今回の業務・情報・権限を整理する

業務・サービス・利用プランごとに作成。印刷・PDF注記用です。足りない欄は複写してください。

委託元・業務責任者・確認担当者：

委託先の契約法人・対象部署・回答責任者／回答日：

対象業務・サービス名・利用プラン・契約期間：

今回行う作業・成果物：

渡す情報の項目・概算件数・頻度：

個人データ・要配慮個人情報・営業秘密等の有無：

渡さずに済む情報・架空データで進められる工程：

付与するアクセス権・操作可能範囲・利用期限：

情報が漏れた場合／業務が止まった場合の影響：

回答希望日・確認日・次回見直し日：

記入済みシートの共有先・保存場所・保管期限：

使い方

委託元が対象を整理 → 使う質問を選択 → 委託先が回答 → 委託元が根拠を確認 → 開始条件を合意。法令が一律に定めた24項目ではなく、実務用のひな形です。

パスワード、APIキー、顧客の実データは記入せず、資料の参照先を残してください。

質問を選び、回答のルールをそろえる

必要な質問を選び、対象外には理由を残します。提出資料は必要な箇所の抜粋・伏字で構いません。

情報の流れ：自社 → 委託先 → 別会社・外部サービス

名称・役割・渡す情報・保存先・アクセス元。法的な扱いは契約・取扱実態で確認

今回使う質問ID／対象外とするIDと理由：

確認に使う既存資料の名称・版・該当箇所／資料を共有する方法：

委託先の回答状態

情報確認：回答済み／不明／対象外。
対策確認：実施済み／一部実施／未実施／不明／対象外。

未実施・不明・対象外を分ける

未実施は行っていないと分かっている状態。不明は確認できていない状態。対象外は今回に適用しない理由を記録します。

具体的な回答と根拠を残す

対象・方法・例外・実施時期を記入し、設定・契約・運用記録と照合できる形にします。根拠は文書名・版・箇所・確認日を記録します。

委託元の確認状態は9ページで記録

未確認／確認済み／追加確認／改善待ち／対象外。回答の受領と根拠確認を分けます。対象外には委託元も理由を確認・記録します。

質問の追加例と判断の着眼点は、記事と編集用CSVにも掲載しています。個人情報や秘密値を含む資料一式の提出は求めず、必要な事実を確認してください。

A 情報と取扱範囲

委託先が記入。例外・対象外の理由も回答欄へ。根拠は参照先を記入し、詳細は別紙を添付できます。

Q01 業務に必要な情報 ［情報確認］

今回の作業に必要な情報の項目と、その利用目的を教えてください。当社が渡す予定の情報から、削除・置換できる項目はありますか。

回答に含めること：必要な項目・工程・件数・頻度／不要な項目・架空データへの置換

☐ 回答済み ☐ 不明 ☐ 対象外

具体的な回答・例外・対象外の理由（続きは別紙）：

根拠・資料の版・箇所／回答者・回答日：

Q02 保存先とアクセスする場所 ［情報確認］

当社の情報は、どのサービス・端末に保存され、どの国・地域からアクセスされますか。

回答に含めること：サービス・プラン・契約法人／保存国・バックアップ先・アクセス元国

☐ 回答済み ☐ 不明 ☐ 対象外

具体的な回答・例外・対象外の理由（続きは別紙）：

根拠・資料の版・箇所／回答者・回答日：

Q03 再委託先と外部サービス ［情報確認］

今回の業務で、当社の情報を扱う別会社・個人事業者・外部サービスはありますか。追加・変更時にはどのように知らせますか。

回答に含めること：名称・役割・渡す情報・取扱場所／監督方法・変更時の通知と協議

☐ 回答済み ☐ 不明 ☐ 対象外

具体的な回答・例外・対象外の理由（続きは別紙）：

根拠・資料の版・箇所／回答者・回答日：

Q04 作業者へのルール周知 ［対策確認］

今回の作業者に、情報の持ち出し・共有・事故連絡のルールをどのように周知していますか。

回答に含めること：開始前の説明・対象者・実施日／外部スタッフ・途中参加者への適用

☐ 実施済み ☐ 一部実施 ☐ 未実施 ☐ 不明 ☐ 対象外

具体的な回答・例外・対象外の理由（続きは別紙）：

根拠・資料の版・箇所／回答者・回答日：

B 人・権限・端末

委託先が記入。例外・対象外の理由も回答欄へ。根拠は参照先を記入し、詳細は別紙を添付できます。

Q05 アカウントと権限 ［対策確認］

誰が当社の情報やシステムにアクセスし、何を操作できますか。個人別のアカウントと業務に必要な権限で管理していますか。

