CA Asset Portfolio Management

管理ガイド

リリース 12.9.00

CA Technologies 製品リファレンス

このドキュメント セットには以下の CA Technologies ブランドと製品についての記述があります。

- CA Asset Converter
- CA Asset Portfolio Management （CA APM）
- CA Business Intelligence
- CA Client Automation

  （旧称： CA IT Client Manager）
- CA Configuration Management Database （CA CMDB）
- CA Embedded Entitlements Manager （CA EEM）
- CA 管理データベース（CA MDB）
- CA Process Automation™
- CA Service Catalog
- CA Service Desk Manager
- CA Software Asset Manager （CA SAM）
- CA SiteMinder®

このドキュメント セットには、以下のコンポーネントについての記述もあります。このコンポーネントには以前は別の名前が使用されていました。

- Common Asset Viewer

  （以前のアセット管理システム（AMS））

CA への連絡先

テクニカル サポートの詳細については、弊社テクニカル サポートの Web サイト（http://www.ca.com/jp/support/）をご覧ください。

目次

第 1 章: はじめに

このセクションには、以下のトピックが含まれています。

対象読者

本書は、製品の管理に関して全面的な責任を負う CA APM 管理者を対象としています。 このガイドは、ユーザがアセットを毎日管理できるように、この製品の準備をサポートすることを目的としています。

また、このガイドは「実装ガイド」の情報に基づいて製品がインストールされていることを前提としています。

環境管理

CA APM の全般的な管理には、セキュリティの設定、ユーザ インターフェースの設定、ハードウェア照合の管理、オプションの製品コンポーネントの設定変更などが含まれます。 この製品の管理機能には柔軟性があり、以下の管理タスクを任意の順序で完了できます。

以下のタスクを完了してから、製品にログインするための CA APM の URL およびログイン認証情報をすべてのユーザに提供します。

セキュリティ

製品および機能へのユーザ アクセスを制御するためにセキュリティを定義します。 たとえば、あるユーザにモデルとアセットへのアクセス権を付与して、別のユーザにリーガル ドキュメントへのアクセス権を付与することができます。

注: 詳細については、「セキュリティ (P. 15)」を参照してください。

ユーザ インターフェースの設定

ユーザ インターフェースを設定して、ユーザによるデータの入力、管理、および検索方法を簡略化できます。 また、許可されていないタスクをユーザが実行できないようにすることでユーザのセキュリティと保護を提供し、IT アセット管理プラクティスの準拠を保証することができます。たとえば、すべての CA APM ユーザに対して［連絡先］ページをグローバルに非表示にできます。 ただし、一部のユーザは連絡先情報を参照および更新できる必要があります。 そのため、それらのユーザに対して[連絡先]ページを表示します。ユーザ インターフェースの設定には柔軟性があり、ユーザ インターフェースのほぼすべての側面を設定できます。

注: 詳細については、「ユーザ インターフェースの設定方法」を参照してください。

ハードウェア照合

ハードウェア照合を使用して、*検出されたアセット*を別の論理リポジトリ内の対応する*所有アセット*に一致させ、アセットを管理します。許可されていない、紛失している、あまり使用されていない、または過剰に使用されているアセットを特定し、ハードウェア アセット ベースの最適化に役立てることができます。

注: 詳細については、「ハードウェア照合」を参照してください。

製品コンポーネント

製品のインストール中に設定された製品コンポーネント構成を変更できます。たとえば、Oracle のリスニング ポートを変更できます。また、追加のサーバにコンポーネントを追加し、製品のパフォーマンスを管理し、製品の拡張を可能にすることもできます。たとえば、追加のサーバにハードウェア照合エンジンを追加できます。 柔軟に設定できるため、多くのコンポーネントの設定を変更できます。

注: 詳細については、「製品コンポーネントの設定 (P. 143)」および「コンポーネント サーバの追加 (P. 169)」を参照してください。

CA APM へのログイン

製品をインストールした後、実装者はサービスがすべて開始されたことを確認し、Web インターフェースを起動して CA APM の使用準備ができていることを確認します。 実装者から、製品にログインするための URL と認証情報が提供されます。これで、製品でアセットを管理する準備が整いました。

デフォルト システム管理者ユーザのログイン認証情報（ユーザ名とパスワード）は、デフォルトで uapmadmin です。 CA EEM コンポーネントの設定を変更することにより、要件に合わせてパスワードを変更できます。

注: デフォルト パスワードはインストール プロセス中にも変更できます。

第 2 章: セキュリティの確保

このセクションには、以下のトピックが含まれています。

セキュリティ

CA APM へのユーザ アクセスを許可する前に、許可されていない変更や不正な変更からリポジトリを保護し、ユーザが必要なデータを利用できるように、セキュリティを設定します。 たとえば、あるユーザにモデルとアセットへのアクセス権を付与して、別のユーザにリーガル ドキュメントへのアクセス権を付与することができます。

セキュリティを設定するには、以下のタスクを実行します。

1. ユーザ (P. 16)。 製品にアクセスできるユーザを定義します。
2. ユーザの役割 (P. 19)。同様のタスクを実行するユーザのグループを定義します。
3. 認証 (P. 29)。 ユーザがログインしたときに認証する方法を定義します。
4. 検索 (P. 31)。 検索を使用できるユーザを定義します。
5. 設定 (P. 35)。許可されていないタスクをユーザが実行できないようにします。

1 人以上のシステム管理者が、CA APM 内でこれらのセキュリティ タスクを実行します。 ユーザ ID *uapmadmin* を使用するシステム管理者は、グローバル システム管理者として製品のセキュリティ全般を完全に制御できます。

Web インターフェースを使用することにより、企業の全域にセキュリティを適用します。これらのタスクを実行するのには、最低限のデータベース スキルが必要です。

ユーザ

製品に新しいユーザを追加してユーザ ID とパスワードを割り当てると、ユーザのセキュリティが確立されます。 ユーザは、有効なユーザ ID とパスワードがないとログインできません。ユーザごとにユーザ レコードが作成され、そのレコードは ca_contact テーブル内の連絡先と関連付けられます。

製品にユーザを追加するには、以下の方法があります。

1. ユーザをインポートする (P. 17)。
2. ユーザを手動で定義する (P. 17)。

手動でユーザを定義する場合、ただちにユーザを許可して製品を使用させることができます。 ただしユーザをインポートする場合は、まずインポートしてからユーザを許可 (P. 18)できます。

注: ユーザを手動で定義するときは、対応する CA EEM ユーザも作成されます。ユーザが CA APM にログインするときに、CA EEM はユーザ名とパスワードを検証します。

CA APM ユーザをすべて定義したら、各ユーザをユーザの役割に割り当てて、ユーザがログインしたときに参照およびアクセスできる内容を指定するために役割のアクセス権全体を割り当てます。

ベスト プラクティス(ユーザおよび役割)

ユーザと役割を効果的に管理するには、以下のベスト プラクティスを使用します。

- ユーザは有効なユーザ ID とパスワードを提供され、ログインを許可されている必要があります。
- 新しい役割をユーザに割り当てる前に、役割からユーザを削除します。

  注: ユーザを複数の役割に割り当てることはできません。
- 役割を削除する前に、その役割に割り当てられたユーザがいないことを確認します。
- 役割を削除する前にユーザを削除します。

ユーザのインポートおよび同期

重要: このタスクを実行するユーザが、ユーザ管理アクセスが有効な役割に属することを確認します。

CA EEM を通じて、Active Directory などの外部ユーザ ストアからユーザのリストをインポートし、そのリストを同期して CA APM 内に連絡先として保存できます。ユーザのインポートによって、ユーザを定義する時間を節約でき、ユーザ情報の正確性も確保されます。ユーザをインポートして保存した後、ユーザに対して製品へのアクセスを許可します。

ユーザをインポートおよび同期する方法

1. ［管理］-［ユーザ/役割管理］をクリックします。
2. 左側の［ユーザ管理］メニューを展開します。
3. ［LDAP データ インポートおよび同期］をクリックします。

   ［LDAP データ インポートおよび同期］ページが表示されます。
4. マルチテナントが有効な場合は、ドロップダウン リストからテナントを選択します。
5. ［LDAP データ インポートおよび同期の開始］をクリックします。

   インポート プロセスが開始され、ユーザが外部ストアからインポートされます。 マルチテナントが有効な場合、ユーザは選択したテナントの連絡先として ca_contact テーブル内にインポートされます。 その後、インポートされたユーザによる製品へのアクセスを許可 (P. 18)できます。

重要: ［LDAP データ インポートおよび同期］は、ユーザ名の先頭が文字または数値の場合に機能します。ユーザ名の先頭が特殊文字の場合はインポートされません。

ユーザの定義

重要: このタスクを実行するユーザが、ユーザ管理アクセスが有効な役割に属することを確認します。

CA APM のユーザをすべて定義して、製品へのアクセス権を付与します。 ユーザを定義した後、ユーザに役割を割り当てます (P. 25)。

ユーザを定義する方法

1. ［管理］-［ユーザ/役割管理］をクリックします。
2. 左側の［ユーザ管理］メニューを展開します。

3. ［新規ユーザ］をクリックします。

   ［新規ユーザ］ページが表示されます。

4. 新規ユーザの情報および連絡先関連の情報を入力します。
5. （オプション）ユーザの製品へのアクセスを許可するかどうかを指定します。
6. ［保存］をクリックします。

   ユーザが定義されます。

ユーザの許可

重要: このタスクを実行するユーザが、ユーザ管理アクセスが有効な役割に属することを確認します。

ユーザが製品にログインして使用できるように、ユーザを許可できます。ユーザを許可する前に、連絡先としてユーザを保存します。

ユーザを許可する方法

1. ［管理］-［ユーザ/役割管理］をクリックします。
2. 左側の［ユーザ管理］メニューを展開します。
3. ［ユーザの許可］をクリックします。

   ［ユーザの許可］ページが表示されます。

4. 検索して、利用可能なユーザのリストを見つけます。
5. 許可するユーザを選択し、［OK］をクリックします。

   ユーザが［許可されたユーザ］リストに表示されます。

6. ユーザ名の横にある［編集］アイコンをクリックします。
7. （オプション）連絡先を選択し、連絡先詳細にユーザを割り当てます。

   注: 連絡先を選択しない場合、そのユーザ用に新しい連絡先が作成されます。

8. （オプション）ユーザに割り当てる役割を選択します。
9. ［許可］をクリックします。

   選択されたユーザが、製品へのログインを許可されます。

ユーザ アクセスの拒否

重要: このタスクを実行するユーザが、ユーザ管理アクセスが有効な役割に属することを確認します。

ユーザ アクセスを拒否し、製品へのログインを禁止できます。たとえば、新しいアセット技術者を雇用し、そのアセット技術者が適切なトレーニングを受講するまで製品を使用できないようにする必要があるとします。ユーザ アクセスを拒否しても、ユーザの連絡先情報は製品から削除されません。

ユーザ アクセスを拒否する方法

1. ［管理］-［ユーザ/役割管理］をクリックします。
2. 左側の［ユーザ管理］メニューを展開します。
3. ［ユーザの許可］をクリックします。

   ［ユーザの許可］ページが表示されます。
4. ［許可されたユーザ］リストで、アクセスを拒否するユーザを選択します。
5. ［認証の無効化］をクリックします。

   ユーザは製品にログインできなくなります。

ユーザの役割

*ユーザの役割*は、製品内のセキュリティおよびユーザ インターフェース ナビゲーションを制御するプライマリ レコードです。ユーザがビジネスの役割に対して割り当てられているタスクを実行するために必要な機能のみを公開することによって、役割ごとに製品の限定ビューが定義されます。 ユーザのデフォルトの役割および関連するユーザ インターフェース設定は、ユーザが利用できるデータおよび機能を決定します。 ユーザは 1 つの役割のみに属することができます。

ユーザの役割を定義して、機能およびフィールド レベルでリポジトリのアクセス権を適用します。 各役割に必要なアクセス権のレベルを決定し、割り当てます。同じ職務のユーザをグループ化し、対応する役割をグループに割り当てます。 役割を割り当てることで、データの追加や削除といった許可されていないタスクをユーザが実行できないようにします。 たとえば、管理者の役割のユーザにはすべてのレコードへのフル アクセス権が必要ですが、アセット技術者の役割のユーザにはより少数のレコードに対する限定されたアクセス権が必要です。

注: この製品には、ユーザ管理の基盤として使用できる事前定義済みのシステム管理者およびユーザの役割が用意されています。

次のタスクを実行して、ユーザの役割を設定および管理できます。

- 役割の定義 (P. 21)
- ユーザへの役割の割り当て (P. 25)
- 役割からのユーザの削除 (P. 26)
- 役割の更新 (P. 27)
- 役割の削除 (P. 28)
- 役割への設定の割り当て (P. 27)

事前定義役割

製品はシステム管理者の役割を提供します。この役割にはすべてのオブジェクトおよびテナント データに対する完全なコントロールおよびアクセス権が付与されています。 この役割はシステム管理者の連絡先に関連付けられ、削除できません。 この役割のユーザは、ビジネス要件を満たすための追加の役割の定義および更新に加えて、オブジェクトの定義、更新、削除が可能です。 システム管理者の役割に設定を割り当てることはできません。

また、製品はユーザを管理するのに役立つ以下の事前定義済みユーザ役割を提供します。

- CA APM アセット技術者 - アセット情報を操作するために必要なデータおよび機能のみにアクセスできます。
- CA APM 契約管理者 - リーガル ドキュメントおよび契約管理プロセスを操作するために必要なデータおよび機能のみにアクセスできます。
- CA APM デフォルト ユーザ - 製品の一部を読み取り専用で表示できます。 この役割は、製品内のほとんどのデータを表示できます。 ただし、この役割は製品データを変更できません。
- CA APM 実行者 - アセット フルフィルメント タスクに必要なデータおよび機能のみにアクセスできます。
- CA APM 取得 - フルフィルメント プロセスから受け取ったアセットの更新に必要なデータおよび機能のみにアクセスできます。

