共有モデルの仕組み

Salesforce, Summer '16

@salesforcedocs

最終更新日: 2016/04/22

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 2000–2016 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

共有モデルの仕組み 1
はじめに 1
データアクセスの種別 1
顧客の実装シナリオ 8
考慮事項 10
トラブルシューティング 12

共有モデルの仕組み

はじめに

Salesforce共有モデルは、安全なアプリケーションデータアクセスを組織で提供するうえで不可欠な要素です。このため、現在および将来のアクセス要件を満たすように共有モデルを正しく構築することが重要です。このドキュメントでは、データアクセシビリティコンポーネント、共有モデルの使用事例、顧客の実際の共有ソリューションを確認し、トラブルシューティングに関する一部のガイドラインについて説明します。

対象利用者および前提条件

このドキュメントは、熟練したシステム管理者およびアーキテクトを対象にしています。概念を理解するには、Salesforceのセキュリティと共有モデルに関する知識が必要です。このガイドを読み進める前に、以下の資料を参照することをお勧めします。

- *Security Implementation Guide (セキュリティ実装ガイド)*
- Force.com Platform Fundamentals (Force.com プラットフォームの基本)
- http://wiki.developerforce.com/page/An_Overview_of_Force.com_Security

対象外のデータアクセス

データアクセシビリティアーキテクチャでは、次のトピックについては説明していません。

- フォルダアクセス
- コンテンツアクセス
- Chatterアクセス
- 知識ベースアクセス
- アイデア、質問/回答アクセス
- Salesforce2Salesforce
- モバイルデータアクセシビリティ

データアクセスの種別

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。ほとんどのアプリケーションの場合と同様に、データアクセスの設定はユーザから開始します。アプリケーションでは、アクセス権限を付与する前にどのようなユーザであるかを識別する必要があります。Salesforceには異なる種別のユーザが含まれ、その種別によってアクセスレベルが異なる場合があります。ここでは、すべてのライセンスの種類のすべての属性について説明するのではなく、データアクセスに大幅な影響を与える属性に焦点を絞ります。レコード所有者と

フルアクセスは同じ意味を持ち、代替可能であり、レコードに対する最大限のアクセス権限をユーザに付与します。

ライセンス

フル共有モデル使用ユーザ/ライセンス
: Salesforce のほとんどの種類の標準ライセンスでは、共有モデルコンポーネントが最大限に活用されます。ライセンスによっては、モジュールや一部のオブジェクトにアクセスできない場合があります。たとえば、Force.com Free Edition では CRM オブジェクトにアクセスできません。その場合でも、共有エンティティおよび機能は存在するため、モジュールが有効になれば使用できます。

大規模カスタマーポータルライセンス
: 大規模カスタマーポータル (HVPU) ライセンスユーザ (コミュニティおよび Service Cloud ライセンスユーザを含む)は、共有モデルを使用しません。HVPU ライセンスには、ポータルユーザ(ライセンス保有者)と取引先検索や取引先責任者検索のデータ間で外部キーの一致によって動作する、独自の共有モデルがあります。HVPU ライセンスはカスタマーポータル専用であり、パートナーポータルでは使用しません。

Chatter Free ライセンス
: Chatter Free ライセンスは、標準の共有モデルに準拠していません。Chatter Free はコラボレーション専用のライセンスであり、Chatter、プロファイル、人、グループ、ファイル、Chatter デスクトップ、および Salesforce1 アプリケーションアクセスの各機能があります。このライセンスでは CRM レコード(標準オブジェクトまたはカスタムオブジェクト) およびコンテンツ機能にアクセスできないため、共有はありません。

このドキュメントの以降の部分では、フル共有モデルを利用する Salesforce ユーザ種別であることを前提としています。使用できる各ライセンスの種類についての詳細は、「ユーザライセンスの概要」を参照してください。

コンポーネント

プロファイルと権限セット
: プロファイルと権限セットはオブジェクトレベルのセキュリティを提供するものであり、ユーザが表示できるデータ型や、ユーザがレコードを編集、作成、削除できるかどうかを決定します。「すべての参照」および「すべての編集」権限を使用すると、各オブジェクトの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迅速にアクセス権を許可できます。「すべてのデータの参照」や「すべてのデータの編集」管理権限の代わりにこれらの権限を使用することがよくあります。