回答に含めること：担当者の役割／閲覧・編集・出力・管理の区分／共用と例外の追跡

☐ 実施済み ☐ 一部実施 ☐ 未実施 ☐ 不明 ☐ 対象外

具体的な回答・例外・対象外の理由（続きは別紙）：

根拠・資料の版・箇所／回答者・回答日：

Q06 多要素認証の適用範囲 ［対策確認］

今回使うアカウントには、多要素認証をどこまで適用していますか。対象外の入口はありますか。

回答に含めること：対象システムとアカウント／強制・任意・例外／復旧と代替策

☐ 実施済み ☐ 一部実施 ☐ 未実施 ☐ 不明 ☐ 対象外

具体的な回答・例外・対象外の理由（続きは別紙）：

根拠・資料の版・箇所／回答者・回答日：

Q07 権限を取り消す手順 ［対策確認］

担当変更・退職・契約終了の際、誰がいつアクセス権を取り消し、完了を確認しますか。

回答に含めること：連絡の起点・実行担当・期限／外部招待・API等の対象／完了記録

☐ 実施済み ☐ 一部実施 ☐ 未実施 ☐ 不明 ☐ 対象外

具体的な回答・例外・対象外の理由（続きは別紙）：

根拠・資料の版・箇所／回答者・回答日：

Q08 作業端末の管理 ［対策確認］

当社の情報を扱う端末について、更新・画面ロック・紛失時の保護をどのように管理していますか。

回答に含めること：会社・私物の区分／更新担当・サポート期間・暗号化／紛失時の対応

☐ 実施済み ☐ 一部実施 ☐ 未実施 ☐ 不明 ☐ 対象外

具体的な回答・例外・対象外の理由（続きは別紙）：

根拠・資料の版・箇所／回答者・回答日：

C 共有・AI・消去

委託先が記入。例外・対象外の理由も回答欄へ。根拠は参照先を記入し、詳細は別紙を添付できます。

Q09 送信と共有の方法 ［対策確認］

情報はどの方法で受け渡し、共有先・有効期限・誤送信をどう確認しますか。

回答に含めること：受渡し方法・共有先・公開リンク・通信保護・期限／誤送信時の手順

☐ 実施済み ☐ 一部実施 ☐ 未実施 ☐ 不明 ☐ 対象外

具体的な回答・例外・対象外の理由（続きは別紙）：

根拠・資料の版・箇所／回答者・回答日：

Q10 手元への保存と紙の扱い ［対策確認］

当社の情報を端末、USB、個人用クラウド、紙へ複製することはありますか。許可範囲と廃棄方法を教えてください。

回答に含めること：持出しの許可と承認／作業場所・保管／回収・削除・廃棄の確認

☐ 実施済み ☐ 一部実施 ☐ 未実施 ☐ 不明 ☐ 対象外

具体的な回答・例外・対象外の理由（続きは別紙）：

根拠・資料の版・箇所／回答者・回答日：

Q11 生成AI等への入力 ［情報確認］

今回の情報を生成AI、文字起こし、翻訳等の外部ツールへ入力する予定はありますか。ある場合は、その条件を教えてください。

回答に含めること：サービス・プラン・入力項目・目的／学習・保存・閲覧・削除・利用合意

☐ 回答済み ☐ 不明 ☐ 対象外

具体的な回答・例外・対象外の理由（続きは別紙）：

根拠・資料の版・箇所／回答者・回答日：

Q12 終了時の返却と消去 ［対策確認］

契約終了時に、何をいつ返却・消去し、どの記録で完了を確認できますか。

回答に含めること：本体・コピー・再委託先・バックアップ／返却・消去期限・記録・例外

☐ 実施済み ☐ 一部実施 ☐ 未実施 ☐ 不明 ☐ 対象外

具体的な回答・例外・対象外の理由（続きは別紙）：

根拠・資料の版・箇所／回答者・回答日：

D システム・記録・復旧

委託先が記入。例外・対象外の理由も回答欄へ。根拠は参照先を記入し、詳細は別紙を添付できます。

Q13 更新と脆弱性への対応 ［対策確認］

今回の対象システムの更新と脆弱性情報の確認を、誰がどの手順で行いますか。

回答に含めること：対象部品・確認担当・緊急判断／適用前の確認／代替策と期限

☐ 実施済み ☐ 一部実施 ☐ 未実施 ☐ 不明 ☐ 対象外

具体的な回答・例外・対象外の理由（続きは別紙）：

根拠・資料の版・箇所／回答者・回答日：

Q14 開発・変更後の検証 ［対策確認］

変更前後にどんな検証を行い、問題があればどのように元へ戻しますか。

回答に含めること：検証環境・データ・確認対象・承認／戻す方法・秘密情報・結果の受渡し

☐ 実施済み ☐ 一部実施 ☐ 未実施 ☐ 不明 ☐ 対象外

具体的な回答・例外・対象外の理由（続きは別紙）：

根拠・資料の版・箇所／回答者・回答日：