事前定義済みユーザ役割にはそれぞれ設定が関連付けられています。この設定は、特定の機能を完了するのに必要なデータへのアクセスを提供します。各事前定義済み役割に関連付けられた設定を変更できます。事前定義済み役割は新規インストールの後にのみ使用可能です。

ユーザの役割の定義

重要: このタスクを実行するユーザが、役割管理アクセスが有効な役割に属することを確認します。

サイト固有のビジネス要件を満たすために、カスタマイズされたユーザの役割を定義できます。たとえば、照合管理にアクセスできる役割と、別のアセット フルフィルメントにアクセスできる役割を定義できます。

ユーザの役割を定義する方法

1. ［管理］-［ユーザ/役割管理］をクリックします。
2. 左側の［役割管理］メニューを展開します。
3. ［新規役割］をクリックします。
4. 役割の情報を入力します。

ユーザ管理アクセス

このチェック ボックスをオンにすると、役割に割り当てられたユーザがユーザ管理機能（［管理］、［ユーザ/役割管理］、［ユーザ管理］）にアクセスできるようになります。［ユーザ/役割管理］サブタブは、ユーザ管理機能、役割管理機能、またはその両方へのアクセス権が役割に付与されている場合にのみ利用可能です。

役割管理アクセス

このチェック ボックスをオンにすると、役割に割り当てられたユーザが役割管理機能（［管理］、［ユーザ/役割管理］、［役割管理］）にアクセスできるようになります。［ユーザ/役割管理］サブタブは、ユーザ管理機能、役割管理機能、またはその両方へのアクセス権が役割に付与されている場合にのみ利用可能です。

システム設定アクセス

このチェック ボックスをオンにすると、役割に割り当てられたユーザがシステム設定機能（［管理］、［システム構成］）にアクセスできるようになります。

Web サービス アクセス

このチェック ボックスをオンにすると、役割に割り当てられたユーザが CA APM Web サービス ドキュメントと WSDL （［管理］-［Web サービス］）にアクセスできます。 このチェック ボックスがオンにされていないときに、役割を持つユーザが外部クライアント アプリケーションから Web サービスにアクセスしようとすると、ログイン エラーが表示されます。

フィルタ管理アクセス

このチェック ボックスをオンにすると、役割に割り当てられたユーザがフィルタ管理機能（［管理］、［フィルタ管理］）にアクセスできるようになります。

その他情報設定へのアクセス

このチェック ボックスをオンにすると、役割を持つユーザがその他の情報設定機能にアクセスできるようになります。 この機能を使用すると、選択したオブジェクトに関する追加情報にアクセスできます。 この追加情報にアクセスするには、ページ左側の［関係］の下にあるメニュー項目を選択します。

Data Importer ユーザ アクセス

このチェック ボックスをオンにすると、役割に割り当てられたユーザがユーザ許可を使用して Data Importer 機能（［管理］、［Data Importer］）にアクセスできるようになります。 ユーザはインポートを作成し、自分のインポートを変更または削除できます。また、他のユーザによって作成されたどのインポートを表示することもできます。

Data Importer 管理者アクセス

このチェック ボックスをオンにすると、役割に割り当てられたユーザが管理者許可を使用して Data Importer 機能（［管理］、［Data Importer］）にアクセスできるようになります。 管理者はインポートを作成できます。また、任意のユーザによって作成されたどのインポートも変更または削除できます。

照合管理アクセス

このチェック ボックスをオンにすると、役割に割り当てられたユーザが照合ルール管理機能（［管理］、［照合管理］）にアクセスできるようになります。

アセット フルフィルメント アクセス

このチェック ボックスをオンにすると、役割に割り当てられた CA Service Catalog ユーザが CA Service Catalog を使用してアセット フルフィルメントを実行できるようになります。

注: CA Service Catalog を使用するアセット フルフィルメントの詳細については、CA Service Catalog のドキュメントを参照してください。

テナント管理アクセス

このチェック ボックスをオンにすると、役割に割り当てられたユーザがマルチテナント管理機能（［管理］、［テナント管理］）にアクセスし、マルチテナントの有効化、テナントの定義、サブテナントの定義、テナント グループの定義を実行できるようになります。

正規化アクセス

このチェック ボックスをオンにすると、役割に割り当てられたユーザが正規化ルール管理機能（［ディレクトリ］、［リスト管理］、［正規化］）にアクセスできるようになります。

大量変更ユーティリティ アクセス

このチェック ボックスをオンにすると、役割を持つユーザが大量変更ユーティリティ機能にアクセスできるようになります。 この機能を使用すると、モデルのアセット ファミリを変更し、アセットのモデルを変更することもできます。

5. （オプション）テナントの読み書き許可を指定します。 マルチテナントは、役割内のユーザがアクセスできるテナントまたはテナントのグループを制御するために役割の目的を拡張します。 マルチテナントが有効な場合、［テナント情報］セクションに［テナント読み取りアクセス］ドロップダウン リストと［テナント書き込みアクセス］ドロップダウン リストが表示されます。

注: マルチテナントが有効な場合にのみ、［テナント情報］セクションが表示されます。 マルチテナントを有効にする方法の詳細については、「*実装ガイド*」を参照してください。 また、サービス プロバイダ以外のテナントに関連付けられたユーザは、自分のテナントに関連付けられたオブジェクトのみを作成または更新できます。サービス プロバイダと関連付けられたユーザのみが、自分のテナント以外のテナントに属するオブジェクトの作成または更新を許可されます。

すべてのテナント

テナントの制限がありません。 このアクセス権を持つ役割に割り当てられたユーザは、データベース内の任意のオブジェクト（パブリック オブジェクトを含む）を表示できます。 また、サービス プロバイダに関連付けられたユーザは、任意のテナントに関連付けられたオブジェクトを更新または作成できます。 このアクセス権を持つサービス プロバイダ ユーザがオブジェクトを作成する場合、新しいオブジェクトのテナントを選択する必要があります。

連絡先のテナント

（デフォルト値）連絡先のテナントに役割を関連付けます。 このアクセス権を持つ役割に割り当てられたユーザは、自分のテナントに関連付けられたオブジェクトのみを表示、作成、更新（およびパブリック オブジェクトを表示）できるように制限されます。 このアクセス権を持つユーザがオブジェクトを作成する場合、テナントは選択できません。 テナントは連絡先のテナントに自動的に設定されます。

連絡先のテナント グループ

役割と連絡先のテナント グループを関連付けます。 このアクセス権を持つ役割に割り当てられたユーザは、自分のテナント グループ内のテナントに関連付けられたオブジェクトのみを表示、作成、更新（およびパブリック オブジェクトを表示）できるように制限されます。 このアクセス権を持つユーザがオブジェクトを作成する場合、自分のテナント グループに属する任意のテナントを選択できます。

単一テナント

役割と指定されたテナントを関連付けます。 このオプションを選択するときは、［テナント書き込み］フィールドまたは［テナント読み取り］フィールドのいずれかで、特定のテナントを選択します。 このアクセス権を持つ役割に割り当てられたユーザは、選択したテナントに関連付けられたオブジェクトのみを表示、作成、更新（およびパブリック オブジェクトを表示）できるように制限されます。 このアクセス権を持つユーザがオブジェクトを作成する場合、テナントは選択できません。 テナントは、選択したテナントに自動的に設定されます。

注: サービス プロバイダ ユーザのみが、自分以外のテナントに対してデータを作成または更新できます。 別のテナントへの単一テナント アクセスの役割を持つテナント ユーザのアクセスは読み取りアクセスに制限されます。

テナント グループ

役割と指定されたテナント グループを関連付けます。 このオプションを選択するときは、［テナント グループ書き込み］フィールドまたは［テナント グループ読み取り］フィールドのいずれかで特定のテナント グループを選択します。 このアクセス権を持つ役割に割り当てられたユーザは、テナント グループ内の任意のテナントに属するオブジェクトのみを表示できるように制限されます。また、サービス プロバイダに関連付けられたユーザは、グループ内の任意のテナントに関連付けられたオブジェクトを更新または作成できます。このアクセス権を持つサービス プロバイダ ユーザがオブジェクトを作成する場合、新しいオブジェクトのテナントを選択する必要があります。

パブリックの更新（チェック ボックス）

［すべてのテナント］を選択した場合に限り利用可能です。 このチェック ボックスをオンにすると、この役割に割り当てられたユーザがテナントの公開データの作成または削除を許可されます。

6. ［保存］をクリックします。

役割が定義され、ユーザを役割に割り当てることができます。

ユーザへの役割の割り当て

重要: このタスクを実行するユーザが、役割管理アクセスが有効な役割に属することを確認します。 また、ユーザに役割を割り当てないと、そのユーザには［管理］タブが表示されません。

ユーザに役割を割り当てて製品の限定ビューを定義し、ログイン時にユーザに表示される内容を指定できます。 たとえば、管理者をシステム設定役割に割り当てます。ユーザは 1 つの役割のみに割り当てることができます。役割にユーザを割り当てる前に、ユーザを連絡先として保存します。

注: ユーザに新しい役割を割り当てる前に、ユーザを前の役割から削除してください。

ユーザに役割を割り当てる方法

1. ［管理］-［ユーザ/役割管理］をクリックします。
2. 左側の［役割管理］メニューを展開します。

3. ［役割の検索］をクリックします。
4. 役割を検索し選択します。

   役割の詳細が表示されます。
5. ページの［役割の連絡先］領域で、［連絡先の割り当て］をクリックします。

   役割に割り当てられていないユーザがすべて表示されます。
6. 役割を割り当てるユーザを選択します。
7. ［OK］をクリックします。
8. ［保存］をクリックします。

   役割がユーザに割り当てられます。

役割からのユーザの削除

重要: このタスクを実行するユーザが、役割管理アクセスが有効な役割に属することを確認します。

役割からユーザを削除することにより、ユーザのアクセス権を制限できます。たとえば、管理者が別の部門に異動したとき、システム設定の役割から管理者を削除します。別の役割に割り当てる前に、またはユーザがサイトや組織のメンバでなくなる場合は、役割からユーザを削除します。

役割からユーザを削除する方法

1. ［管理］-［ユーザ/役割管理］をクリックします。
2. 左側の［役割管理］メニューを展開します。
3. ［役割の検索］をクリックします。
4. 役割を検索し選択します。

   役割の詳細が表示されます。
5. 役割から削除するユーザの横にある削除アイコンをクリックします。
6. ［保存］をクリックします。

   ユーザが役割から削除されます。

ユーザの役割の更新

重要: このタスクを実行するユーザが、役割管理アクセスが有効な役割に属することを確認します。

いつでもユーザの役割を更新し、製品へのログイン時にユーザに表示される内容を変更できます。 たとえば、特定の役割のユーザがテナント管理機能を実行しなくなったとします。その場合、その役割のテナント管理アクセス権を削除します。

ユーザの役割を更新する方法

1. ［管理］-［ユーザ/役割管理］をクリックします。
2. 左側の［役割管理］メニューを展開します。
3. ［役割の検索］をクリックします。
4. 役割を検索し選択します。

   役割の詳細が表示されます。
5. 役割の情報を変更します。
6. ［保存］をクリックします。

   役割が更新されます。

役割への設定の割り当て

重要: このタスクを実行するユーザが、役割管理アクセスが有効な役割に属することを確認します。

ユーザ インターフェースを設定して、ユーザによるデータの入力、管理、および検索方法を簡略化できます。 設定を役割に割り当てると、その役割に割り当てられたすべてのユーザに対して、設定したとおりに製品が表示されます。

例: アセット マネージャに設定を割り当てる

この例では、製品に入力された最も重要なアセットの情報を、アセット マネージャが迅速に表示およびモニタする必要があります。 この情報はレポート、コスト分析、および在庫管理に使用されます。 管理者は、アセット名、モデル名、数量、シリアル番号、オペレーティング システム、発注書番号、およびコスト センターを表示するように検索結果を設定します。 管理者は設定を保存し、アセット マネージャの役割にその設定を割り当てます。アセット マネージャが製品にログインすると、アセット マネージャの役割用の設定が選択され、表示されます。

注: 設定の詳細については、「ユーザ インターフェースの設定 (P. 35)」を参照してください。

役割に設定を割り当てる方法

1. ［管理］-［ユーザ/役割管理］をクリックします。
2. 左側の［役割管理］メニューを展開します。
3. ［役割の検索］をクリックします。
4. 役割を検索し選択します。

   役割の詳細が表示されます。
5. ［役割の設定］をクリックします。
6. ［新規の選択］をクリックします。

   保存された設定のリストが表示されます。
7. 役割に割り当てる設定を選択します。
8. ［OK］をクリックします。
9. ［保存］をクリックします。

   設定が役割に割り当てられます。 役割に割り当てられたユーザが製品にログインすると、この設定が表示されます。

ユーザの役割の削除

重要: このタスクを実行するユーザが、役割管理アクセスが有効な役割に属することを確認します。

サイトまたは組織で役割が使用されていない場合や役割の機能が不要になった場合は、役割を削除できます。ただし、事前定義済みのシステム管理者役割 (P. 20)は削除できません。

注: 役割を削除する前に、役割に割り当てられたユーザがいないことを確認してください。ベスト プラクティスとして、役割を削除する前にその役割からすべてのユーザを削除します。

ユーザの役割を削除する方法

1. ［管理］-［ユーザ/役割管理］をクリックします。
2. 左側の［役割管理］メニューを展開します。
3. ［役割の検索］をクリックします。
4. 役割を検索し選択します。