  また、プロファイルと権限セットは項目レベルのセキュリティも制御し、これによりすべてのオブジェクトでユーザがアクセスできる項目が決まります。たとえば、オブジェクトに 20 個の項目が含まれていても、そのうちの 5 個はユーザに表示されないように項目レベルのセキュリティを設定できます。

レコード所有者とキュー
: すべてのレコードは単一ユーザまたはキューが所有します。所有者には、所有者のプロファイルの [オブジェクト設定] に基づいて、レコードに対するアクセス権があります。たとえば、所有者のプロファイルに、あるオブジェクトに対する［作成］権限と［参照］権限があり、［編集］権限および［削除］権限がない場合、所有者はそのオブジェクトに対してレコードを作成し、その新しいレコードを参照できますが、レコードを編集または削除することはできません。階層(ロールまたはテリトリー)内で上位にあるユーザは、標準オブジェクトに対して下位ユーザと同じデータアクセス権を継承します。マネージャは、部下と同じ

アクセス権を取得します。部下に「参照のみ」アクセス権しかない場合は、マネージャもそのアクセス権になります。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。

キューは、レコードに優先度を付けたり、レコードを配布したり、ワークロードを共有するチームにレコードを割り当てたりするのに役立ちます。キューへはリストビューからアクセスでき、キューメンバーはキュー内の任意のレコードの所有権を持つことができます。キューは、ケース、リード、注文、カスタムオブジェクト、サービス契約、ナレッジ記事バージョンに使用できます。

単一ユーザが所有するレコードが 10,000 件を超える場合は、次のようにすることをお勧めします。

- 所有者のユーザレコードで、ロール階層内のロールを保持しない。
- 所有者のユーザレコードでロールを保持する必要がある場合は、ロール階層の自分のブランチで階層の最上位にロールを配置する。

組織の共有設定

組織の共有設定では、お互い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許可します。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あるとします。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の参照はできますが、レコード所有者であるか、追加の権限が付与されていない限り、これらのレコードの編集はできません。組織の共有設定は、レコードへのユーザアクセスを制限する唯一の方法です。

組織の共有設定をある設定から別の設定に変更する (*private* から *controlled by parent* に変更してから、*private* に戻すなど) ことはできますが、このような変更は共有再適用を必要とし、データ量によっては処理に長時間かかることがあります。

カスタムオブジェクトの場合にのみ、階層を使用したアクセス許可設定がオフになっている (デフォルトではオン) 場合はその設定を使用して、マネージャがアクセス権を継承しないようにします。この設定は、組織の共有設定に含まれています。

ロール階層

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、マネージャは、組織の共有設定に関係なく従業員と同じデータに確実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。

組織には 500 個のロールを設定できますが、Salesforce ではこの数値を増加できます。非ポータルロールは 25,000、ポータルロールは 100,000 以内に抑えることをお勧めします。

ロール階層は、階層内のブランチで 10 レベル以内に抑えることをお勧めします。

ユーザのロールを変更すると、関連する共有ルールが評価され、必要に応じてアクセス権が修正されます。同じロールに含まれる同僚には、互いのデータに対するアクセス権は保証されません。

ロール階層をモデル化するには、まず組織の構成を理解する必要があります。通常、組織の構成を理解するには、最上位から開始して、マネージャの範囲を把握します。CEO は会社全体を統括します。CEO の下には通常、部署 (営業やサポート) または地域 (EMEA、APAC) 別に分類できる直属の部下がいます。その下には、さらに分類できる部下がいます。これは HR 組織図に非常に似ていますが、データアクセスをモデル化する場合は、HR 組織体系を考慮しながらデータアクセシビリティに焦点を絞ります。

フロート表示は、階層に関して常に注意を要する部分です。自分のブランチにフロート表示が存在する場合、必要なアクセス権を取得するために、共有ルール、チーム、またはテリトリーの管理が必要です。フロート表示が階層内に組み込まれていると、レポートに影響が及ぶ可能性があります。