Q15 操作記録と異常の確認 ［対策確認］

誰がいつ閲覧・出力・変更したかを、どの範囲まで記録し、異常を確認していますか。

回答に含めること：記録できる範囲・保存期間・閲覧権限／異常の確認・通知・事故時の保全

☐ 実施済み ☐ 一部実施 ☐ 未実施 ☐ 不明 ☐ 対象外

具体的な回答・例外・対象外の理由（続きは別紙）：

根拠・資料の版・箇所／回答者・回答日：

Q16 バックアップと復旧 ［対策確認］

消失や障害に備えたバックアップについて、戻せる範囲と最近の復旧確認結果を教えてください。

回答に含めること：対象・頻度・保護／最近の復旧確認・戻せる範囲・時間／担当と費用

☐ 実施済み ☐ 一部実施 ☐ 未実施 ☐ 不明 ☐ 対象外

具体的な回答・例外・対象外の理由（続きは別紙）：

根拠・資料の版・箇所／回答者・回答日：

E 事故連絡・継続確認

委託先が記入。例外・対象外の理由も回答欄へ。根拠は参照先を記入し、詳細は別紙を添付できます。

Q17 緊急連絡先 ［情報確認］

事故や不正アクセスの疑いがある場合、当社から誰にどう連絡し、つながらない場合はどこへ連絡できますか。

回答に含めること：双方の連絡先・受付時間・夜間休日・代替先／更新担当

☐ 回答済み ☐ 不明 ☐ 対象外

具体的な回答・例外・対象外の理由（続きは別紙）：

根拠・資料の版・箇所／回答者・回答日：

Q18 疑いの段階での第一報 ［対策確認］

当社情報の漏えい等や不正アクセスの疑いを把握したとき、どの段階で、何を、いつまでに第一報として知らせますか。

回答に含めること：通知の起点・合意期限／事実と不明点・暫定対応・次報／再委託先の連絡

☐ 実施済み ☐ 一部実施 ☐ 未実施 ☐ 不明 ☐ 対象外

具体的な回答・例外・対象外の理由（続きは別紙）：

根拠・資料の版・箇所／回答者・回答日：

Q19 調査と情報提供への協力 ［情報確認］

事故時の証拠保全、影響調査、委託元への説明は、誰がどこまで担当しますか。

回答に含めること：保全・影響調査・再委託先との連携／提供資料・報告と本人通知の役割

☐ 回答済み ☐ 不明 ☐ 対象外

具体的な回答・例外・対象外の理由（続きは別紙）：

根拠・資料の版・箇所／回答者・回答日：

Q20 変更時と継続中の再確認 ［対策確認］

担当者・保管先・再委託先・利用ツール・業務内容が変わるとき、どの変更をいつ通知し、対策を見直しますか。

回答に含めること：通知対象・事前確認が必要な変更／定期確認の周期・前回日・次回日

☐ 実施済み ☐ 一部実施 ☐ 未実施 ☐ 不明 ☐ 対象外

具体的な回答・例外・対象外の理由（続きは別紙）：

根拠・資料の版・箇所／回答者・回答日：

F 役割・契約・確認資料

委託先が記入。例外・対象外の理由も回答欄へ。根拠は参照先を記入し、詳細は別紙を添付できます。

Q21 双方の担当範囲 ［情報確認］

当社と貴社のどちらが、設定・アカウント管理・更新・バックアップ等を担当するか、今回の業務で該当する範囲を確認できますか。

回答に含めること：作業別の実施者・承認者／クラウド側の担当／契約範囲・追加費用

☐ 回答済み ☐ 不明 ☐ 対象外

具体的な回答・例外・対象外の理由（続きは別紙）：

根拠・資料の版・箇所／回答者・回答日：

Q22 利用目的と守秘の合意 ［情報確認］

今回の情報を使える目的と、守秘・目的外利用の制限は、どの契約・条項に定めますか。

回答に含めること：対象情報と処理／二次利用・AI学習等／外部スタッフ／規約との整合

☐ 回答済み ☐ 不明 ☐ 対象外

具体的な回答・例外・対象外の理由（続きは別紙）：

根拠・資料の版・箇所／回答者・回答日：

Q23 認証・監査等の確認資料 ［情報確認］

今回の業務の対策を確認できる認証・監査報告・運用記録等はありますか。確認できる範囲と日付を教えてください。

回答に含めること：資料名・主体・対象範囲・期間／登録番号と有効性／代替確認の方法

☐ 回答済み ☐ 不明 ☐ 対象外

具体的な回答・例外・対象外の理由（続きは別紙）：

根拠・資料の版・箇所／回答者・回答日：

Q24 追加確認と改善の進め方 ［情報確認］

回答に不明点や未対応が残った場合、どの方法で追加確認し、誰がいつまでに対応しますか。

回答に含めること：確認窓口・方法・費用・範囲／秘密情報／改善担当・期限・完了の根拠

