Salesforce ガバナンス・アクセス権限管理

Salesforce 内のデータの安全性・機密性を保持しつつ、各ユーザーが業務に必要なデータへ適切にアクセスできる環境を維持・管理するための運用ルールを定めるものです。

【 基本原則 】

■ 最小権限の原則:
ユーザーには業務上必要な最小限の権限のみを付与します。

■ 最小限のプロファイル運用:
プロファイルは組織共通の基本設定と最小限のオブジェクトアクセス制御にとどめ、
個別権限は「権限セット」で付与します。

■ 責任の分離:
管理者権限（システム管理者）の付与対象者を厳格に制限・監視します。

アクセス権限の階層構造

Salesforce の権限管理は、大きく分けて以下の 2 つで構成されます。

■ システム/オブジェクト機能への権限
【機能・項目権限】（何ができるか）
├── プロファイル（基盤となる最小権限・システム設定）
└── 権限セット / 権限セットグループ（個別・追加権限の付与）

■ データの閲覧・編集権限（レコード権限）
【レコード権限】（どのデータが見えるか）
├── 組織の共有設定（最も厳しいアクセス基準を適用）
├── ロール階層（上司・上位役職への自動権限昇格）
├── 共有ルール（条件・所有者に基づく自動共有）
└── 手動共有（ユーザー判断による例外的な一時共有）

各権限要素の設定ガイドライン

1. プロファイル設定

権限管理の全体像から見ると、プロファイルはユーザーに必ず 1 つ割り当てられる「ベース（基盤）」の役割を果たします。

① システムレベルの制御（認証・セキュリティルール）
ユーザーごとに個別に設定するのではなく、グループ単位で共通化したいログイン周りのルールを設定します。

- ログイン制限: ログインを許可する IP アドレス範囲（例：社内ネットワークのみ）やログイン時間帯
- パスワードポリシー: パスワードの有効期限、文字数、複雑さ
- セッション設定: タイムアウトまでの時間
- システム権限: 「レポートの書き出し」「全データの参照」「API の利用」などのシステム機能の利用可否

② オブジェクト・項目レベルのアクセス制御

- オブジェクト権限（CRUD）：各オブジェクト（取引先、商談など）に対する「参照(Read)」「作成（Create)」「編集（Edit)」「削除（Delete)」の基本権限
- 項目レベルセキュリティ（FLS: Field-Level Security）：オブジェクト内の特定項目（例：見込み客の「電話番号」や商談の「粗利益」など）を「表示する / 隠す / 参照のみにする」制御
- アプリ・ページレイアウト設定: ログイン時に表示されるデフォルトのアプリケーションや、画面のレイアウト（どの入力項目をどの配置で見せるか）

ユーザー1 人につき、プロファイルは「必ず 1 つ」
プロファイルを未設定にすることはできません。
また、2 つ以上のプロファイルを同時に割り当てることもできません。

権限を「削る」ことはできるが、プロファイル同士を合算することはできない
ユーザーごとに異なる権限を追加したい場合は、プロファイルを増やすのではなく
「権限セット（Permission Set)」を併用します。

【推奨される権限構成】

[ユーザー]
　　|
　　├── ① プロファイル（全員共通の最小権限 ＋ ログイン制限など）
　　|
　　├── ② 権限セット A（例：営業用オブジェクトの編集権限）
　　└── ③ 権限セット B（例：インポート・エクスポート実行権限）

なぜプロファイルを絞るべきなのか？

- 保守が楽になる: プロファイルが 50 個あると、新しいカスタムオブジェクトを作った際に 50 個すべてで権限チェックを行う必要があり、設定漏れや運用の形骸化につながります。
- 柔軟な運用ができる: 「営業部だけど、一時的にマーケティングのレポート作成権限も渡したい」という場合、プロファイルを変更するのではなく、該当の権限セットを 1 つ付与するだけで済みます。

設定や見直しを行う際は、以下の点に注意してください。

[　] 標準プロファイルをそのまま使っていないか？
　　Salesforce 標準のプロファイル（Standard User など）は権限の編集ができません。必ず一度クローン（複製）してカスタムプロファイルを作成してから割り当ててください。