ロール階層は共有モデル全体の基盤であるため、時間をかけて設定することが重要です。

ロール階層の使用事例
管理アクセス – 部下が表示および実行できるすべてのものをマネージャが表示および実行できる機能。
管理レポート – 階層内で上位にあるユーザが下位ユーザより多くのデータを表示できるようにするための、階層形式における上位ロールへのレポート機能。
組織のブランチ間の分離–異なる部署では互いのデータを表示する必要はありません。階層内で別のブランチを定義できると、部署内の表示を分離しながら、その部署より上位にある管理レベルでは引き続き表示できます。
ロール内での分離–多くの組織またはアプリケーションでは、同じロールのすべてのユーザが、必ずしも互いのデータを表示する必要はありません。階層ロールで「リーフ」ノードを定義できると、すべてのデータを基本的には非公開にしながら、親ロールではすべてのデータを引き続き表示できます。

公開グループ

公開グループ (Chatter グループではない) は、全員が共通の機能を持つ個々のユーザ、ロール、テリトリーなどの集まりです。公開グループは、次のもので構成できます。

- ユーザ
- カスタマーポータルユーザ
- パートナーユーザ
- ロール
- ロール & 内部下位ロール
- ロール、内部 & ポータル下位ロール
- ポータルロール
- ポータルロール & 下位ロール
- テリトリー
- テリトリーおよび下位テリトリー
- その他の公開グループ (ネスト)

グループはネストできます (グループ A がグループ B にネストされるなど) が、ネストは 5 レベル以内にする必要があります。ネストではグループメンバーの適用が行われるため、グループのメンテナンスおよびパフォーマンスに影響を及ぼします。組織の公開グループの合計数は 100,000 以内に抑えることをお勧めします。

公開グループの使用事例

任意のユーザグループにアクセス権を付与する必要がある場合、対象ユーザをまとめるための公開グループを作成し、他の共有ツールを使用してグループに必要なアクセス権を付与できます。グループメンバーだけではデータアクセスを提供できません。

グループは互いにネストできるため、ネストされる側のグループは、それをネストする側のグループと同じアクセス権を取得できます。これにより、ロール階層やテリトリー階層とは必ずしも連動しない、小規模な特別な目的のための階層を作成できます。グループ A がグループ B のメンバーである場合、グループ A のメンバーは、グループ B のメンバーと同じアクセスレベルで、グループ B と共有されるデータにアクセスできます。

グループには、ロール階層でグループメンバーより上位にあるユーザが、グループで共有されるデータにアクセスできないよう保護する機能もあります。この機能 (およびレコード所有者とその管理階層のアクセス処理) により、機密性がきわめて高い情報を共有できるグループを作成できます。データにアクセスできるのはグループメンバーのみであり、組織内の他のユーザは一切アクセスできません。これは、階層を使用したアクセス許可設定を使用することで実現できます。

所有権に基づく共有ルール

所有権に基づく共有ルールを使用して、組織の共有設定およびロール階層に例外を許可し、所有しないレコードに対して追加のユーザアクセス権を付与できます。所有権に基づく共有ルールは、レコード所有者のみを基にしています。

取引先責任者の所有権に基づく共有ルールは、非公開の取引先責任者には適用されません。

オブジェクトあたりの所有権に基づく共有ルール数は 1,000 以内に抑えることをお勧めします。

所有権に基づく共有ルールの使用事例

ロールに基づくマトリックス管理またはフロート表示の場合: サービス部門の社員が販売データを表示する必要がありますが、階層の異なるブランチに属している場合、ブランチが異なるロール間でデータを共有するルールを作成できます。

同じロールまたはテリトリーを持つ同僚にデータアクセスを提供します。

他のユーザグループ (公開グループ、ポータルロール、テリトリー) にデータアクセスを提供します。レコードを所有するグループのメンバーは、他のグループのメンバーと共有できます。

条件に基づく共有ルール

条件に基づく共有ルールでは、レコードの項目値 (条件) に基づいて、レコードへのアクセス権が提供されます。条件(1つまたは複数の項目値)が一致すると、ルールに対して共有レコードが作成されます。レコード所有権は考慮されません。

