキュリティ認証

- 通常のISMS（ISO/IEC 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

- 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。

● ASP・SaaS情報開示認定制度

- 安全性・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していることを認定する制度です。

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？**

● 管理担当者の選任

(例) クラウド型顧客間システムの導入にあたり管理担当者を選任

- 入力項目やその活用 担当：営業部長
- 技術やヘルプデスク 担当：システム管理者 ...など

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？**

- サービスが必要なのは誰か？
（例）社長と営業部門だけ利用者アカウントを作成する
- 誰に、どのような権限を与えるか？
（例）承認権限は管理職に付与する ...など

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)**

- パスワード
 - 攻撃に対して破られにくいもの
 - ID・パスワードを共有しない
- その他の認証機能も利用
 - 電子証明書
 - 2段階認証 ...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？**

- 拡張機能にバックアップがある場合は利用する
- 社内のストレージにバックアップする
- 複数世代取得する ...など

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？**

- 通信の暗号化（https、VPN 等）
- ファイアーウォール、侵入検知
- ウイルス対策
- 脆弱性対応、セキュリティパッチ ...など

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？**

- サポート受付時間（週末夜間も受付可能か）
- 連絡方法（メール、電話、チャット、オンラインなど）
- 料金 ...など

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？**

- 全データの返却、パソコンなどにダウンロード
- データの互換性、移植性
- 残留データの完全消去
- 別の利用者が再利用できないことを保証 ...など

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？**

- 利用者の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
- 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
- 利用者が入力した個人情報に対する個人情報保護法準拠 ...など

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？**

- 事業者または事業者が利用しているプラットフォーム事業者・インフラ事業者が公表するデータセンターが所在する国・地域
- 個人情報保護に係わる国内および海外の法律・規制
 - 外国にある第三者への提供（個人情報保護法）
 - EU域内 GDPR（一般データ保護規則） ...など

【参考】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関わるリスク対応のためにJIS Q 27002から適切な管理策を選択し、導入するための助言とその適切な実施のためのガイドラインです。

● 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たガイドブックです。

● 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在り方を示した指針です。

中小企業の情報セキュリティ対策ガイドライン第3.1版

- 中小企業の経営者や実務担当者が、情報セキュリティ対策の必要性を理解し、情報を安全に管理するための具体的な手順等を示したガイドラインです。
- ガイドラインは、中小企業の情報セキュリティ対策の考え方や実践方法について、本編 2 部と付録より構成されています。

	構 成	概 要
本 編	第 1 部 経営者編	経営者が知っておくべき事項、および自らの責任で考えなければならない事項について説明しています。
	第 2 部 実践編	情報セキュリティ対策を実践する方向けに、対策の進め方についてステップアップ方式で具体的に説明しています。
付 録	付録 1 情報セキュリティ 5 か条	組織の規模を問わず必ず実行していただきたい重要な対策を 5 か条にまとめ説明しています。
	付録 2 情報セキュリティ基本方針 (サンプル)	組織としての情報セキュリティに対する基本方針書のサンプルです。
	付録 3 5 分でできる！ 情報セキュリティ自社診断	あまり費用をかけることなく実行することで効果がある 25 項目のチェックシートです。
	付録 4 情報セキュリティハンドブック (ひな形)	従業員に対して対策内容を周知するために作成するハンドブックのひな形です。
	付録 5 情報セキュリティ関連規程 (サンプル)	情報セキュリティに関する社内規則を文書化したもののサンプルです。
	付録 6 中小企業のための クラウドサービス安全利用の手引き	クラウドサービスを安全に利用するための手引きです。15 項目のチェックシートが付いています。
	付録 7 リスク分析シート	情報資産、脅威の状況、対策状況をもとに損害を受ける可能性（リスク）の見当をつけることができます。
	付録 8 中小企業のためのセキュリティ インシデント対応の手引き	情報漏えいやシステム停止などのインシデント対応のための手引きです。

参考情報一覧

- 情報セキュリティ対策支援サイト

<https://www.ipa.go.jp/security/sme/isec-portal.html>

- 5分でできる！情報セキュリティ自社診断

<https://www.ipa.go.jp/security/guide/sme/5minutes.html>

- 情報セキュリティ対策ベンチマーク

<https://www.ipa.go.jp/security/sec-tools/benchmark.html>

- 5分でできる！ポイント学習

https://www.ipa.go.jp/security/sec-tools/5mins_point.html

- セキュリティプレゼンター向け資料ダウンロード

<https://www.ipa.go.jp/security/sme/presenter/presenter-materials.html>

- 中小企業の情報セキュリティ対策ガイドライン

<https://www.ipa.go.jp/security/guide/sme/about.html>

- SECURITY ACTION セキュリティ対策自己宣言

<https://www.ipa.go.jp/security/security-action/>

- 映像で知る情報セキュリティ ～映像コンテンツ一覧～

<https://www.ipa.go.jp/security/videos/list.html>

- YouTube「IPAチャンネル」内の 情報セキュリティ普及啓発映像コンテンツ

<https://www.youtube.com/playlist?list=PLF9FCB56776EBCABB>

IPA