   役割の詳細が表示されます。

5. ［削除］をクリックし、役割を削除することを確認します。
6. ［保存］をクリックします。

   選択した役割が削除されます。

認証

*認証*は、認証情報を検証してユーザの存在を確認するために、名前とパスワードなどのユーザの識別認証情報を取得するプロセスです。 認証情報が有効な場合、ユーザが認証されます。 ユーザが認証されると、認証プロセスはユーザが製品にログインできるかどうかを決定します。

注: CA APM は CA EEM を使用してユーザ認証を処理します。

サポートされている認証のタイプは、以下のとおりです。

- フォーム認証。 ユーザが製品にログインする際、ユーザ名とパスワードの入力を求められます。

  注: フォーム認証はデフォルト認証タイプです。
- Windows 統合認証。 Windows ドメインにログイン済みのユーザは、追加のログイン認証情報を提供することなく製品にアクセスできます。

注: セキュリティを強化するには、製品内のタブおよびメニュー設定を定義して、ユーザがアクセスできるページおよびタブを制限します。

関連項目:

シングル サインオン (P. 31)

フォーム認証の設定

重要: このタスクを実行するユーザが、システム設定アクセスが有効な役割に属することを確認します。

フォーム認証を設定すると、ユーザがログインするときにユーザ名とパスワードの入力を要求できます。

フォーム認証の設定方法

1. ［管理］-［システム構成］をクリックします。
2. 左側の［EEM］をクリックします。

3. ［認証タイプ］ドロップダウン リストから、［フォーム］を選択します。
4. ［保存］をクリックします。

   フォーム認証が有効になります。

Windows 統合認証の設定

重要: このタスクを実行するユーザが、システム設定アクセスが有効な役割に属することを確認します。

Windows 統合認証を設定すると、CA EEM サーバから認証に使用する Active Directory を参照できます。 Windows 統合認証を有効にすると、Windows ドメインにログイン済みのユーザは、追加のログイン認証情報を提供することなく製品にアクセスできます。

また、CA EEM および CA SiteMinder との Windows 統合認証を設定できます。 CA SiteMinder は、認証に Active Directory を使用します。この設定の詳細については、CA EEM 製品マニュアルを参照してください。

注: Windows 統合認証が正常に機能するには、CA EEM サーバ、Active Directory、および認証リクエストを行うクライアント コンピュータが同じドメインに属している必要があります。 また、Active Directory 内に存在するユーザ名を持つユーザを CA EEM ローカル ストア内に作成して許可すると、対応する Active Directory ユーザが自動的に許可されます。

Windows 統合認証の設定方法

1. CA EEM がインストールされているコンピュータで、Active Directory または LDAP システムを参照するように CA EEM サーバを設定します。

   注: これらの機能の実行については、CA EEM 製品マニュアルを参照してください。
2. CA APM で、［管理］-［システム構成］をクリックします。
3. 左側の［EEM］をクリックします。
4. ［認証タイプ］ドロップダウン リストから、［Windows 統合］を選択します。
5. ［保存］をクリックします。

   Windows 統合認証が有効になります。

シングル サインオン

*シングル サインオン*は、ユーザが 1 つのユーザ ID とパスワードを入力するだけで、組織内の多くのリソースにアクセスできる認証処理です。シングル サインオンでは、ソリューションを切り替える際に追加の認証情報を入力する手間が省けます。

シングル サインオンにより、ユーザは Windows ログイン情報を使用して自動的に製品にログインできます。 任意の役割にユーザ ID を追加すると、ユーザのログイン認証情報が確認され、適切なホーム ページが表示されます。

注: シングル サインオンを正しく機能させるには、ローカル ユーザ アカウントではなくドメイン ユーザ アカウントとして Windows ユーザ アカウントを設定する必要があります。

セキュリティの検索

デフォルト検索を使用して、リポジトリ内のオブジェクトを検索できます。 たとえば、デフォルト検索を使用して、アセット、モデル、連絡先などを検索できます。 デフォルト検索のセキュリティでは、すべてのユーザおよび設定がデフォルト検索を使用できます。 これらの検索を使用して、追加の検索を作成できます。

一方、検索を使用するユーザを制限するために、作成した検索にセキュリティを適用できます。設定した検索を保存するときに、特定のユーザ 役割および設定を選択できます（管理者に限る）。 デフォルトでは、作成した検索のセキュリティでは、すべてのユーザおよび設定に対して利用可能になっています。 作成した検索に一意のセキュリティを適用することで、検索によって返される機密情報が特定のユーザに対して表示されないように制御できます。

検索にセキュリティを適用する場合は、以下の点を考慮します。

- 管理者はすべての検索（デフォルト検索およびユーザ定義検索）にアクセスできるため、ユーザの検索を設定およびトラブルシューティングできます。
- 管理者はすべてのスケジュール済み検索にアクセスしてエクスポートできるため、スケジュール済みの検索を設定およびトラブルシューティングして、ユーザ用にエクスポートできます。
- 役割と設定に割り当てられているすべてのユーザは、その役割と設定に割り当てられたユーザ定義検索とデフォルト検索を使用できます。 ただし、デフォルト検索結果には、管理者が非表示にして保護している情報およびフィールドは表示されません。
- 設定の変更によりデフォルト検索とユーザ定義検索が無効になると、検索が不要になる場合があります。 CA APM 内のすべてのデフォルト検索およびユーザ定義検索を削除できます。

関連項目:

検索のセキュリティのトラブルシューティング (P. 32)

検索のセキュリティのトラブルシューティング

設定された検索を操作するときに役立つ、検索のセキュリティに関するトラブルシューティングのヒントです。

設定された検索に役割を割り当てられない

すべてのサポートされているオペレーティング環境で有効です。

問題の状況:

設定された検索へのアクセス権を役割に付与しようとすると、以下のようなエラーのいずれかが表示されます。

役割<役割名>はフィールド（アセットタイプ<アセットファミリ>の<フィールド名>）にアクセスできないため、検索に割り当てることができません。

役割<役割名>はアセットタイプ<アセットファミリ>にアクセスできないため、検索に割り当てることができません。

役割<役割名>はフィールド：<フィールド名>、<フィールド名>にアクセスできないため、検索に割り当てることができません。

解決方法:

このエラーを解決するには、以下のいずれかのソリューションを使用します。

1. 設定を更新し、検索へのアクセス権を役割またはユーザに付与する。
2. 設定を更新し、検索から非表示フィールドを削除する。
3. 役割に対して検索へのアクセスを許可しない。
4. 役割から設定を削除する。

設定された検索に設定を割り当てられない

すべてのサポートされているオペレーティング環境で有効です。

問題の状況:

設定された検索へのアクセス権をグローバルまたはローカル設定に付与しようとすると、以下のようなエラーのいずれかが表示されます。

設定<設定名>は次のフィールド（アセットタイプ<アセットファミリ>の<フィールド名>）にアクセスできないため、検索に割り当てることができません。

設定<設定名>は次のフィールド（アセットタイプ<アセットファミリ>）にアクセスできないため、検索に割り当てることができません。

設定<設定名>は次のフィールド（<フィールド名>、<フィールド名>）にアクセスできないため、検索に割り当てることができません。

解決方法:

このエラーを解決するには、以下のいずれかのソリューションを使用します。

1. 設定を更新し、検索で非表示フィールドを利用可能にする。
2. 設定を更新し、検索から非表示フィールドを削除する。
3. 設定に対して検索へのアクセスを許可しない。

第 3 章: ユーザ インターフェースの設定

このセクションには、以下のトピックが含まれています。

設定

管理者はユーザ インターフェースを設定して、ユーザによるデータの入力、管理、および検索方法を簡略化し、許可されていないタスクをユーザが実行できないようにして、IT アセット管理プラクティスに準拠することができます。ユーザ インターフェースを設定すると、管理者および設定変更の影響を受けるすべてのユーザに対して、ただちに表示が変更されます。たとえば、アセット マネージャ以外のすべてのユーザに対して、サイトと会社の情報を参照できないようにする必要があるとします。そのため、［サイト］タブと［会社］タブを非表示にし、アセット マネージャの役割に割り当てられたユーザのみにそれらのタブを表示するように指定します。

ユーザ インターフェースを設定する場合、以下のタイプの設定を使用します。

- **グローバル設定**。 役割に関係なく、すべてのユーザを対象に製品を設定します。

  *グローバル設定*では、実装されている製品の機能を修正できます。 すべてのユーザや役割ごとに設定を変更する必要がなくなり、使用する実装に応じてページ、オブジェクト、フィールドなどの設定に集中できます。

  たとえば、連絡先の管理機能が不要だとします。 この場合、［連絡先］ページでグローバル設定を定義し、この機能をすべてのユーザに対して非表示にして、グローバル設定を保存します。 その結果、グローバル設定を上書きするローカル設定を定義しない限り、どのユーザにも［連絡先］ページは表示されません。

  グローバル設定は、すべてのアセット ファミリまたはリーガル テンプレート、または特定のファミリまたはテンプレートに適用できます。 使用できるグローバル設定は、すべてのファミリまたはテンプレートに適用されるもの、または特定のファミリまたはテンプレートに適用されるもののいずれか 1 つのみです。

  注: 実装のグローバル ユーザ インターフェースを変更しない場合、グローバル設定を定義する必要はありません。 グローバル設定を定義せずにローカル設定を定義することができます。

- **ローカル設定**。 特定のユーザおよび役割を対象に製品を設定します。

  *ローカル設定*を使用すると、さまざまなユーザおよび役割の要件とニーズに基づいてユーザ インターフェース ページを設定できます。

  注: ローカル設定変更はグローバル設定変更よりも優先されます。

  たとえば、実装で連絡先の管理機能を非表示にするようにグローバル設定を定義します。 ただし特定の役割のユーザは、連絡先情報を参照して更新できるようにする必要があります。 この場合、［連絡先］ページでローカル設定を定義し、連絡先情報を表示させて、ローカル設定を保存します。 このローカル設定を割り当てられた役割のユーザは、連絡先情報を参照できます。

  ローカル設定は、すべてのアセット ファミリまたはリーガル テンプレート、または特定のファミリまたはテンプレートに適用できます。 すべてのファミリまたはテンプレートに適用される、または特定のファミリまたはテンプレートに適用される複数のローカル設定を使用できます。 役割には、すべてのファミリまたはテンプレートに適用される、または特定のファミリまたはテンプレートに適用されるローカル設定を 1 つのみ割り当てることができます。

重要: 役割にグローバル設定を割り当てることはできません。 デフォルトでは、ユーザがログインして役割のセキュリティ権限を判断する際に、グローバル設定がすべての役割に割り当てられます。役割に割り当てることができるのはローカル設定のみです。

役割をローカル設定に割り当てた場合でも、グローバル設定は常にすべての役割に割り当てられます。ローカル設定によって上書きされないグローバル設定の権限はすべてその役割に適用されます。グローバル設定は（システム管理者の役割、*uapmadmin* を除く）すべてのユーザを対象に製品を設定するために使用されます。役割ごとに、より詳細なレベルでユーザ インターフェースを設定するには、ローカル設定を追加します。この場合、すべての役割のすべてユーザに対して、グローバル設定変更に基づき設定されたインターフェースが表示されます。また、ローカル設定に割り当てられたユーザには、さらに変更が加えられたインターフェースが表示されます。

ユーザがローカル設定に割り当てられている場合、そのユーザがログインするとローカル設定がその役割に割り当てられます。

アセット ファミリとリーガル テンプレートを使用したページ設定

ほとんどのオブジェクトに対して、ユーザ インターフェースを設定したり、設定を保存します。また、選択した設定に割り当てられた役割のすべてのユーザには、同じようにページが表示されます。 その他の設定オプションは使用できません。特定のオブジェクト（アセット、モデルおよびリーガル ドキュメント）については、特定の *アセット ファミリ*または *リーガル テンプレート*、*またはすべてのアセット ファミリまたはリーガル テンプレート*を選択することにより、より具体的な設定を提供できます。

ページは以下の方法で管理できます。

- アセット ファミリごとにモデル ページまたはアセット ページを設定する。（P. 39）
- リーガル テンプレートごとにリーガル ドキュメント ページを設定する（P. 39）。

例: ハードウェア アセットおよびソフトウェア アセットの設定

- （ハードウェア アセットの場合）重要なフィールド（［アセット名］、［モデル名］、［数量］、［シリアル番号］、［オペレーティング システム］、［発注番号］、および［サービス ステータス］）をページの最上部に移動し、そのフィールドを必須にして、アセットのページを設定します。 また、［ホスト名］フィールドを削除します。 設定を保存するときに、アセット ファミリで［*Hardware*］を選択します。 その結果、その設定を割り当てたユーザがハードウェア アセットを入力するときに、ユーザが設定したとおりのページが表示されます。
- （ソフトウェア アセットの場合）重要なフィールド（［アセット名］、［モデル名］、［数量］、［シリアル番号］、［部門］、［コスト センター］、および［発注番号］）をページの最上部に移動し、そのフィールドを必須にして、アセットのページを設定します。 また、［サービス ステータス］および［サービス ステータス日］フィールドを削除します。 設定を保存するときに、アセット ファミリで［*Software*］を選択します。 その結果、その設定を割り当てたユーザがソフトウェア アセットを入力するときに、ユーザが設定したとおりのページが表示されます。

例: すべてのアセット ファミリに対して設定

［請求 ID］および［発注書 ID］フィールドをアセット実行者以外のすべてのユーザに対して読み取り専用にすることにより、すべてのアセット ファミリ内のアセットのページを設定します。アセット実行者はこれらの 2 つのフィールドを編集できます。 この結果を達成するには、2 つの設定を作成します。