オブジェクトあたりの条件に基づく共有ルール数は 50 以内に抑えることをお勧めしますが、Salesforce ではこの数値を増加できます。

条件に基づく共有ルールの使用事例
レコードの項目値に基づいて、ユーザまたはグループにデータアクセスを提供します。

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を必要とするユーザの一貫性のあるグループを定義することが必要な場合があります。このような場合、レコード所有者は共有の直接設定を使用して、レコードにアクセス権限を持たないユーザに参照権限および編集権限を与えます。共有の直接設定は組織の共有設定、ロール階層、または共有ルールのように自動化されていませんが、レコード所有者に、レコードを参照する必要があるユーザと特定のレコードを共有する柔軟性を提供します。

レコード所有者が変更された場合や、付与された共有アクセス権ではオブジェクトに関する組織の共有設定のアクセスレベルを超える追加アクセス権が許可されない場合には、共有の直接設定は削除されます。これは、プログラムで作成される共有の直接設定にも適用されます。

標準オブジェクトで作成できるのは、共有の直接設定レコードのみです。共有の直接設定レコードは、共有理由が共有の直接設定に設定された共有レコードとして定義されます。

共有理由が*共有の直接設定*に設定されたすべての共有レコード(標準オブジェクトおよびカスタムオブジェクト)は、共有レコードがプログラムで作成された場合でも、オブジェクトのページレイアウトの[共有]ボタンを使用して編集および削除できます。

共有の直接設定の使用事例
現在のレコードに対するアクセス権限(「参照のみ」または「参照・更新」)を他のユーザ、グループ、ロールに付与する機能をユーザに提供します。

チーム

チームとは、取引先、営業商談、またはケースを担当するユーザで構成されるグループです。レコード所有者は、所有しているレコードごとにチームを作成できます。レコード所有者は、チームメンバーを追加し、レコードに対する各チームメンバーのアクセスレベルを指定できます。一部のチームメンバーには「参照のみ」権限を付与し、他のメンバーには「参照・更新」権限を付与できます。

チームメンバーを追加し、メンバーに他のアクセス権限を付与できるのは、所有者、上位階層のユーザ、およびシステム管理者のみです。「参照・更新」権限を持つチームメンバーは、チームが関連付けられているレコードに対してすでにアクセス権を持つ別のメンバーを追加できますが、そのメンバーに他のアクセス権限を付与することはできません。

アプリケーションでチームメンバーを作成すると、チームレコードと関連共有レコードの2つのレコードが作成されます。チームメンバーをプログラムで作成する場合は、チームレコードと関連共有レコードの両方を管理する必要があります。レコード(取引先、商談、ケース)ごとに1つのチームのみが存在します。複数のチームが必要な場合は、特定のニーズに応じてテリトリー管理またはプログラムによる共有を考慮してください。

チームオブジェクトはファーストクラスオブジェクトではありません。チームに対してカスタム項目、入力規則、トリガは作成できません。

チーム (取引先および商談) の使用事例
アクセス権限 (「参照のみ」または「参照・更新」) を 1 つのユーザグループ (チーム) に付与する機能をユーザに提供します。
外部コミッションやテリトリー管理システムなどによってチームが外部で管理される場合は、インテグレーションを使用して取引先チームを管理できます。外部システムのテリトリー管理をSalesforce内のチームソリューションと連携できる場合もあります。
取引先の複数の所有者は、取引先チームで管理できます。
1 つのユーザグループ (チーム) には、商談レコードに対する「参照のみ」または「参照・更新」権限のいずれかが必要です (商談チーム)。

テリトリー階層

テリトリー階層とは、階層構造内の部署または任意のセグメント別に構築できる 1 次元の追加階層です。テリトリー管理が有効な場合は、ロール階層とテリトリー階層の両方を管理する必要があります。

テリトリーは、取引先、商談、および取引先と商談の主従関係の子にのみ存在します。組織には 500 個のテリトリーを設定できますが、Salesforce ではこの数値を増加できます。テリトリー階層は、階層内のブランチで 10 レベル以内に抑えることをお勧めします。