☐ 回答済み ☐ 不明 ☐ 対象外

具体的な回答・例外・対象外の理由（続きは別紙）：

根拠・資料の版・箇所／回答者・回答日：

委託元が、根拠と残る課題を確認する

質問IDごとに記録します。記録が足りない場合は、このページを複写するかCSVを使ってください。

対象業務・委託先／質問ID：

☐ 未確認　☐ 確認済み　☐ 追加確認　☐ 改善待ち　☐ 対象外

確認した根拠・資料の版・箇所／確認担当者・確認日：

残る課題・追加質問／対象外の理由：

暫定措置・利用条件／対応担当者・期限：

再確認日・確認方法／結果と参照先：

対象業務・委託先／質問ID：

☐ 未確認　☐ 確認済み　☐ 追加確認　☐ 改善待ち　☐ 対象外

確認した根拠・資料の版・箇所／確認担当者・確認日：

残る課題・追加質問／対象外の理由：

暫定措置・利用条件／対応担当者・期限：

再確認日・確認方法／結果と参照先：

「回答済み」は「確認済み」と別の状態です。資料が出せない場合も、伏字・閲覧限定・要約等で必要な事実を確認できるか検討します。

開始判断と条件を合意する

必要な条件を満たした範囲で判断。法令上必要な条件を、条件付きの合意で省略することはできません。

☐ 開始可　☐ 条件付きで開始

☐ 確認・改善まで保留　☐ 見送り

対象業務・委託先／判断日：

判断した理由・確認した資料／残る課題：

開始できる情報・権限・作業／開始を保留する範囲：

暫定措置・利用条件／実行担当・期限：

契約・別紙・仕様書へ反映する事項／文書の版・条項：

利用目的、対策・役割、外部ツール、事故連絡、追加確認、返却・消去

承認者／双方の合意担当・合意日／記録の参照先：

再確認日・確認方法／未達の場合の停止・制限・移行の手順：

この4区分は実務上の整理です。点数や認証の有無だけで会社全体の安全性を判定しません。

継続中の変更と、終了時の処理を記録する

変更があれば定期確認を待たずに確認。終了時は、アクセス取消と保存データの処理を分けます。

対象業務・委託先／記録担当・記録日：

変更点・確認する質問ID／変更前に合意する条件：

情報、権限、作業者、保存先、再委託先、AI等、契約・連絡先の変更

確認結果と根拠／対応担当・期限／次回確認日：

終了時の確認記録（状態・実施日・担当・根拠の参照先）

返却データ：対象・形式・受領・内容確認

アクセス：アカウント・招待・API・外部連携・共有リンクの取消

保存データ：通常データ・端末コピー・紙の消去／再委託先の処理

残る情報：バックアップ・法令保存の理由／利用制限・消去期限

未完了の処理：担当・期限・完了確認方法／再確認日

「削除済み」の一言で終えず、何をいつ処理し、何が残るかを記録します。

出典・資料の使い方

2026年10月16日確認。質問文・記入欄はレイズ作成。制度・法令の説明は一次資料を参照しています。

S01 個人情報保護委員会：通則編 3-4-4等

S02 IPA：中小企業の情報セキュリティ対策ガイドライン 第4.0版

S03 IPA：クラウドサービス安全利用の手引き

S04 個人情報保護委員会：Q7-53（クラウドと委託）

S05 個人情報保護委員会：Q7-54（利用者の安全管理）

S06 個人情報保護委員会：Q12-3（外国サーバー）

S07 個人情報保護委員会：Q12-4（外国事業者）

S08 個人情報保護委員会：生成AIサービスの利用に関する注意喚起

S09 ISMS-AC：ISMS適合性評価制度

S10 JIPDEC：プライバシーマークとは

S11 IPA：セキュリティインシデント対応の手引き

S12 IPA：サイバーセキュリティ経営ガイドライン プラクティス集

S13 ISMS-AC：認証取得組織検索

このシートを使うとき

業務に応じて質問を選び、必要な項目を追加してください。回答だけで安全性を保証するものではありません。医療・金融・マイナンバー等では、対象分野のルールに沿って確認を加えます。

実在する委託先の回答は未記入です。記入後は共有先と保管場所を決めて管理してください。PDFは印刷・注記用です。入力フォームはありません。

自社サイトの公開情報から、現状を確認する

無料のAIセキュリティ検査：公開ページを最大10ページ・40項目、約3分で確認。委託先内部の運用や契約は、この質問シート等で別途確認します。

無料のAIセキュリティ検査を始める →

確認の進め方を相談する →