1. ［請求 ID］および［発注書 ID］フィールドを読み取り専用にするグローバル設定。 この設定で［すべてのファミリ］を選択すると、フィールドがすべてのアセット ファミリの［アセット］ページ上で読み取り専用になります。 このグローバル設定はすべてのユーザに適用されます。
2. ［請求 ID］および［発注書 ID］フィールドをユーザが編集できるようにするローカル設定。また、この設定で［すべてのファミリ］を選択すると、フィールドがすべてのアセット ファミリの［アセット］ページ上で編集可能になります。 このローカル設定は、アセット実行者の役割のユーザに割り当てられます。

その結果、アセット実行者でないユーザは、どのアセット ファミリの［アセット］ページ上でも［請求 ID］および［発注書 ID］フィールドを編集できなくなります。ただし、アセット実行者の役割のユーザは、すべてのアセット ファミリの［アセット］ページ上でこの 2 つのフィールドを編集できます。

例: 機密保持契約の設定

重要なフィールド（［ドキュメント識別子］、［発効日］、［終了日］、および［交渉担当者］）をページの最上部に移動し、そのフィールドを必須にして、リーガル ドキュメントのページを設定します。また、［ステータス］および［ステータスの日付］フィールドを削除します。設定を保存するときに、リーガル テンプレートで［*機密保持契約*］を選択します。 その結果、その設定を割り当てたユーザが機密保持契約を入力するときに、ユーザが設定したとおりのページが表示されます。

カスタム アセット ファミリ

追加のアセット ファミリを作成 (P. 106)してハードウェアとソフトウェア以外の製品を追跡することで、製品を拡張できます。 *カスタム アセット ファミリ*を使用すると、IT 環境内のほとんどすべての分類のアセットに関する情報を追跡できます。 たとえば、通信、サービスなどのアセット ファミリを作成できます。 カスタム アセット ファミリを作成したら、ページを設定し、カスタム アセット ファミリの設定を保存します。 その結果、そのカスタム アセット ファミリの設定を割り当てたユーザには、ユーザが設定したとおりのページが表示されます。

アセット ファミリごとのモデル ページまたはアセット ページの設定

モデル ページまたはアセット ページは、特定のアセット ファミリ（たとえばハードウェア アセットおよびソフトウェア アセット）に対して、またはすべてのアセット ファミリに対して設定できます。設定に割り当てられた役割のユーザには、設定したようにページが表示されます。

次の手順に従ってください:

1. ［モデル］または［アセット］タブをクリックします。
2. 左側の［設定: オン］をクリックします。

   ページの設定が有効になります。
3. ページの［構成情報］領域で、アセット ファミリを選択するか、［すべてのファミリ］を選択します。

   注: グローバル設定を作成していて、グローバル設定がすでにすべてのファミリに存在する場合、［すべてのファミリ］フィールドは表示されません。
4. 新しいグローバルまたはローカル設定 (P. 35)の情報を指定するか、または変更する既存の設定を選択します。

   重要: グローバル設定の変更は、役割にかかわらず、すべてのユーザに影響します。 ローカル設定の変更は、選択した設定に割り当てられている役割内のユーザのみに影響します。
5. 以下のいずれかの手順に従います。
   - フィールド ラベルを変更します (P. 53)。
   - フィールドを新しいロケーションに移動します (P. 53)。
   - フィールドを読み取り専用、必須、またはオプションにします (P. 55)。
   - フィールドを非表示にします (P. 56)。
   - 以前に非表示に設定されたフィールドを表示します (P. 57)。
   - フィールドを追加します (P. 59)。
6. ［設定の保存］をクリックします。

   設定を役割に割り当てる (P. 27)と、その役割のユーザには設定したとおりのページが表示されます。

リーガル テンプレートごとのリーガル ドキュメント ページの設定

特定のリーガル テンプレート（たとえば機密保持契約）、またはすべてのリーガル テンプレートの［リーガル ドキュメント］ページを設定できます。 設定に割り当てられた役割のユーザには、設定したようにページが表示されます。

次の手順に従ってください:

1. ［リーガル ドキュメント］ページをクリックします。
2. 左側の［設定: オン］をクリックします。

   ページの設定が有効になります。
3. ページの［構成情報］領域で、リーガル テンプレートを選択するか、［すべてのファミリ］を選択します。

   注: グローバル設定を作成していて、グローバル設定がすでにすべてのテンプレートに存在する場合、［すべてのテンプレート］フィールドは表示されません。
4. 新しいグローバルまたはローカル設定 (P. 35)の情報を指定するか、または変更する既存の設定を選択します。

   重要: グローバル設定の変更は、役割にかかわらず、すべてのユーザに影響します。 ローカル設定の変更は、選択した設定に割り当てられている役割内のユーザのみに影響します。
5. 以下のいずれかの手順に従います。
   - フィールド ラベルを変更します (P. 53)。
   - フィールドを新しいロケーションに移動します (P. 53)。
   - フィールドを読み取り専用、必須、またはオプションにします (P. 55)。
   - フィールドを非表示にします (P. 56)。
   - 以前に非表示に設定されたフィールドを表示します (P. 57)。
   - フィールドを追加します (P. 59)。
6. ［設定の保存］をクリックします。

   設定を役割に割り当てる (P. 27)と、その役割のユーザには設定したとおりのページが表示されます。

ユーザ インターフェースの設定方法

ユーザ インターフェースを設定するには、以下のタスクを実行します。

- オブジェクト アクセス設定 (P. 41)と、タブおよびメニュー設定 (P. 46)を使用して、許可されていないタスクをユーザが実行できないようにする。
- フィールド設定 (P. 52)を使用して、ユーザが管理するオブジェクトの情報を入力しやすくする。
- フィールド データ検証設定 (P. 66)を使用して、フィールド フォーマットとデータ入力の要件を検証および適用します。

- ハイパーリンク (P. 68)およびボタン設定 (P. 70)を使用して、許可されていないタスクをユーザが実行できないようにする。
- 拡張フィールド設定 (P. 73)を使用して、より多くのデータを格納できるようにリポジトリを拡張する。
- 参照フィールド設定 (P. 75)を使用して、製品を拡張し、ユーザが管理するオブジェクト情報の入力方法を強化する。
- 階層設定 (P. 84)を使用して、製品を拡張し、オブジェクトのより多くの情報および詳細を追跡できるようにする。
- ページ設定 (P. 37)を使用して、ファミリとリーガル テンプレートによるモデル、アセットおよびリーガル ドキュメントの情報を入力しやすくする。
- 検索設定 (P. 87)を使用して、検索時に管理対象のオブジェクトを見つけやすくする。
- リーガル テンプレート設定 (P. 102)を使用して、リーガル ドキュメントの情報を入力しやすくする。
- イベントおよび通知設定 (P. 103)を使用して、予定されているイベントについてユーザに通知し、適切なタスクが適切なタイミングおよび正しい順序で実行されるようにする。
- リスト管理 (P. 106)を使用して、リストから正しい項目を選択しやすくする。
- カスタム関係 (P. 109)を使用して、製品を拡張し、ユーザがオブジェクト情報を管理する方法を強化する。

オブジェクト アクセス設定

オブジェクト アクセスを設定すると、データの整合性を保護し、許可されていないタスクをユーザが実行するのを防ぎ、ユーザの職務権限に関連する情報のみをユーザに提供することができます。以下の方法でオブジェクト アクセスを設定できます。

- オブジェクトを非表示にする (P. 42)。ユーザがモデルの価格情報を参照できないようにする必要があります。 そのため、［モデル］ページの［部品と価格］領域を非表示にします。
- オブジェクトを表示する (P. 43)。ユーザがモデルの価格情報を参照できるようにする必要があります。 そのため、［モデル］ページの［部品と価格］領域を表示します。

- オブジェクトを読み取り専用にする (P. 44)。ユーザがモデルの価格情報を参照できるが変更できないようにする必要があります。 そのため、［モデル］ページの［部品と価格］領域を読み取り専用にします。
- オブジェクトをアクセス可能にする (P. 44)。ユーザがモデルの価格情報を参照および編集できるようにする必要があります。 そのため、［モデル］ページの［部品と価格］領域をアクセス可能にします。
- オブジェクトを保護するためにユーザに権限を付与する (P. 45)。

オブジェクト アクセスとフィールド設定を組み合わせて、より詳細なレベルの権限を適用できます。

オブジェクトを非表示にする

ユーザがオブジェクトのページの特定の領域を参照できないように、オブジェクトを非表示にできます。

オブジェクトを非表示にする方法

1. 設定するオブジェクトのタブおよびオプションのサブタブをクリックします。
2. 左側の［設定: オン］をクリックします。

   ページの設定が有効になります。
3. ページの［構成情報］領域で、以下の手順に従います。
   a. 新しいグローバルまたはローカル設定の情報を指定するか、または変更する既存の設定を選択します。
   b. （オプション）［オブジェクト］ドロップダウン リストで、設定するオブジェクトの一部を選択します。 権限の変更（フィールドの移動権限を拒否するなど）は、オブジェクトのその部分にのみ適用されます。

      たとえば、リーガル ドキュメントを設定する場合、［オブジェクト］ドロップダウン リストで［リーガル ドキュメント ステータス履歴］を選択します。オブジェクトの該当する部分（ステータス履歴）に対して、フィールドの移動権限が拒否されます。 権限の変更は、ステータス履歴部分のみに適用され、オブジェクトの他の部分には適用されません。

      重要: グローバル設定変更は、ユーザの役割にかかわらずすべてのユーザに影響します。 ローカル設定変更は、選択した設定に割り当てられた役割のユーザのみに影響します。

4. ページの領域（たとえば、［モデル］ページの［部品と価格］）のタイトルの右横にある［権限の許可］アイコンをクリックします。

   オブジェクトに対して［権限の拒否］アイコンが表示されます。

5. ［設定の保存］をクリックします。

   役割に設定を割り当てると、その役割のユーザはオブジェクト情報を参照できません。

オブジェクトを表示する

ユーザが特定のオブジェクトを参照する必要がある場合、オブジェクトを表示させることができます。

オブジェクトを表示する方法

1. 設定するオブジェクトのタブおよびオプションのサブタブをクリックします。
2. 左側の［設定: オン］をクリックします。

   ページの設定が有効になります。

3. ページの［構成情報］領域で、以下の手順に従います。
   a. 新しいグローバルまたはローカル設定の情報を指定するか、または変更する既存の設定を選択します。
   b. （オプション）［オブジェクト］ドロップダウン リストで、設定するオブジェクトの一部を選択します。 権限の変更（フィールドの移動権限を拒否するなど）は、オブジェクトのその部分にのみ適用されます。

      たとえば、リーガル ドキュメントを設定する場合、［オブジェクト］ドロップダウン リストで［リーガル ドキュメント ステータス履歴］を選択します。オブジェクトの該当する部分（ステータス履歴）に対して、フィールドの移動権限が拒否されます。 権限の変更は、ステータス履歴部分のみに適用され、オブジェクトの他の部分には適用されません。

   重要: グローバル設定変更は、ユーザの役割にかかわらずすべてのユーザに影響します。 ローカル設定変更は、選択した設定に割り当てられた役割のユーザのみに影響します。

4. オブジェクトへのアクセスがすでに拒否されている場合は、ページの領域（たとえば、［モデル］ページの［部品と価格］）のタイトルの右横にある［権限の拒否］アイコンをクリックします。

   オブジェクトに対して［権限の許可］アイコンが表示されます。

5. ［設定の保存］をクリックします。

   役割に設定を割り当てると、その役割のユーザはオブジェクト情報を参照できます。

オブジェクトを読み取り専用にする

ユーザが特定のオブジェクトを参照できるが変更できないようにする必要がある場合、オブジェクトを読み取り専用にすることができます。

オブジェクトを読み取り専用にする

1. 設定するオブジェクトのタブおよびオプションのサブタブをクリックします。
2. 左側の［設定: オン］をクリックします。

   ページの設定が有効になります。
3. ページの［構成情報］領域で、以下の手順に従います。
   a. 新しいグローバルまたはローカル設定の情報を指定するか、または変更する既存の設定を選択します。
   b. （オプション）［オブジェクト］ドロップダウン リストで、設定するオブジェクトの一部を選択します。 権限の変更（フィールドの移動権限を拒否するなど）は、オブジェクトのその部分にのみ適用されます。

      たとえば、リーガル ドキュメントを設定する場合、［オブジェクト］ドロップダウン リストで［リーガル ドキュメント ステータス履歴］を選択します。オブジェクトの該当する部分（ステータス履歴）に対して、フィールドの移動権限が拒否されます。 権限の変更は、ステータス履歴部分のみに適用され、オブジェクトの他の部分には適用されません。

   重要: グローバル設定変更は、ユーザの役割にかかわらずすべてのユーザに影響します。 ローカル設定変更は、選択した設定に割り当てられた役割のユーザのみに影響します。
4. ページの領域（たとえば、［モデル］ページの［部品と価格］）のタイトルの右横にある［編集可能］アイコンをクリックします。

   オブジェクトに対して［読み取り専用］アイコンが表示されます。
5. ［設定の保存］をクリックします。

   役割に設定を割り当てると、その役割のユーザはオブジェクト情報を参照できますが変更はできません。

オブジェクトをアクセス可能にする

ユーザが特定のオブジェクトに関する情報を参照および変更できるようにする必要がある場合、オブジェクトをアクセス可能にすることができます。

オブジェクトをアクセス可能にする方法

1. 設定するオブジェクトのタブおよびオプションのサブタブをクリックします。
2. 左側の［設定: オン］をクリックします。

   ページの設定が有効になります。
3. ページの［構成情報］領域で、以下の手順に従います。
   a. 新しいグローバルまたはローカル設定の情報を指定するか、または変更する既存の設定を選択します。
   b. （オプション）［オブジェクト］ドロップダウン リストで、設定するオブジェクトの一部を選択します。 権限の変更（フィールドの移動権限を拒否するなど）は、オブジェクトのその部分にのみ適用されます。