[　] 「すべてのデータの参照」「すべてのデータの編集」にチェックが入っていないか？
　　このチェックが入っていると、組織の共有設定で「非公開」にしていても、組織内の全データが見え・変更でき・消せてしまいます。システム管理者プロファイル以外では絶対にオンにしないでください。

[　] 不要な削除（Delete）権限を与えていないか？
　　一般ユーザーには「参照・作成・編集」のみを許可し、「削除」権限は管理職や管理者のみに制限するのが安全です。

2. 権限セット / 権限セットグループ

権限セット（Permission Set）は、プロファイルで設定されたベース権限に対して、「ユーザー単位や役割単位で追加の権限を足し算（付与）する」ための機能です。

① 権限セットの基本概念：「引き算」ではなく「足し算」

プロファイルと権限セットの最も大きな違いは、権限の与え方にあります。

- プロファイル（ベース）：
  ユーザーが持つ最小限の権限（土台）。権限を「剥奪（禁止）」することはできますが、1 人に 1 つしか割り当てられません。
- 権限セット（拡張）：
  プロファイルで許可されていない操作を「追加で許可」します。1 人のユーザーに複数の権限セットを自由に重ねて割り当てることができます。

[一般ユーザー用プロファイル]（最小限の参照権限・ログイン制限など）
＋
[権限セット：商談編集]（営業担当者に付与）
＋
[権限セット：エクスポート許可]（特定のリーダーだけに付与）

⚠ 重要ルール: 権限セットで「このオブジェクトを見ちゃダメ」「この項目を非表示にする」というアクセス制限はできません。あくまで「できることを増やす」ツールです。

② 権限セットで設定できる主な項目（プロファイルとほぼ同様の設定項目を追加付与できます。）

- オブジェクト権限: 特定のオブジェクトに対する参照・作成・編集・削除権限の追加
- 項目レベルセキュリティ: プロファイルでは非表示になっている特定項目の表示・編集権限
- アプリ・タブのアクセス: 特定のアプリケーションやタブへのアクセス許可
- システム権限 / ユーザー権限: レポートのエクスポート、データのインポート、ダッシュボードの管理などの機能利用権限

権限セットを活用する 3 つのメリット

① プロファイルの乱立を防げる（保守性の向上）

「営業部の A さんだけレポートをエクスポートさせたい」「マーケ部の B さんにだけ特定のカスタムオブジェクトを触らせたい」といった要望のたびにプロファイルを作っていると、あっという間に数十個のプロファイルが乱立して管理不能になります。
基本プロファイルは 1〜2 個に絞り、個別の要望は権限セットで対応することで、管理が非常にシンプルになります。

② 期間限定・プロジェクト単位の柔軟な運用が可能

「今月だけデータ移行作業を手伝ってもらうために一時的に権限を増やしたい」という場合、権限セットを使えば以下のような運用が可能です。
有効期限付き割り当て: 権限セットの割り当て時に「有効期限（例: 30 日後に自動解除）」を設定することもできます。

③ 権限セットグループによる整理

複数の権限セットを 1 つの「グループ」としてまとめることができます。
例えば、「営業担当者グループ」という箱を作り、その中に「商談編集」「名刺データ参照」「見積作成」の 3 つの権限セットを入れておくことで、新入社員にはそのグループを 1 つ割り当てるだけで設定が完了します。

【 プロファイルと権限セットの使い分けまとめ 】

項目	プロファイル	権限セット
割り当て数	1 ユーザーにつき 1 つのみ	1 ユーザーに 複数割り当て可能
主な役割	土台・認証ルール (ログイン IP 制限、パスワード設定、 デフォルトアプリ)	業務機能の追加 (特定のオブジェクト編集、 エクスポート権限など)
権限の制御	権限の許可・制限（基本設定）	権限の追加許可のみ（足し算）
設計の 考え方	最小限の権限に抑える	業務の「役割」や「機能」単位で細かく作成する

① 機能単位で小さく作る
「商談管理権限」「キャンペーン管理権限」「データエクスポート権限」のように、
機能ごとに単機能の権限セットを作っておくと、後から組み合わせが効きやすくなります。