テリトリーの割り当てルールが変更されると、そのテリトリーをソースとして使用する取引先テリトリー共有ルールが再適用されます。同様に、テリトリーのメンバーシップが変更されると、そのテリトリーをソースとして使用する所有権に基づく共有ルールが再適用されます。

テリトリー管理の使用事例
複数のユーザグループ(複数のチーム)には、取引先に対する「参照のみ」または「参照・更新」権限のいずれかが必要です。
追加の階層構造 (ロール階層とは異なる) が必要です。
単一ユーザが、階層内の複数レベルを保持する必要があります。
グローバルユーザ (GAM – グローバルパートナー担当営業) は、グローバルアカウント以下にあるすべてを表示する必要があります。

取引先テリトリー共有ルール

取引先テリトリー共有ルールは、組織でテリトリー管理が有効な場合にのみ使用できます。この共有ルールでは、ルールで定義されたテリトリーでスタンプが付けられた取引先レコードへのアクセス権が付与されます。

取引先テリトリー共有ルールの使用事例
テリトリー内の取引先(所有権には基づかない)へのデータアクセスをユーザグループに提供します。テリトリー管理が有効な場合に、取引先に対してのみ適用されます。

プログラムによる共有

プログラムによる共有 (Apex による正式な共有管理) では、データアクセス要件を他の手段で満たすことができない場合に、コード (Apex またはその他) を使用して高度で動的な共有設定を作成できます。

共有レコードをプログラムで作成し、標準の共有理由 (*共有の直接設定*) を使用すると、この共有レコードをアプリケーションの [共有] ボタンで管理できます。共有レコードは、所有者の移行による削除など、共有の直接設定の共有理由に関するすべてのルールの対象になります。

プログラムによる共有を使用する前に、https://developer.salesforce.com/page/Using_Apex_Managed_Sharing_to_Create_Custom_Record_Sharing_Logic を確認してください。

プログラムによる共有の使用事例
他の共有方法 (宣言型) でデータアクセスのニーズが満たされない場合。
ユーザアクセスの割り当て用に既存の外部システムがある場合。このシステムはアクセスを引き続き制御し、Salesforce と統合されます。
ネイティブの共有コンポーネントを使用すると、パフォーマンスが低下する場合 (通常、データ量が多い場合)。
カスタムオブジェクトでのチーム機能。

暗黙的な共有

暗黙的な共有は自動的に行われます。オンまたはオフに設定することはできず、アプリケーションに対してネイティブに設定されます。つまり、これは構成可能な設定ではありませんが、アーキテクトがこれを把握していることが非常に重要です。親の暗黙的な共有では、ユーザが取引先の子の商談、ケース、または取引先責任者へのアクセス権を持っている場合に親レコード (取引先のみ) へのアクセス権が付与されます。Salesforce には、ユーザが取引先責任者 (あるいは商談、ケース、または注文) を表示できる場合には、関連する取引先も暗黙的に表示されることを示すデータアクセスポリシーがあります。子の暗黙的な共有では、取引先の子レコードへのアクセス権が取引先所有者に付与されます。このアクセス権は、ロール階層の所有者のロールで定義されます。子の暗黙的な共有は、取引先責任者、商談、およびケースオブジェクト (取引先の子) に対してのみ適用されます。ロールの作成時にそれぞれの子オブジェクトに付与できるアクセスレベルは、「参照」、「編集」、および「アクセス権限なし」です。アクセスレベルを「参照」に設定すると、取引先所有者は関連するオブジェクトレコード (取引先責任者、商談、またはケース) を暗黙的に表示できます。「編集」に設定すると、取引先所有者は関連するオブジェクトレコード (取引先責任者、商談、またはケース) を暗黙的に変更できます。

暗黙的な共有は、カスタムオブジェクトには適用されません。

顧客の実装シナリオ

すべての組織に適合する共有モデルはありません。最適な共有モデルを設計するときの要件や課題は、組織ごとに異なります。組織の共有要件に合わせて最適なデータアクセスコンポーネントを使用することが重要です。次のシナリオは、共有モデルを設計するときの一般的な問題です。