      たとえば、リーガル ドキュメントを設定する場合、［オブジェクト］ドロップダウン リストで［リーガル ドキュメント ステータス履歴］を選択します。オブジェクトの該当する部分（ステータス履歴）に対して、フィールドの移動権限が拒否されます。 権限の変更は、ステータス履歴部分のみに適用され、オブジェクトの他の部分には適用されません。

   重要: グローバル設定変更は、ユーザの役割にかかわらずすべてのユーザに影響します。 ローカル設定変更は、選択した設定に割り当てられた役割のユーザのみに影響します。
4. オブジェクトがすでに読み取り専用である場合は、ページの領域（たとえば、［モデル］ページの［部品と価格］）のタイトルの右横にある［読み取り専用］アイコンをクリックします。

   オブジェクトに対して［編集可能］アイコンが表示されます。
5. ［設定の保存］をクリックします。

   役割に設定を割り当てると、その役割のユーザはオブジェクト情報にアクセスできます。

オブジェクトを保護するために権限を付与する

ユーザ インターフェースの設定、オブジェクトの表示/非表示の設定、オブジェクトの読み取り専用/アクセス可能の設定ができるように、ユーザに権限を付与できます。

オブジェクトを保護するために権限を付与する方法

1. 設定するオブジェクトのタブおよびオプションのサブタブをクリックします。
2. 左側の［設定: オン］をクリックして、ページの設定を有効にします。

3. ページの［構成情報］領域で、新しいグローバルまたはローカル設定の情報を指定するか、または変更する既存の設定を選択します。

   重要: グローバル設定変更は、ユーザの役割にかかわらずすべてのユーザに影響します。 ローカル設定変更は、選択した設定に割り当てられた役割のユーザのみに影響します。

4. ページの［許可］領域で、［保護 (読み取り専用およびアクセス)］を［権限の許可］リストに移動します。

5. （オプション）［親オブジェクトから権限を継承］チェック ボックスをオンにすると、最上位の（親）オブジェクトからより下位の（子）オブジェクトに、同じ設定を使用してセキュリティ権限を適用できます。

   たとえば、組織のローカル設定を作成するとします。 この設定では、フィールド ラベルの変更、フィールドの移動、フィールドを必須にする、フィールドを非表示にする権限を拒否します。 設定を保存してから、［組織］の［添付ファイル］を開き、［親オブジェクトから権限を継承］チェック ボックスをオンにします。組織のすべての権限が添付ファイルに適用されます。 この例では、フィールド ラベルの変更、フィールドの移動、フィールドを必須にする、フィールドを非表示にする権限が組織に適用されているため、これらの権限は添付ファイルにも適用されます。

6. ［設定の保存］をクリックします。

   役割に設定を割り当てると、その役割のユーザはオブジェクトの表示/非表示の設定、オブジェクトの読み取り専用/アクセス可能の設定ができるようになります。

タブおよびメニューの設定

タブおよびメニューのアクセスを設定すると、オブジェクトのデータの整合性を確保したり、ユーザが許可されていないタスク（オブジェクト情報の追加や削除など）を実行できないようにしたり、ユーザ固有の職務に適した情報のみを参照できるように役割を分担したりできます。

注: アセット、モデル、およびリーガル ドキュメントについては、アセット ファミリ（アセットおよびモデル）とリーガル テンプレート（リーガル ドキュメント）を指定して、固有の設定を定義できます。

以下の方法で、タブおよびメニューのアクセスを設定できます。

- タブを非表示にする (P. 47)。リーガル ドキュメントの情報をユーザがまったく参照できないようにする必要があります。そのため、［リーガル ドキュメント］タブを非表示にします。
- タブを表示する (P. 48)。リーガル ドキュメントの情報をユーザがすべて参照できるようにする必要があります。 そのため、［リーガル ドキュメント］タブを表示させます。

- タブを読み取り専用にする (P. 48)。ユーザがモデルの情報を参照できるが変更できないようにする必要があります。 そのため、［モデル］タブを読み取り専用にします。
- タブをアクセス可能にする (P. 49)。ユーザがモデルのすべての情報を参照および編集できるようにする必要があります。 そのため、［モデル］タブをアクセス可能にします。
- メニュー オプションを非表示にする (P. 50)。ユーザがモデルの依存関係を参照できないようにする必要があります。 そのため、［依存関係］メニュー オプションを非表示にします。
- メニュー オプションを表示する (P. 50)。ユーザがモデルの依存関係を参照できるようにする必要があります。 そのため、［依存関係］メニュー オプションを表示させます。
- メニュー オプションを読み取り専用にする (P. 51)。ユーザがモデルの特記事項を変更できないようにする必要があります。 そのため、［特記事項］メニュー オプションを読み取り専用にします。
- メニュー オプションをアクセス可能にする (P. 51)。ユーザがモデルの汎用構成を変更できるようにする必要があります。 そのため、［モデル構成］メニュー オプションをアクセス可能にします。

タブおよびメニュー設定とフィールド設定を組み合わせて、より詳細なレベルの権限を適用できます。

タブを非表示にする

ユーザが特定のタブを参照できないようにする必要がある場合、タブを非表示にすることができます。

タブを非表示にする方法

1. 設定するオブジェクト アクセスのタブおよびオプションのサブタブをクリックします。
2. 左側の［設定: オン］をクリックします。

   オブジェクト アクセスの設定が有効になります。

3. ページの［構成情報］領域で、新しいグローバルまたはローカル設定の情報を指定するか、または変更する既存の設定を選択します。

   重要: グローバル設定変更は、ユーザの役割にかかわらずすべてのユーザに影響します。 ローカル設定変更は、選択した設定に割り当てられた役割のユーザのみに影響します。

4. タブで［権限の許可］アイコンをクリックします。

   タブに対して［権限の拒否］アイコンが表示されます。

5. ［設定の保存］をクリックします。

   役割に設定を割り当てると、その役割のユーザはタブを参照できません。

タブを表示する

ユーザに特定のタブを表示する必要がある場合、タブを表示させることができます。

タブを表示する方法

1. 設定するオブジェクト アクセスのタブおよびオプションのサブタブをクリックします。
2. 左側の［設定: オン］をクリックします。

   オブジェクト アクセスの設定が有効になります。

3. ページの［構成情報］領域で、新しいグローバルまたはローカル設定の情報を指定するか、または変更する既存の設定を選択します。

   重要: グローバル設定変更は、ユーザの役割にかかわらずすべてのユーザに影響します。 ローカル設定変更は、選択した設定に割り当てられた役割のユーザのみに影響します。

4. タブがすでに非表示にされている場合は、タブ上の［権限の拒否］アイコンをクリックします。

   タブに対して［権限の許可］アイコンが表示されます。

5. ［設定の保存］をクリックします。

   役割に設定を割り当てると、その役割のユーザはタブを参照できます。

タブを読み取り専用にする

ユーザが特定のタブの情報を参照できるが変更できないようにする必要がある場合、タブを読み取り専用にすることができます。

タブを読み取り専用にする方法

1. 設定するオブジェクト アクセスのタブおよびオプションのサブタブをクリックします。
2. 左側の［設定: オン］をクリックします。

   オブジェクト アクセスの設定が有効になります。
3. ページの［構成情報］領域で、新しいグローバルまたはローカル設定の情報を指定するか、または変更する既存の設定を選択します。

   重要: グローバル設定変更は、ユーザの役割にかかわらずすべてのユーザに影響します。 ローカル設定変更は、選択した設定に割り当てられた役割のユーザのみに影響します。
4. タブで、［編集可能］アイコンをクリックします。

   タブに対して［読み取り専用］アイコンが表示されます。
5. ［設定の保存］をクリックします。

   役割に設定を割り当てると、その役割のユーザはタブの情報を変更できません。

タブをアクセス可能にする

ユーザがタブの情報を表示したり変更できるようにする必要がある場合は、タブをアクセス可能にすることができます。

タブをアクセス可能にする方法

1. 設定するオブジェクト アクセスのタブおよびオプションのサブタブをクリックします。
2. 左側の［設定: オン］をクリックします。

   オブジェクト アクセスの設定が有効になります。
3. ページの［構成情報］領域で、新しいグローバルまたはローカル設定の情報を指定するか、または変更する既存の設定を選択します。

   重要: グローバル設定変更は、ユーザの役割にかかわらずすべてのユーザに影響します。 ローカル設定変更は、選択した設定に割り当てられた役割のユーザのみに影響します。
4. タブがすでに読み取り専用に設定されている場合は、タブの［読み取り専用］アイコンをクリックします。

   タブに［編集可能］アイコンが表示されます。
5. ［設定の保存］をクリックします。

   設定を役割に割り当てると、その役割のユーザはタブの情報にアクセスできるようになります。

メニュー オプションの非表示

ユーザがすべてまたは特定のメニュー オプションを参照できないようにする必要がある場合は、メニュー オプションを非表示にすることができます。

メニュー オプションを非表示にする方法

1. 設定するオブジェクト アクセスのタブおよびオプションのサブタブをクリックします。
2. 左側の［設定: オン］をクリックします。

   オブジェクト アクセスの設定が有効になります。
3. ページの［構成情報］領域で、新しいグローバルまたはローカル設定の情報を指定するか、または変更する既存の設定を選択します。

   重要: グローバル設定変更は、ユーザの役割にかかわらずすべてのユーザに影響します。 ローカル設定変更は、選択した設定に割り当てられた役割のユーザのみに影響します。
4. メニューまたはメニュー オプションで、［権限の許可］アイコンをクリックします。

   メニューまたはメニュー オプションに［権限の拒否］アイコンが表示されます。
5. ［設定の保存］をクリックします。

   設定を役割に割り当てると、その役割のユーザはメニュー オプションを参照できなくなります。

メニュー オプションの表示

ユーザがすべてまたは特定のメニュー オプションを参照できるようにする必要がある場合は、メニュー オプションを表示することができます。

メニュー オプションを表示する方法

1. 設定するオブジェクト アクセスのタブおよびオプションのサブタブをクリックします。
2. 左側の［設定: オン］をクリックします。

   オブジェクト アクセスの設定が有効になります。
3. ページの［構成情報］領域で、新しいグローバルまたはローカル設定の情報を指定するか、または変更する既存の設定を選択します。

   重要: グローバル設定変更は、ユーザの役割にかかわらずすべてのユーザに影響します。 ローカル設定変更は、選択した設定に割り当てられた役割のユーザのみに影響します。

4. メニューまたはメニュー オプションがすでに非表示に設定されている場合は、メニューまたはメニュー オプションの［権限の拒否］アイコンをクリックします。

   メニューまたはメニュー オプションに［権限の許可］アイコンが表示されます。

5. ［設定の保存］をクリックします。

   設定を役割に割り当てると、その役割のユーザはメニュー オプションを表示して使用できるようになります。

メニュー オプションの読み取り専用化

ユーザが特定のメニュー オプションを参照できるが使用できないようにする必要がある場合は、メニュー オプションを読み取り専用にすることができます。

メニュー オプションを読み取り専用にする方法

1. 設定するオブジェクト アクセスのタブおよびオプションのサブタブをクリックします。
2. 左側の［設定: オン］をクリックします。

   オブジェクト アクセスの設定が有効になります。
3. ページの［構成情報］領域で、新しいグローバルまたはローカル設定の情報を指定するか、または変更する既存の設定を選択します。

   重要: グローバル設定変更は、ユーザの役割にかかわらずすべてのユーザに影響します。 ローカル設定変更は、選択した設定に割り当てられた役割のユーザのみに影響します。
4. メニューまたはメニュー オプションで、［編集可能］アイコンをクリックします。

   メニュー オプションに［読み取り専用］アイコンが表示されます。
5. ［設定の保存］をクリックします。

   設定を役割に割り当てると、その役割のユーザはメニュー オプションを表示できますが、メニュー オプションを使用できなくなります。

メニュー オプションへのアクセスの有効化

ユーザが特定のメニュー オプションを参照して使用できるようにする必要がある場合は、メニュー オプションをアクセス可能にすることができます。

メニュー オプションをアクセス可能にする方法

1. 設定するオブジェクト アクセスのタブおよびオプションのサブタブをクリックします。
2. 左側の［設定: オン］をクリックします。

   オブジェクト アクセスの設定が有効になります。
3. ページの［構成情報］領域で、新しいグローバルまたはローカル設定の情報を指定するか、または変更する既存の設定を選択します。

   重要: グローバル設定変更は、ユーザの役割にかかわらずすべてのユーザに影響します。 ローカル設定変更は、選択した設定に割り当てられた役割のユーザのみに影響します。
4. メニューまたはメニュー オプションがすでに読み取り専用に設定されている場合は、メニューまたはメニュー オプションの［読み取り専用］アイコンをクリックします。

   メニュー オプションに［編集可能］アイコンが表示されます。
5. ［設定の保存］をクリックします。

   設定を役割に割り当てると、その役割のユーザはメニュー オプションを表示して使用できるようになります。

フィールドの設定

アセット管理プラクティスに準拠するようにページのフィールド情報の表示および属性を変更し、ユーザによる管理対象オブジェクトの情報入力を簡略化できます。 この製品では、これらのフィールドを*設定フィールド*と呼びます。

フィールドは以下の方法で管理できます。

- フィールド ラベルを変更します (P. 53)。
- ページ上の新しい場所にフィールドを移動する (P. 53)。
- フィールドを読み取り専用、必須、またはオプションにします (P. 55)。
- フィールドを非表示にします (P. 56)。
- 以前に非表示に設定されたフィールドを表示します (P. 57)。
- フィールドを追加します (P. 59)。

- フィールド ラベルを変更する (P. 60)、フィールドを移動する (P. 61)、フィールドを必須にする (P. 62)、フィールドを非表示にする (P. 63)、および大量変更を実行する (P. 64) 権限を付与します。
- フィールド情報を表示する (P. 65)。