② 命名ルールを統一する
一覧を見ただけで何が付与されるか分かる命名にしましょう。
- [オブジェクト名]_[権限内容]（例: Opportunity_Edit_PS）
- [業務役割名]（例: Sales_Leader_PSG）
-

③ 割り当て解除（クリーンアップ）の定期確認
部署異動やプロジェクト終了時に不要になった権限セットが残りっぱなしにならないよう、定期的に割り当て状況を監査します。

3. レコードのアクセス権制御（セキュリティモデル）

プロファイルや権限セットが「そもそも商談オブジェクトにアクセスできるか（機能の権限）」を決めるのに対し、セキュリティモデルは「商談オブジェクトの中の『どの商談データ』まで見せてよいか（データの権限）」を制御します。
Salesforce のデータ制御は、「最初は最も厳しく絞り込み、後から段階的にアクセス権を解放する」という原則で設計されています。

【アクセス権の広がり方（下から上へ解放）】

[4. 手動共有]
▲ 例外的な一時共有
[3. 共有ルール]
▲ 部門間や特定条件での自動共有
[2. ロール階層]
▲ 役職（上司・上位組織）への自動共有
==========
[1. 組織の共有設定] ← ★土台（最も厳しいアクセス基準）

① 組織の共有設定

データセキュリティの「一番下の土台（ベースライン）」となる設定です。全ユーザーに対するデフォルトのアクセス範囲をオブジェクトごとに設定します。

- 役割: 組織内で最も厳しいデータアクセス基準を定義する。
- 基本方針（ベストプラクティス）:
  原則として 「非公開」 または 「参照のみ」 に設定します。
  最初から「参照・編集可能」にすると、全ユーザーが他人のデータを自由に編集できてしまい、後から権限を絞ることができなくなります。
- 設定の選び方:
  非公開:「自分（または同僚の一部）のデータしか見せたくない」場合
  （例: 個人別の商談データ、個人の活動履歴など）。
  参照のみ:「全社で情報は共有・閲覧したいが、他人のデータは勝手に書き換えさせたくない」場合（例: 取引先マスター、商品カタログなど）。

② ロール階層

会社の「組織図」や「役職階層」に基づき、上位者が下位者の所有するレコードへ自動的にアクセスできるようにする仕組みです。

- 役割: 上司が部下のデータを自動的に閲覧・編集できるようにする。
- 仕組み:
  組織の共有設定で「非公開」に設定されていても、ロール階層で下位にあるユーザーが所有するレコードは、階層の上位にいるユーザーへ自動的にアクセス権限が昇格されます。
- 注意点（プロファイルとの違い）:
  ・プロファイルは「職種や権限」を表すもの（例: 営業担当、経理担当）。
  ・ロールは「データの見え方の階層」を表すもの
  （例: 東日本営業部長 > 東京営業課長 > 営業メンバー）。
  ・組織変更や人事異動が多い企業では、ロール階層を細かく作りすぎず、アクセス権の共有に必要なレベルに留めるのが保守のコツです。

③ 共有ルール

ロール階層だけではカバーできない「部門をまたぐ共有」や「特定の条件に一致するデータの共有」を自動化する仕組みです。

- 役割: 組織の共有設定で「非公開」または「参照のみ」にしているデータに対し、
  特定のグループへ例外的にアクセス権を開放する。
- 主な共有ルールの種類:
  所有者に基づく共有ルール:
  「『東日本営業部』が所有するレコードを、『西日本営業部』にも参照許可する」など、レコードの所有者のロールやグループを基準に共有。
  条件に基づく共有ルール:
  「『金額』が 1,000 万円以上の商談レコードは、所有者に関わらず『役員グループ』に参照許可する」など、フィールドの値（条件）を基準に共有。
- アクセスレベル: 共有相手に対して「参照のみ」か「参照/編集可能」かを選択できます。