顧客のシナリオ:カスタマーマスタシステムによって外部管理されるチーム割り当て

要件/課題	解決策
ある地域を担当する営業マネージャが、サポート目的で別の担当地域にもアクセスする必要がある (一人二役)。	所有権に基づく共有ルール: これは通常の場合ではなく例外であるため、所有権に基づく共有ルールを使用します。この場合は信頼できるマネージャであるため、所有権に基づく共有ルールによって、実際に必要な権限以上のアクセス権が付与されてもかまいません。
国に基づく操作で、ユーザがすべての国の販売データにアクセスする必要がある。	所有権に基づく共有ルール:販売以外の部署が販売データにアクセスする必要がある場合の、共有ルールの一般的な使用例です。
全体の 80% 以上で、取引先に「コア 4」チーム (アカウントエグゼクティブ、営業担当内、セールスコンサルタント、技術営業担当) がある。取引先チームのレコードのシステムは SFDC に対して外部。取引先にはチームが常に 1 つだけ。	チーム (取引先および商談): 取引先ごとにチームが常に1つしかないため、ロールが異なる多くのメンバーが存在しても、取引先チームの機能でこの要件が満たされます。
チームのマネージャに、部下と同じアクセス権が必要。	ロール階層:部下のデータに対するアクセス権をマネージャに許可することによって、ロール階層を使用して解決できます。
割り当てられた取引先チームを変更できない。	チーム (取引先および商談): 取引先チームの機能では実際には対応できませんが、取引先チームを使用できない状態を回避する必要があります。チームをロックダウンする方法はいくつかありますが、この場合は、取引先チームのページレイアウトを削除する方法を使用します。
あるユーザが病欠または休暇中に、取引先または商談に対して標準アクセス権を持たない別のユーザがその期間中アクセスできるようにする「バディ」機能が必要。	チーム (取引先および商談): 「バディ」は、この要件を満たすためのチーム上のロールにすぎません。ただし、課題はチームを変更できないという以前の要件にあります。SFDC 内でチームを変更できる一連のユーザグループを設定し、必要に応じて「バディ」ロールを作成することが唯一の解決策です。
案件でカスタムソリューションが必要な場合に、他のユーザ(必ずしも販売組織に属さない)が案件にアクセスできるようにする必要がある。	チーム (取引先および商談): 新しいメンバーを (関連リストを使用して) 商談チームに手動で追加することによって実現する、商談チームの標準的な使用例です。追加するメンバーが常にわかっている場合は、トリガを使用してもかまいません。この場合は、商談別の商談となります。

顧客のシナリオ: 標準テリトリー管理

要件/課題	解決策
2 つの異なる部門 (小売販売と再マーケティング) の 2 つの異なる商談チームで、同じ取引先レコードにアクセスする必要がある。この2部門は取引先責任者を共有しており、取引先のすべての活動を認識している。また、それぞれの部門独自の階層と積み上げ集計もある。	テリトリー管理: 最も適切な対応策は、構造が大幅に異なる2つのブランチを階層に含めることです。取引先にアクセスする必要がある 2 レベル (どちらのレベルもメンバーはその部門の商談チーム) の 2 つの異なるブランチがあるということで、テリトリー管理が妥当です。チーム概念を使用して実現することもできますが、これは細かすぎます。営業のセグメント化は、取引先レベルではなく階層内で行われます。
特定の商談チーム(テリトリー)の特定の取引先に割り当てられ、この取引先へのアクセスを必要とする、ビジネス開発者の別個のグループがある。ビジネス開発者は商談チームの共有リソースであり、各ビジネス開発者は、1 つ以上の商談チームの 1 つ以上の取引先に割り当てられる可能性がある。	テリトリー管理: これはユーザグループ(またはチーム)であり、各ビジネス開発チームは取引先ごとに異なる可能性があります。また、別の理由によりテリトリー管理が必要であるため、最良の方法は、これらのビジネス開発チームを表すサブテリトリーを作成することであるといえます。
取引先に 1 回だけアクセスする必要がある、コミッションに基づかない営業サポートロールがある。	チーム (取引先および商談): この要件の重要な部分は「1 回限り」という点です。これは、取引先ごとに行われるため、取引先チームでネイティブに提供されます。
クレジット部門で、特定の部署のすべての取引先にアクセスする必要がある。	所有権に基づく共有ルール: これは、特定の部署全体でユーザグループがすべてのものを表示する必要がある状況です。グループが属するロールの共有ルール、グループが属すロール階層のブランチ (ロールまたは下位ロール)、または公開グループで実現できます。
マネージャに、部下と同じアクセス権が必要である。	ロール階層:部下のデータに対するアクセス権をマネージャに許可することによって、ロール階層を使用して解決できます。