注: さらに大幅にフィールドを変更するには、ユーザがフィールドのすべての属性を定義できる拡張フィールドを作成 (P. 73) します。

フィールド ラベルの変更

フィールドをユーザが使いやすくしたり、IT のアセット管理の実務に合うように、フィールド ラベルを変更できます。

フィールド ラベルを変更する方法

1. 設定するオブジェクトのタブおよびオプションのサブタブをクリックします。
2. 左側の［設定: オン］をクリックします。

   ページの設定が有効になります。
3. ページの［構成情報］領域で、以下の手順に従います。
   a. 新しいグローバルまたはローカル設定の情報を指定するか、または変更する既存の設定を選択します。
   b. （オプション）［オブジェクト］ドロップダウン リストで、設定するオブジェクトの一部を選択します。 権限の変更（フィールドの移動権限を拒否するなど）は、オブジェクトのその部分にのみ適用されます。

      たとえば、リーガル ドキュメントを設定する場合、［オブジェクト］ドロップダウン リストで［リーガル ドキュメント ステータス履歴］を選択します。オブジェクトの該当する部分（ステータス履歴）に対して、フィールドの移動権限が拒否されます。 権限の変更は、ステータス履歴部分のみに適用され、オブジェクトの他の部分には適用されません。

   重要: グローバル設定変更は、ユーザの役割にかかわらずすべてのユーザに影響します。 ローカル設定変更は、選択した設定に割り当てられた役割のユーザのみに影響します。
4. フィールド ラベルをクリックし、新しいラベルを入力します。
5. ［設定の保存］をクリックします。

   設定を役割に割り当てると、その役割のユーザには新しいフィールド ラベルが表示されます。

フィールドを新しいロケーションに移動する

ユーザがページでフィールドを簡単に見つけられるように、フィールドを新しいロケーションに移動できます。

フィールドを新しいロケーションに移動する方法

1. 設定するオブジェクトのタブおよびオプションのサブタブをクリックします。
2. 左側の［設定: オン］をクリックします。

   ページの設定が有効になります。
3. ページの［構成情報］領域で、以下の手順に従います。
   a. 新しいグローバルまたはローカル設定の情報を指定するか、または変更する既存の設定を選択します。
   b. （オプション）［オブジェクト］ドロップダウン リストで、設定するオブジェクトの一部を選択します。 権限の変更（フィールドの移動権限を拒否するなど）は、オブジェクトのその部分にのみ適用されます。

      たとえば、リーガル ドキュメントを設定する場合、［オブジェクト］ドロップダウン リストで［リーガル ドキュメント ステータス履歴］を選択します。オブジェクトの該当する部分（ステータス履歴）に対して、フィールドの移動権限が拒否されます。 権限の変更は、ステータス履歴部分のみに適用され、オブジェクトの他の部分には適用されません。

   重要: グローバル設定変更は、ユーザの役割にかかわらずすべてのユーザに影響します。 ローカル設定変更は、選択した設定に割り当てられた役割のユーザのみに影響します。
4. フィールドを現在のセクションの新しいロケーションにドラッグアンドドロップします。

   注: フィールドをページの別のセクションに移動することはできません。 たとえば、［追加情報］セクションから［基本情報］セクションにフィールドを移動することはできません。
5. ［設定の保存］をクリックします。

   設定を役割に割り当てると、その役割のユーザには新しいロケーションにあるフィールドが表示されます。

フィールドを読み取り専用、必須、またはオプションにする

*必須フィールド*とは、レコードを保存する際に値を必ず含む必要があるフィールドを表します。 フィールドを設定するか拡張フィールドを作成する場合に、フィールドを読み取り専用、必須、またはオプションにすることができます。 重要なデータを含むフィールドは必須にしておくと便利です。

重要: 新しい必須フィールドを作る場合、保存済みのレコードのフィールドにはデータが含まれない場合があります。 今後レコードを保存する場合には、新しい必須フィールドにデータを入力する必要があります。 また、Web サービスを使用して作成されたアプリケーションによって既存のレコードを更新する場合も、データを入力する必要があります。 クライアント アプリケーションは、必須フィールドにデータが含まれていること、またはそのフィールドにデータが入力されていることを確認する必要があります。 データがない場合、レコードは更新されません。

フィールドを必須にする前に、既存のすべてのレコードのフィールドにデータを入力しておくことをお勧めします。 NULL またはスペース（値フィールドをクリアする）を検索すると、フィールドに空白の値を持つすべてのケースを検索できます。

フィールドを読み取り専用、必須、またはオプションにする方法

1. 設定するオブジェクトのタブおよびオプションのサブタブをクリックします。
2. 左側の［設定: オン］をクリックします。

   ページの設定が有効になります。

3. ページの［構成情報］領域で、以下の手順に従います。

   a. 新しいグローバルまたはローカル設定の情報を指定するか、または変更する既存の設定を選択します。

   b. （オプション）［オブジェクト］ドロップダウン リストで、設定するオブジェクトの一部を選択します。 権限の変更（フィールドの移動権限を拒否するなど）は、オブジェクトのその部分にのみ適用されます。

      たとえば、リーガル ドキュメントを設定する場合、［オブジェクト］ドロップダウン リストで［リーガル ドキュメント ステータス履歴］を選択します。オブジェクトの該当する部分（ステータス履歴）に対して、フィールドの移動権限が拒否されます。 権限の変更は、ステータス履歴部分のみに適用され、オブジェクトの他の部分には適用されません。

   重要: グローバル設定変更は、ユーザの役割にかかわらずすべてのユーザに影響します。 ローカル設定変更は、選択した設定に割り当てられた役割のユーザのみに影響します。

4. フィールドの横にある適切なアイコンをクリックして、フィールドを読み取り専用、必須、またはオプションに設定します。

5. ［設定の保存］をクリックします。

   設定を役割に割り当てると、その役割のユーザにはそのフィールドが読み取り専用、必須、またはオプションとして表示されます。

フィールドの非表示

ユーザがページの特定のフィールドを表示できないようにする必要がある場合は、フィールドを非表示にすることができます。

フィールドを非表示にする方法

1. 設定するオブジェクトのタブおよびオプションのサブタブをクリックします。
2. 左側の［設定: オン］をクリックします。

   ページの設定が有効になります。

3. ページの［構成情報］領域で、以下の手順に従います。

   a. 新しいグローバルまたはローカル設定の情報を指定するか、または変更する既存の設定を選択します。

   b. （オプション）［オブジェクト］ドロップダウン リストで、設定するオブジェクトの一部を選択します。 権限の変更（フィールドの移動権限を拒否するなど）は、オブジェクトのその部分にのみ適用されます。

      たとえば、リーガル ドキュメントを設定する場合、［オブジェクト］ドロップダウン リストで［リーガル ドキュメント ステータス履歴］を選択します。オブジェクトの該当する部分（ステータス履歴）に対して、フィールドの移動権限が拒否されます。 権限の変更は、ステータス履歴部分のみに適用され、オブジェクトの他の部分には適用されません。

   重要: グローバル設定変更は、ユーザの役割にかかわらずすべてのユーザに影響します。 ローカル設定変更は、選択した設定に割り当てられた役割のユーザのみに影響します。

4. フィールドの横にある［フィールドの削除］アイコンをクリックします。

5. ［設定の保存］をクリックします。

   設定を役割に割り当てると、その役割のユーザにはそのフィールドが表示されなくなります。 非表示にしたフィールドにイベントが定義されている場合、ユーザは引き続き通知を受信します。 ただし、イベントに関連付けられたワークフロー プロセスにアクセスできないマップ済み属性がある場合、その属性は送信される通知には含まれません。

関連項目:

イベントおよび通知の設定 (P. 103)

以前に非表示に設定されたフィールドの表示

以前に非表示に設定されたフィールドをユーザが参照できるようにする必要がある場合は、フィールドを表示することができます。 たとえば、以前に［容量］フィールドを非表示にしたとします。 このフィールドは必須であるため、ユーザはこのフィールドを参照できる必要があります。アセットを定義するときにユーザが値を入力できるように、フィールドをもう一度追加します。

フィールドを表示する方法

1. 設定するオブジェクトのタブおよびオプションのサブタブをクリックします。
2. 左側の［設定: オン］をクリックします。

   ページの設定が有効になります。

3. ページの［構成情報］領域で、以下の手順に従います。

   a. 新しいグローバルまたはローカル設定の情報を指定するか、または変更する既存の設定を選択します。

   b. （オプション）［オブジェクト］ドロップダウン リストで、設定するオブジェクトの一部を選択します。 権限の変更（フィールドの移動権限を拒否するなど）は、オブジェクトのその部分にのみ適用されます。

      たとえば、リーガル ドキュメントを設定する場合、［オブジェクト］ドロップダウン リストで［リーガル ドキュメント ステータス履歴］を選択します。オブジェクトの該当する部分（ステータス履歴）に対して、フィールドの移動権限が拒否されます。 権限の変更は、ステータス履歴部分のみに適用され、オブジェクトの他の部分には適用されません。

   重要: グローバル設定変更は、ユーザの役割にかかわらずすべてのユーザに影響します。 ローカル設定変更は、選択した設定に割り当てられた役割のユーザのみに影響します。

4. ［非表示フィールドの表示］をクリックします。

5. 画面上の指示に従って、ページにフィールドを追加します。

6. ［設定の保存］をクリックします。

   設定を役割に割り当てると、その役割のユーザにはページの該当するフィールドが表示されます。

   注: 以前に非表示に設定されていたフィールドを表示すると、ユーザはそのフィールドのイベントを定義できるようになります。 フィールドはすでに設定に追加されているため、設定を保存する必要はありません。 イベントの管理の詳細については、ユーザ ガイドを参照してください。

フィールドの追加

リポジトリに存在するがグローバル設定には含まれないフィールド、または削除されたりアクセスが拒否されているフィールドをユーザが参照できるようにする必要がある場合は、ページにフィールドを追加できます。たとえば、以前に［アセットの詳細］ページから［chipset］という名前の拡張フィールドを削除したとします。 ユーザはこのフィールドを参照して値を入力できる必要があるため、ページにもう一度フィールドを追加します。 また、以前に拡張を追加したのにグローバル設定を保存しなかった場合は、以下の手順を使用して拡張フィールドをページに追加します。

重要: 複数のアセット ファミリ（アセットおよびモデル）とリーガル テンプレート（リーガル ドキュメント）を持つオブジェクトにフィールドを追加する場合、フィールドの追加先がファミリであるかテンプレートであるかにかかわらず、そのオブジェクトのすべてのファミリおよびテンプレートにフィールドが追加されます。 たとえば、ハードウェア アセット ファミリにフィールドを追加するとします。 フィールドは、コンピュータ、その他、プロジェクト、サービス、およびソフトウェアなどの他のすべてのアセット ファミリに追加されます。

フィールドを追加する方法

1. 設定するオブジェクトのタブおよびオプションのサブタブをクリックします。
2. 左側の［設定: オン］をクリックします。

   ページの設定が可能になります。
3. ページの［構成情報］領域で、以下の手順に従います。
   a. 新しいグローバル設定の情報を指定するか、または変更する既存のグローバル設定を選択します。
   b. （オプション）［オブジェクト］ドロップダウン リストで、設定するオブジェクトの一部を選択します。 権限の変更（フィールドの移動権限を拒否するなど）は、オブジェクトのその部分にのみ適用されます。

      たとえば、リーガル ドキュメントを設定する場合は、［オブジェクト］ドロップダウン リストの［リーガル ドキュメント ステータス履歴］を選択します。 オブジェクトの該当する部分（ステータス履歴）に対して、フィールドの移動権限が拒否されます。 権限の変更は、ステータス履歴部分のみに適用され、オブジェクトの他の部分には適用されません。

   重要: グローバル設定用のフィールドのみを追加できます。 ローカル設定用のフィールドは追加できません。
4. （オプション）［設定の保存］をクリックして、グローバル設定を作成します。
5. ［既存フィールドの追加］をクリックします。

   ウィザードが表示されます。

6. ページに追加するフィールドを選択します。

   注: 拡張フィールドの場合、拡張フィールドを定義したときに指定したオブジェクト ラベル（たとえばアセット ハードウェアの拡張など）に一致するリンクが表示されます。 リンクをクリックして、ページに追加する拡張フィールドを選択します。

7. ［設定の保存］をクリックします。

   そのページの該当するフィールドはすべてのユーザに表示されます。

   注: フィールドを追加して拡張フィールドを定義し、ローカルまたはグローバル設定にフィールドを保存すると、ユーザがフィールドのイベントを定義できます。 イベントの管理の詳細については、ユーザ ガイドを参照してください。

フィールド ラベルを変更する権限の付与

ユーザ インターフェースを設定したり、フィールド ラベルを変更できるように、ユーザに権限を付与することができます。

フィールド ラベルを変更する権限を付与する方法

1. 設定するオブジェクトのタブおよびオプションのサブタブをクリックします。
2. 左側の［設定: オン］をクリックします。

   ページの設定が有効になります。

3. ページの［構成情報］領域で、新しいグローバルまたはローカル設定の情報を指定するか、または変更する既存の設定を選択します。

   重要: グローバル設定変更は、ユーザの役割にかかわらずすべてのユーザに影響します。 ローカル設定変更は、選択した設定に割り当てられた役割のユーザのみに影響します。

4. ページの［許可］領域で、［ラベルの変更］を［権限の許可］リストに移動します。

5. （オプション）［親オブジェクトから権限を継承］チェック ボックスをオンにすると、最上位の（親）オブジェクトからより下位の（子）オブジェクトに、同じ設定を使用してセキュリティ権限を適用できます。