④ 手動共有

組織の共有設定・ロール・共有ルールで自動化できない「一時的・例外的なデータ共有」を行うための機能です。

- 概要: レコードの所有者（または管理者）が、レコード画面上の「共有」ボタンから手動で特定のユーザーやグループにアクセス権を付与します。
- 活用例: 「普段は別プロジェクトのメンバーだが、この案件だけ一時的に外部アドバイザーの A さんに閲覧させたい」といった場合に使用します。

新しいオブジェクトを作成・導入する際は、以下の順番で設計を進めてください。

1. 組織の共有設定を決める:
   「一番厳しい状態でどこまで開くか？」（全社非公開にするか、参照だけ許可するか）
2. ロール階層を確認する:
   「上司や上位役職者は部下のデータを見る必要があるか？」
3. 共有ルールを設計する:
   「他部署や特定チームへの自動共有ルールはあるか？」
4. 個別ケースに対応する:
   「どうしても自動化できない例外は手動共有で対応する」

ユーザーアカウント管理プロセス

ユーザーアカウントのライフサイクル（着任・異動・休職/退職）におけるアクセス権限の適切な付与・変更・剥奪は、セキュリティの維持およびライセンスコスト最適化の観点から極めて重要です。

申請・承認プロセスの厳守
すべてのアカウント操作（作成・権限変更・無効化）は、指定の「ユーザー管理申請票」の事前承認を経てから実施します。口頭やメールでの直接依頼による作業は原則禁止とします。

アカウントの共有禁止
1 ユーザー＝1 アカウントを徹底します。監査上の理由および個別権限管理のため、複数人でのログイン情報の共有（共有アカウント）は禁止です。

無効化の原則（削除不可）
Salesforce では過去の取引履歴や活動履歴の整合性を保つため、ユーザーレコードの削除はできません。不要になったアカウントは「無効化」で対応します。

■アカウント運用の前提ルール■

- 公開グループ / キューの変更管理: 公開グループやキューへのメンバー追加は、共有ルールを経由してデータの参照範囲が一気に広がるセキュリティリスクがあります。ユーザーの作成・異動時と同様、必ず指定の申請・承認フローを経由して実施してください。
- 多要素認証（MFA）の初期設定および端末紛失時の復旧手順については、別途定義されている『多要素認証設定マニュアル』を参照してください。

【 入社・異動・退職時の運用フロー 】

タイミング	実施事項	担当者
新規着任 （入社・配属）	① 申請の受付 （着任日・氏名・メールアドレス・所属部署・役職 等の確認）	人事/申請者
	② 指定の申請書に基づきユーザー作成	システム管理者
	③ ベース権限設定：プロファイルを付与 部署共通の「最小権限カスタムプロファイルを設定」	システム管理者
	④ 個別権限の付与：権限セット・権限セットグループを割り当て （例: 営業機能、ダッシュボード作成機能など）	システム管理者
	⑤ 組織図上の所属位置（上司の下位）にロールを設定	システム管理者
	⑥ 通知・初期設定：新規ユーザー通知メールを送信し、初期ログインおよび MFA（多要素認証）の設定を完了させる。	管理者/ユーザー
部署異動	① 申請受付（異動発令日・新部署・新役職・業務範囲 等の確認）	人事/申請者
	② 異動日に合わせて旧部署の権限セット・ロールを解除	システム管理者
	③ 新部署用の権限セット・ロールを設定	システム管理者
	④ 必要に応じて新部署の公開グループ/キューに追加	システム管理者
	⑤ 所有データの移行：旧部署で所有していた未完了商談・ケース・取引先などの所有者を後任者または引き継ぎ先に一括変更	異動元上司
退職・長期休職	① 退職当日に該当ユーザーの「無効化」を実施	システム管理者
	② 所有レコードの引き継ぎ・割り当て変更	システム管理者
	③ スケジュール済みジョブやダッシュボードの実行ユーザー変更	管理者/後任者
	⚠ **システム管理者のライセンス上限維持やセキュリティ確保のため、 退職者のアカウントは即日無効化してください。**	

● 「無効化」ボタンがエラーで押せない場合（凍結機能の活用）

該当ユーザーがプロセス自動化の実行ユーザーやデフォルトのケース所有者などに設定されている場合、そのままでは無効化できないことがあります。

対処法:

1. 一刻を争う場合は、まずユーザー詳細画面で 「凍結」 ボタンを押します。
   （ライセンスは消費されたままですが、ユーザーのログインを即座に遮断できます）。
2. その後、該当ユーザーが関連している設定（参照）を外してから 「無効化」 を完了させます。

● 退職者からの所有権一括変更（一括転送）

Salesforce 標準機能の「レコード所有権の括変更」や「データローダ」を使用し、退職者の所有レコードを漏れなく新担当者へ引き継ぎます。

ガバナンス・モニタリング体制

1. システム管理者権限の管理
   - 付与基準: システム管理者権限は、システムの運用保守・設計を行う担当者（主・副の最低 2 名〜数名程度）に限定します。
   - 特権アクセスの監視: 「すべてのデータの参照」「すべてのデータの編集」権限を割り当てる場合は事前承認を必須とします。
   - 代理ログインの利用ルール: 管理者が障害調査等で他ユーザーとしてログイン（代理アクセス）を行う場合は、対象ユーザーへの事前了承または変更申請チケットの作成を必須とします。

2. 定期監査の実施（四半期 / 半年ごと）
   - ユーザーアクセス監査:
     最終ログイン日時を確認し、長期間未ログインのユーザーアカウントを一時無効化。
     現在の所属・役職とプロファイル・権限セット・ロールの整合性をチェック。
   - 監査トラップの確認:
     「設定変更履歴」を確認し、重要な権限変更（プロファイル変更・特権付与など）が正しく申請・承認されているか確認。
   - セキュリティ 状態チェックの実行:
     Salesforce 設定からセキュリティ->「状態チェック」を定期実行し、セキュリティスコアを 80%以上に維持。

チェンジマネジメント（変更管理ルール）

本番環境のデータおよび権限構成を安全に維持するため、設定変更は以下のステップで行います。

1. サンドボックス（Sandbox）環境での検証
   権限セットや共有ルールの追加・変更は、必ず Sandbox 環境で動作検証を行います。
   テスト用一般ユーザーでログイン（ユーザー名変更・ログイン機能）し、意図しないデータが見えていないか確認します。

2. 承認プロセスの実施
   権限追加・共有設定の変更依頼は、システム責任者の承認を得た変更申請書を必須とします。
   （変更申請書のサンプルは次頁）

3. 本番環境への反映
   Sandbox 組織から「送信変更セット」を作成し、本番環境「受信変更セット」からリリースし、設定変更履歴を残します。

Salesforce ユーザーアカウント発行・変更・無効化　申請書

システム管理者	部門承認	申請者

申　請　日 ： 20　　年　　月　　日
適用希望日 ： 20　　年　　月　　日（　　時から適用）

◆ 対 象 者 基 本 情 報 ◆			
氏名		社員番号	
メールアドレス			
現所属（異動前）	部署： 役職：	新所属（異動後）	部署： 役職：

◆ 申 請 内 容 詳 細 ◆	
□ 新規着任	■業務担当・役割：
□ 部署異動	■旧権限の取扱い：□ 旧所属の全権限セット・ロールを即時解除 ■引継ぎ・所有権移行： 取引先 引継ぎ担当者：【　　】 商　談 引継ぎ担当者：【　　】
□ 退職・長期休職	■引継ぎ・所有権移行： 取引先 引継ぎ担当者：【　　】 商　談 引継ぎ担当者：【　　】
権限セット/グループ (希望アクセス範囲)	□営業担当　□営業リーダー・承認者　□クラーク担当　□管理マネージャー □レポート・ダッシュボード使用 □グループ・キュー追加：【　　】

※　退職・異動に伴うアカウント処理はセキュリティ保護のため即日実施されます。

※　新規着任（アカウント新規作成）時の多要素認証（MFA）の設定および端末紛失時の再設定手順については『多要素認証設定マニュアル』を参照してください。

◆ シ ス テ ム 管 理 者　処 理 欄 ◆			
設定ユーザー名			
付与プロファイル		設定ロール	
割り当て権限セット			
作業完了日	20　　年　　月　　日	作業担当者	