考慮事項

他の共有コンポーネントをすべて使用していても、テリトリー管理は必要です。テリトリー管理は元に戻せないため、その影響を把握しておくことは非常に重要です。

ロール階層に与える影響は?

ロール階層には影響はありません。2つの階層を管理しているため、共有はさらに複雑になります。ロール階層をできるだけフラット化 (簡略化) することをお勧めします。販売データがほとんどである SFA 組織の場合は、ロール階層をフラット化し、テリトリー階層を販売階層として使用できます。ただし、Service Cloud、HRアプリケーション、法務アプリケーションなど、販売以外のアプリケーションが組織に存在する場合は、(非販売ユーザに対応するため) 大規模なロール階層も必要になります。一般に、ロール階層を非

販売階層にするには、販売部門のブランチをフラット化してから、テリトリー階層を「販売」階層として使用します。ロール階層とテリトリー階層を同じにすると不要な共有アクティビティが発生する原因となるため、お勧めしません。

ロール階層の必要性を検討するうえで考慮すべきもう 1 つの点は、「代理管理」、「私のチーム」条件、フォルダベースのアクセスなどの一部の機能が、ロール階層でしか使用できないということです。

チームを引き続き使用できますか?

はい、できます。ただし、テリトリー階層内でアクセス要件 (フロート表示など) を満たすことができる場合は、チームを使用するよりテリトリー階層で行う方が適切です。すでに2つの階層(ロールとテリトリー)を管理しているので、処理をできるだけ簡単にするため、他の既存の共有コンポーネントがなければ実装チームのみで要件を十分に満たすことができます。

再配置と再割り当て

ロール、チーム、テリトリーのメンバーシップと、階層の構造という 2 種類の変更があります。メンバーシップの変更は通常、毎日発生し、1 時間ごとに発生する場合もあります。階層構造 (再配置) の変更は通常、それより頻度が低く (四半期ごと、半年ごと、1 年ごと)、リソースを大量に消費する可能性があります。考慮すべき点は、変更の量と、各変更によって生じる連鎖変更の数です。一般に、構造の変更は四半期に 1 回を超えないように抑え、大規模なすべての変更 (一括変更など) は十分に計画、テスト、および調整します。

大量のデータ

初期ロールアウト用にモデル化しているか再配置の変更を計画しているかに関わらず、データ量については十分に考慮する必要があります。パフォーマンスが要因となるしきい値があるため、本番稼動する前に変更を Sandbox でテストすることを強くお勧めします。これは、変更の所要時間の基準にもなります。

取引先が 200 万を超え、チームまたはテリトリー管理が実装されている場合は、パフォーマンスに特に注意する必要があります。これらは大量のレコードを共有できる複雑な共有モデルコンポーネントであるため、トランザクションの実行に時間がかかります。

共有適用の延期

共有を利用するオブジェクトおよび大量のレコード (200 万を超える取引先など) があり、一括変更 (階層の変更を要する四半期ごとの再配置など) を行う必要がある場合は、Salesforce サポートで有効にできる機能を使用して、共有適用の自動適用を延期することができます。ロール階層、テリトリー階層、グループ、共有ルール、ユーザロール、チームメンバー、またはレコードの所有権に対する個々のすべての変更によって、自動共有適用がネイティブに開始されます。また、一括変更が行われると、多くの自動共有適用が開始されます。これらを一時停止することにより、変更を加えた後ですべての共有適用をまとめて一度に行うことができます。通常、この方法はより効率的であり、一括変更の実行に適しています。