   たとえば、組織のローカル設定を作成するとします。 この設定では、フィールド ラベルの変更、フィールドの移動、フィールドを必須にする、フィールドを非表示にする権限を拒否します。 設定を保存してから、［組織］の［添付ファイル］を開き、［親オブジェクトから権限を継承］チェック ボックスをオンにします。 組織のすべての権限が添付ファイルに適用されます。 この例では、フィールド ラベルの変更、フィールドの移動、フィールドを必須にする、フィールドを非表示にする権限が組織に適用されているため、これらの権限は添付ファイルにも適用されます。

6. ［設定の保存］をクリックします。

   設定を役割に割り当てると、その役割のユーザにフィールド ラベルを変更する権限が付与されます。

フィールドを移動する権限の付与

ユーザ インターフェースを設定したり、フィールドを移動できるように、ユーザに権限を付与することができます。

フィールドを移動する権限を付与する方法

1. 設定するオブジェクトのタブおよびオプションのサブタブをクリックします。
2. 左側の［設定: オン］をクリックします。

   ページの設定が有効になります。

3. ページの［構成情報］領域で、新しいグローバルまたはローカル設定の情報を指定するか、または変更する既存の設定を選択します。

   重要: グローバル設定変更は、ユーザの役割にかかわらずすべてのユーザに影響します。 ローカル設定変更は、選択した設定に割り当てられた役割のユーザのみに影響します。

4. ページの［許可］領域で、［発注フィールド］を［権限の許可］リストに移動します。

5. （オプション）［親オブジェクトから権限を継承］チェック ボックスをオンにすると、最上位の（親）オブジェクトからより下位の（子）オブジェクトに、同じ設定を使用してセキュリティ権限を適用できます。

   たとえば、組織のローカル設定を作成するとします。 この設定では、フィールド ラベルの変更、フィールドの移動、フィールドを必須にする、フィールドを非表示にする権限を拒否します。 設定を保存してから、［組織］の［添付ファイル］を開き、［親オブジェクトから権限を継承］チェック ボックスをオンにします。 組織のすべての権限が添付ファイルに適用されます。 この例では、フィールド ラベルの変更、フィールドの移動、フィールドを必須にする、フィールドを非表示にする権限が組織に適用されているため、これらの権限は添付ファイルにも適用されます。

6. ［設定の保存］をクリックします。

   設定を役割に割り当てると、その役割のユーザにフィールドを移動する権限が付与されます。

フィールドを必須にする権限の付与

ユーザ インターフェースを設定したり、フィールドを必須に設定できるように、ユーザに権限を付与することができます。

フィールドを必須にする権限を付与する方法

1. 設定するオブジェクトのタブおよびオプションのサブタブをクリックします。
2. 左側の［設定: オン］をクリックします。

   ページの設定が有効になります。

3. ページの［構成情報］領域で、新しいグローバルまたはローカル設定の情報を指定するか、または変更する既存の設定を選択します。

   重要: グローバル設定変更は、ユーザの役割にかかわらずすべてのユーザに影響します。 ローカル設定変更は、選択した設定に割り当てられた役割のユーザのみに影響します。

4. ページの［許可］領域で、［必須］を［権限の許可］リストに移動します。

5. （オプション）［親オブジェクトから権限を継承］チェック ボックスをオンにすると、最上位の（親）オブジェクトからより下位の（子）オブジェクトに、同じ設定を使用してセキュリティ権限を適用できます。

   たとえば、組織のローカル設定を作成するとします。 この設定では、フィールド ラベルの変更、フィールドの移動、フィールドを必須にする、フィールドを非表示にする権限を拒否します。 設定を保存してから、［組織］の［添付ファイル］を開き、［親オブジェクトから権限を継承］チェック ボックスをオンにします。 組織のすべての権限が添付ファイルに適用されます。 この例では、フィールド ラベルの変更、フィールドの移動、フィールドを必須にする、フィールドを非表示にする権限が組織に適用されているため、これらの権限は添付ファイルにも適用されます。

6. ［設定の保存］をクリックします。

   設定を役割に割り当てると、その役割のユーザにフィールドを必須に設定する権限が付与されます。

フィールドを非表示にする権限の付与

ユーザ インターフェースを設定したり、フィールドを非表示に設定できるように、ユーザに権限を付与することができます。

フィールドを非表示にする権限を付与する方法

1. 設定するオブジェクトのタブおよびオプションのサブタブをクリックします。
2. 左側の［設定: オン］をクリックします。

   ページの設定が有効になります。

3. ページの［構成情報］領域で、新しいグローバルまたはローカル設定の情報を指定するか、または変更する既存の設定を選択します。

   重要: グローバル設定変更は、ユーザの役割にかかわらずすべてのユーザに影響します。 ローカル設定変更は、選択した設定に割り当てられた役割のユーザのみに影響します。

4. ページの［許可］領域で、［保護 (読み取り専用およびアクセス)］を［権限の許可］リストに移動します。

5. （オプション）［親オブジェクトから権限を継承］チェック ボックスをオンにすると、最上位の（親）オブジェクトからより下位の（子）オブジェクトに、同じ設定を使用してセキュリティ権限を適用できます。

   たとえば、組織のローカル設定を作成するとします。 この設定では、フィールド ラベルの変更、フィールドの移動、フィールドを必須にする、フィールドを非表示にする権限を拒否します。 設定を保存してから、［組織］の［添付ファイル］を開き、［親オブジェクトから権限を継承］チェック ボックスをオンにします。 組織のすべての権限が添付ファイルに適用されます。 この例では、フィールド ラベルの変更、フィールドの移動、フィールドを必須にする、フィールドを非表示にする権限が組織に適用されているため、これらの権限は添付ファイルにも適用されます。

6. ［設定の保存］をクリックします。

   設定を役割に割り当てると、その役割のユーザにフィールドを非表示に設定する権限が付与されます。

大量変更を実行する権限の付与

ユーザに対して、ユーザ インターフェースを設定する権限や、フィールドに対して大量変更を実行する権限を付与できます。 大量変更は、以下のオブジェクトに関連付けられているフィールドに対して実行できます。

- アセット
- モデル
- リーガル ドキュメント
- 組織
- 連絡先
- 会社
- ロケーション
- サイト

次の手順に従ってください:

1. 設定するオブジェクトのタブおよびオプションのサブタブをクリックします。
2. 左側の［設定: オン］をクリックします。

   ページの設定が有効になります。

3. ページの［構成情報］領域で、新しいグローバルまたはローカル設定の情報を指定するか、または変更する既存の設定を選択します。

   重要: グローバル設定の変更は、役割にかかわらず、すべてのユーザに影響します。 ローカル設定の変更は、選択した設定に割り当てられている役割内のユーザのみに影響します。

4. ページの［権限］領域で、［大量変更］を［権限の許可］リストに移動します。

5. ［設定の保存］をクリックします。

   設定を役割に割り当てると、その役割のユーザにフィールドで大量変更を実行する権限が付与されます。

フィールド情報の表示

拡張フィールドなどの任意のフィールドに関する情報を表示して、データベース関連のフィールド属性を参照できます。任意のフィールドのオブジェクト ラベル、データベースのテーブル名、データベースのフィールド名、属性名、データ タイプ、説明、およびサイズを表示できます。 以下のような場合にこの情報を使用します。

- 外部のレポート ソリューションを使用して、製品外で CA APM データを表示するため、データベース レベルの情報を理解する必要がある場合。たとえば、特定のデフォルト フィールドまたはユーザ定義の拡張フィールドのデータベースのテーブル名、フィールド名、属性名、データ タイプ、説明、またはフィールド サイズを知る必要がある場合などです。
- フィールド ラベルを変更 (P. 53) したり、ページの新しいロケーションにフィールドを移動 (P. 53) した場合。フィールド情報を使用して、そのフィールドがデータベースでどのように表されるかを理解します。 このフィールド情報は、テクニカル サポートと協力して、製品に対する特定の設定変更を理解する場合に役立ちます。

フィールド情報を表示する方法

1. オブジェクトのタブとサブタブ（オプション）をクリックします。
2. 左側の［設定: オン］をクリックします。

   オブジェクトの設定が可能になります。

3. フィールドの横にある［View Details］アイコンをクリックします。

   フィールド情報が表示されます。

フィールド データ検証設定

フィールドのデータ入力を検証するためにフィールド データ検証設定を作成できます。 これらのフィールド データ 検証により、ユーザが正しいフォーマットでデータを入力することが確実になるため、組織内のビジネス ルールを強化できます。

注: データ検証は、追加される新しいデータに適用されます。 既存のデータ レコードが検証されるのは、ユーザがそのデータ レコードにアクセスし、レコードを保存しようとしたときのみです。

たとえば、ユーザが英数字のみ（特殊文字は使用しない）を使用してアセット名を確実に入力するようにしたいとします。［新規アセット］または［アセットの詳細］ページで［アセット名］フィールドに対するデータ検証を作成し、フィールドが英数字の入力のみを許可することを指定します。ユーザが英数字以外の文字を使用すると、エラー メッセージが表示されます。

以下のフィールド データ検証設定を作成できます。

テキスト フィールドへのデータ検証の追加 (P. 66)

テキスト フィールドへのデータ検証の追加

特定のフォーマット要件を施行するためにテキスト フィールドのデータ入力（たとえば連絡先名、電子メール アドレス、または電話番号など）を検証できます 各種タイプのテキスト フィールドに適用される正規表現を定義することでテキスト フィールドに対するデータ検証を作成できます。

注: *正規表現*は特定のパターンまたはフォーマットを説明するテキスト文字列です。 正規表現は、テキストが事前定義済みフォーマットに一致することを確認する目的でテキストを検証するために使用されます。たとえば、電子メール アドレス、電話番号または IP アドレス用の正しいフォーマットを指定するために正規表現を作成します。

重要: テキスト フィールド データ検証を作成する前に正規表現を構成およびテストします。 正規表現の作成、分析、およびテストに関して Web 上のリソースを参照できます。

次の手順に従ってください:

1. 設定するオブジェクトのタブおよびオプションのサブタブをクリックします。
2. 左側の［設定: オン］をクリックします。

   ページの設定が有効になります。

3. ページの［構成情報］領域で、以下の手順に従います。

   a. 新しいグローバルまたはローカル設定の情報を指定するか（35 ページを参照）、または変更する既存の設定を選択します。

      注: データ検証の権限はデフォルトによって許可されています。 現在の設定でデータ検証の権限を拒否できます。 これにより、その設定に割り当てられたユーザにはデータ検証アイコンが表示されなくなり、データ検証を追加できなくなります。

   b. （オプション）［オブジェクト］ドロップダウン リストで、設定するオブジェクトの一部を選択します。 権限の変更（フィールドの移動権限を拒否するなど）は、オブジェクトのその部分にのみ適用されます。

      たとえば、リーガル ドキュメントを設定する場合は、［オブジェクト］ドロップダウン リストの［リーガル ドキュメント ステータス履歴］を選択します。 オブジェクトの該当する部分（ステータス履歴）に対して、フィールドの移動権限が拒否されます。 権限の変更は、ステータス履歴部分のみに適用され、オブジェクトの他の部分には適用されません。

   重要: グローバル設定の変更は、役割にかかわらず、すべてのユーザに影響します。 ローカル設定の変更は、選択した設定に割り当てられている役割内のユーザのみに影響します。

4. 検証するテキスト フィールドの横の［データ検証］アイコンをクリックします。

5. フィールドのタイプ（たとえば電話番号または電子メール アドレス）に適用される正規表現を入力し、［OK］をクリックします。

   重要: フィールド タイプに正しい正規表現を選択し、正規表現を正確に入力したことを確認します。

   注: 既存のデータ検証を変更または削除するには、以下のいずれかの手順を完了します。

   - 検証を変更するには、テキスト入力フィールドの正規表現を編集し［OK］をクリックします。
   - 検証を削除するには、テキスト入力フィールドの正規表現をクリアし［OK］をクリックします。

6. ［設定の保存］をクリックします。

   役割に設定を割り当てる場合、その役割のユーザはテキスト入力が定義されたフォーマットと一致しない場合はデータ検証メッセージを受け取ります。

ハイパーリンクの設定

ユーザが許可されていないタスクを実行するのを防ぎ、ユーザの特定の職務権限に適した情報のみを表示できるように、ハイパーリンク アクセスを設定できます。ハイパーリンクは以下の方法で設定できます。

- ハイパーリンクを非表示にします (P. 68)。ユーザがオブジェクトの監査履歴を参照できないようにしたい場合があります。 そのような場合は、［監査履歴の表示］のハイパーリンクを非表示にします。
- 以前に非表示に設定されたハイパーリンクを表示します (P. 69)。［監査履歴の表示］のハイパーリンクを非表示にしていますが、そのハイパーリンクを表示する必要が出てきたとします。 そのような場合は、［監査履歴の表示］ハイパーリンクを表示します。

ハイパーリンクの非表示

ユーザが特定のハイパーリンクを参照できないようにする必要がある場合は、ハイパーリンクを非表示にすることができます。

ハイパーリンクを非表示にする方法

1. 設定するオブジェクトのタブおよびオプションのサブタブをクリックします。
2. 左側の［設定: オン］をクリックします。

   ページの設定が有効になります。
3. ページの［構成情報］領域で、以下の手順に従います。
   a. 新しいグローバルまたはローカル設定の情報を指定するか、または変更する既存の設定を選択します。
   b. （オプション）［オブジェクト］ドロップダウン リストで、設定するオブジェクトの一部を選択します。 権限の変更（フィールドの移動権限を拒否するなど）は、オブジェクトのその部分にのみ適用されます。

      たとえば、リーガル ドキュメントを設定する場合、［オブジェクト］ドロップダウン リストで［リーガル ドキュメント ステータス履歴］を選択します。オブジェクトの該当する部分（ステータス履歴）に対して、フィールドの移動権限が拒否されます。 権限の変更は、ステータス履歴部分のみに適用され、オブジェクトの他の部分には適用されません。