データスキュー/所有者スキュー

データスキューとは、少数の親レコードに多くの子レコードが存在することです。少数の取引先に多くの取引先責任者、商談、ケースが存在すると、深刻な問題となります。比率が1:10,000になると、パフォーマンスが低下し始めます。そのため、この比率を超えないようにすることをお勧めします(低い比率を推奨)。

所有者スキューはデータスキューと似ていますが、データスキューは、単一ユーザ、ロール、またはグループがオブジェクトの大量のレコードを所有していることを指します。所有者スキューの場合も、トランザクションの実行時間が長くなり、変更が生じた時点でパフォーマンスが低下します。所有者とレコード数の比率も 1:10,000 をお勧めします。

単一ユーザが所有するレコードが 10,000 件を超える場合は、次のようにすることをお勧めします。

- 所有者のユーザレコードで、ロール階層内のロールを保持しない。

- 所有者のユーザレコードでロールを保持する必要がある場合は、ロール階層の自分のブランチで階層の最上位にロールを配置する。

取引先階層がデータアクセスに及ぼす影響
取引先階層を実装する場合、多くのユーザーが誤った認識を持つことがあります。それは、親取引先にアクセスできるユーザは、子取引先にもアクセスできるというものです。2つのレコードが親子関係にあるというだけではアクセスは制御されません。ロール階層とテリトリー階層はこのように動作しますが、これは取引先階層には当てはまりません。

トラブルシューティング

モデルアーキテクチャの共有が完了すると、ユーザがレコードを表示できる理由、または表示できない理由を確認する必要が生じる可能性があります。通常、表示されないはずのレコードが表示される場合に問い合わせがあることはありませんが、このような状況が発生した場合、レコードに対するアクセス権を持つすべてのユーザとその理由を確認する方法があります。

これよりも困難で、おそらくよくある問題として、ユーザがレコードを表示できない理由を確認する必要がある場合があります。設計したセキュリティレイヤによって、どこを最初に確認するかが決まります。共有モデルを十分に把握しており、アクセス権を付与したコンポーネントが明白な場合は、その確認から始めます。ただし、共有モデルに精通していない場合は、ロール階層から開始し、各レイヤを1つずつ入念に確認して、アクセス権を付与し更新を行うレイヤを判断します。トラブルシューティングフローを次に示します。

1. オブジェクトへのアクセス権限がユーザにあることを確認します。
2. レコードを表示できないユーザのロールを特定し、記録します。
3. レコード所有者のロールを特定し、記録します。
4. ロール階層を調べて、これらの 2 つのロールが 2 つの異なるブランチにあることを確認します (そうなっている必要があります)。
5. 次に、オブジェクトの共有ルールを調べて、ユーザアクセスを付与するルールがないことを確認する必要があります。公開グループの調査が必要になる場合もあります。共有ルールが存在するグループからユーザが漏れてしまっただけなのか、あるいは、ユーザアクセスを付与する新しい共有ルールを作成すべきなのかを判断します。これは、管理するアーキテクチャによって異なり、所有権に基づく共有ルールと条件に基づく共有ルールの両方に適用されます。
6. チームを使用している場合は、そのレコードのチームにユーザを含めるべきかを判断します。また、チームはどのように管理され、この状況がどのようにして発生したのかを検証します。
7. 共有の直接設定を使用している場合は、レコード所有者が変更になったためにユーザがアクセス権を失った可能性があります。共有の直接設定は、所有権が変更されると削除されます。共有の直接設定が、[共有] ボタンを使用して削除された可能性もあります。
8. テリトリー管理を使用している場合は、テリトリーのいずれかからユーザが欠落していないか確認します。また、テリトリーのメンバーシップはどこで管理され、欠落がどのようにして発生したのか検証します。この他にも、ユーザがメンバーとなっているテリトリーでレコードにスタンプが付けられていないという可能性もあります。
9. プログラムによる共有を作成しており、コードで共有を作成するための条件がある場合は、コードを調べてこのユーザが漏れた理由を確認します。

『共有モデルの仕組み』に関するご意見は、ccefeedback@salesforce.com までお寄せください。