   重要: グローバル設定変更は、ユーザの役割にかかわらずすべてのユーザに影響します。 ローカル設定変更は、選択した設定に割り当てられた役割のユーザのみに影響します。

4. ハイパーリンクの横にある［権限の許可］アイコンをクリックします。

   ハイパーリンクに［権限の拒否］アイコンが表示されます。

5. ［設定の保存］をクリックします。

   設定を役割に割り当てると、その役割のユーザにはそのハイパーリンクが表示されなくなります。

以前に非表示に設定されたハイパーリンクの表示

以前に非表示に設定されたハイパーリンクをユーザが参照できるようにする必要がある場合は、ハイパーリンクを表示することができます。 たとえば、以前に［監査履歴の表示］ハイパーリンクを非表示にしたとします。 ユーザはアセットを定義するときにこのハイパーリンクを参照できる必要があるため、［アセット］ページにもう一度ハイパーリンクを追加します。

ハイパーリンクを表示する方法

1. 設定するオブジェクトのタブおよびオプションのサブタブをクリックします。
2. 左側の［設定: オン］をクリックします。

   ページの設定が有効になります。

3. ページの［構成情報］領域で、以下の手順に従います。

   a. 新しいグローバルまたはローカル設定の情報を指定するか、または変更する既存の設定を選択します。

   b. （オプション）［オブジェクト］ドロップダウン リストで、設定するオブジェクトの一部を選択します。 権限の変更（フィールドの移動権限を拒否するなど）は、オブジェクトのその部分にのみ適用されます。

      たとえば、リーガル ドキュメントを設定する場合、［オブジェクト］ドロップダウン リストで［リーガル ドキュメント ステータス履歴］を選択します。オブジェクトの該当する部分（ステータス履歴）に対して、フィールドの移動権限が拒否されます。 権限の変更は、ステータス履歴部分のみに適用され、オブジェクトの他の部分には適用されません。

   重要: グローバル設定変更は、ユーザの役割にかかわらずすべてのユーザに影響します。 ローカル設定変更は、選択した設定に割り当てられた役割のユーザのみに影響します。

4. ハイパーリンクがすでに非表示に設定されている場合は、ハイパーリンクの横にある［権限の拒否］アイコンをクリックします。

   ハイパーリンクに［権限の許可］アイコンが表示されます。

5. ［設定の保存］をクリックします。

   設定を役割に割り当てると、その役割のユーザはハイパーリンクを表示して使用できるようになります。

ボタンの設定

ユーザが許可されていないタスクを実行するのを防ぐことができるように、ボタン アクセスを設定できます。 ボタンは以下の方法で設定できます。

- ボタンを非表示にします (P. 70)。ユーザがアセットをコピーまたは削除できないようにしたい場合があります。 そのような場合は、［アセット］ページの［コピー］および［削除］ボタンを非表示にします。
- 以前に非表示に設定されたボタンを表示します (P. 71)。［アセット］ページの［コピー］ボタンを非表示にしていますが、そのボタンを表示する必要が出てきたとします。 そのような場合は、［コピー］ボタンを表示します。

ボタンの非表示

ユーザに［新規］メニュー オプションや［保存］、［コピー］、および［削除］ボタンを表示したり、これらのボタンをユーザが使用できないようにする場合は、オプションやボタンを非表示にすることができます。

ボタンを非表示にする方法

1. 設定するオブジェクトのタブおよびオプションのサブタブをクリックします。
2. 左側の［設定: オン］をクリックします。

   ページの設定が有効になります。
3. ページの［構成情報］領域で、以下の手順に従います。
   a. 新しいグローバルまたはローカル設定の情報を指定するか、または変更する既存の設定を選択します。
   b. （オプション）［オブジェクト］ドロップダウン リストで、設定するオブジェクトの一部を選択します。 権限の変更（フィールドの移動権限を拒否するなど）は、オブジェクトのその部分にのみ適用されます。

      たとえば、リーガル ドキュメントを設定する場合、［オブジェクト］ドロップダウン リストで［リーガル ドキュメント ステータス履歴］を選択します。オブジェクトの該当する部分（ステータス履歴）に対して、フィールドの移動権限が拒否されます。 権限の変更は、ステータス履歴部分のみに適用され、オブジェクトの他の部分には適用されません。

   重要: グローバル設定変更は、ユーザの役割にかかわらずすべてのユーザに影響します。 ローカル設定変更は、選択した設定に割り当てられた役割のユーザのみに影響します。

4. ページの［許可］領域の［権限の許可］リストおよび［権限の拒否］リストで、以下の手順に従います。

   a. ［新規］オプションおよび［保存］ボタンを非表示にするには、［作成］を［権限の拒否］リストに移動します。

   b. ［コピー］ボタンを非表示にするには、［コピー］を［権限の許可］リストに移動します。

   c. ［削除］ボタンを非表示にするには、［削除］を［権限の拒否］リストに移動します。

5. （オプション）［親オブジェクトから権限を継承］チェック ボックスをオンにすると、最上位の（親）オブジェクトからより下位の（子）オブジェクトに、同じ設定を使用してセキュリティ権限を適用できます。

   たとえば、組織のローカル設定を作成するとします。 この設定では、フィールド ラベルの変更、フィールドの移動、フィールドを必須にする、フィールドを非表示にする権限を拒否します。 設定を保存してから、［組織］の［添付ファイル］を開き、［親オブジェクトから権限を継承］チェック ボックスをオンにします。組織のすべての権限が添付ファイルに適用されます。 この例では、フィールド ラベルの変更、フィールドの移動、フィールドを必須にする、フィールドを非表示にする権限が組織に適用されているため、これらの権限は添付ファイルにも適用されます。

6. ［設定の保存］をクリックします。

   設定を役割に割り当てると、その役割のユーザには該当するメニュー オプションやボタンが表示されなくなります。

以前に非表示に設定されたボタンの表示

ユーザが［新規］メニュー オプションや［保存］、［コピー］、および［削除］ボタンを表示して使用できるようにする必要がある場合は、ボタンを表示することができます。 たとえば、以前に［コピー］および［削除］ボタンを非表示にしたとします。 ユーザはオブジェクトをコピーおよび削除できる必要があるため、ページにもう一度ボタンを追加します。

以前に非表示に設定されたボタンを表示する方法

1. 設定するオブジェクトのタブおよびオプションのサブタブをクリックします。
2. 左側の［設定: オン］をクリックします。

   ページの設定が有効になります。

3. ページの［構成情報］領域で、以下の手順に従います。

   a. 新しいグローバルまたはローカル設定の情報を指定するか、または変更する既存の設定を選択します。

   b. （オプション）［オブジェクト］ドロップダウン リストで、設定するオブジェクトの一部を選択します。 権限の変更（フィールドの移動権限を拒否するなど）は、オブジェクトのその部分にのみ適用されます。

      たとえば、リーガル ドキュメントを設定する場合、［オブジェクト］ドロップダウン リストで［リーガル ドキュメント ステータス履歴］を選択します。オブジェクトの該当する部分（ステータス履歴）に対して、フィールドの移動権限が拒否されます。 権限の変更は、ステータス履歴部分のみに適用され、オブジェクトの他の部分には適用されません。

   重要：グローバル設定変更は、ユーザの役割にかかわらずすべてのユーザに影響します。 ローカル設定変更は、選択した設定に割り当てられた役割のユーザのみに影響します。

4. ページの［許可］領域の［権限の許可］リストおよび［権限の拒否］リストで、以下の手順に従います。

   a. ［新規］オプションおよび［保存］ボタンを表示するには、［作成］を［権限の許可］リストに移動します。

   b. ［コピー］ボタンを表示するには、［コピー］を［権限の許可］リストに移動します。

   c. ［削除］ボタンを表示するには、［削除］を［権限の許可］リストに移動します。

5. （オプション）［親オブジェクトから権限を継承］チェック ボックスをオンにすると、最上位の（親）オブジェクトからより下位の（子）オブジェクトに、同じ設定を使用してセキュリティ権限を適用できます。

   たとえば、組織のローカル設定を作成するとします。 この設定では、フィールド ラベルの変更、フィールドの移動、フィールドを必須にする、フィールドを非表示にする権限を拒否します。 設定を保存してから、［組織］の［添付ファイル］を開き、［親オブジェクトから権限を継承］チェック ボックスをオンにします。組織のすべての権限が添付ファイルに適用されます。 この例では、フィールド ラベルの変更、フィールドの移動、フィールドを必須にする、フィールドを非表示にする権限が組織に適用されているため、これらの権限は添付ファイルにも適用されます。

6. ［設定の保存］をクリックします。

   設定を役割に割り当てると、その役割のユーザは該当するメニュー オプションやボタンを表示して使用できるようになります。

拡張フィールドの設定

ユーザ独自のフィールド（*拡張フィールド*）を設計してオブジェクトに追加できます。拡張フィールドは、サイトのアセット管理プログラムに不可欠なリポジトリのデータをすべてキャプチャできるように支援する、追加のフィールドです。主要なデータを格納できる適切なフィールドがリポジトリ内に存在しない場合、そのデータ用に拡張フィールドを定義できます。

モデル、アセット、リーガル ドキュメント、コスト、支払い、モデルの部品と価格、連絡先、会社、組織、ロケーション、およびサイト用に拡張フィールドを定義できます。 また、検索やレポート作成にも拡張フィールドを使用できます。

注: リーガル ドキュメントのコストに、アセット コストに対して作成した拡張フィールドを追加できます。リーガル ドキュメントのコスト設定ページの［既存フィールドの追加］をクリックします。

重要: 拡張フィールドは、CA APM （CA Service Desk Manager および CA Service Catalog）と統合する製品と共有されます。 したがって、統合製品で拡張フィールド値を変更すると、CA APM 内にただちに反映されます。 また、CA APM で拡張フィールド値を変更した場合も統合製品内に反映されます。

拡張フィールドの定義

アセット管理プログラムに不可欠なリポジトリのデータをすべてキャプチャできるように、拡張フィールドを定義できます。たとえば、ブレード サーバのアセットを入力するとき、チップセットについて入力できないとします。 そこで「*chipset*」という名前の拡張フィールドを定義すると、［アセットの詳細］ページにそのフィールドが追加されます。 ユーザは、アセット名、シリアル番号、メモリ、プロセッサ、オペレーティング システムなどのその他の情報と共に、チップセット情報（Intel 5520 など）を入力できます。

重要: これらの手順は、初めてウィザードを完了してオブジェクトの拡張フィールドを定義するときにのみ有効です。 拡張フィールドを定義する前に、テーブル名、ラベル、形式（文字、ブール値、通貨、日付、10 進数、または整数）、フィールド名、属性名、フィールド サイズ、および拡張フィールドのエントリが必要かどうかについて参照できる情報を手元に用意します。 ウィザードを完了すると、フィールドと同様に拡張フィールドを設定できます。

拡張フィールドを定義する方法

1. 設定するオブジェクトのタブおよびオプションのサブタブをクリックします。
2. 左側の［設定: オン］をクリックします。

   ページの設定が有効になります。
3. ページの［構成情報］領域で、以下の手順に従います。

a. 新しいグローバル設定の情報を指定するか、または変更する既存のグローバル設定を選択します。

b. （オプション）［オブジェクト］ドロップダウン リストで、設定するオブジェクトの一部を選択します。 権限の変更（フィールドの移動権限を拒否するなど）は、オブジェクトのその部分にのみ適用されます。

たとえば、リーガル ドキュメントを設定する場合は、［オブジェクト］ドロップダウン リストの［リーガル ドキュメント ステータス履歴］を選択します。 オブジェクトの該当する部分（ステータス履歴）に対して、フィールドの移動権限が拒否されます。 権限の変更は、ステータス履歴部分のみに適用され、オブジェクトの他の部分には適用されません。

重要: グローバル設定用の拡張フィールドのみを定義できます。 ローカル設定用の拡張フィールドは定義できません。

4. （オプション）［設定の保存］をクリックして、グローバル設定を作成します。

5. ［拡張の追加］をクリックします。

ウィザードが表示されます。

6. ［単純型のフィールド］オプションを選択し、画面の指示に従って拡張フィールドの情報を入力します。

注: 拡張フィールドのデフォルトのオブジェクト ラベルを変更するには、［オブジェクト ラベル］フィールドでラベルを変更します。たとえば、「*asset hardware Extension*」というデフォルトのラベルを、「*Hardware Extension*」に変更します。

7. ［設定の保存］をクリックします。

ページ上の拡張フィールドは、すべてのユーザに表示されます。

注: フィールドを追加して拡張フィールドを定義し、ローカルまたはグローバル設定にフィールドを保存すると、ユーザがフィールドのイベントを定義できます。 イベントの管理の詳細については、ユーザ ガイドを参照してください。

拡張フィールドを定義する権限の付与

［拡張の追加］リンクを表示して拡張フィールドを定義できるように、ユーザに権限を付与することができます。

拡張フィールドを定義する権限を付与する方法

1. 設定するオブジェクトのタブおよびオプションのサブタブをクリックします。

2. 左側の［設定: オン］をクリックします。

ページの設定が有効になります。

3. ページの［構成情報］領域で、新しいグローバル設定の情報を指定するか、または変更する既存のグローバル設定を選択します。

   重要: グローバル設定用の拡張フィールドのみを定義できます。 ローカル設定用の拡張フィールドは定義できません。

4. ページの［許可］領域で、［オブジェクトの拡張］を［権限の許可］リストに移動します。

5. （オプション）［親オブジェクトから権限を継承］チェック ボックスをオンにすると、最上位の（親）オブジェクトからより下位の（子）オブジェクトに、同じ設定を使用してセキュリティ権限を適用できます。

   たとえば、組織のローカル設定を作成するとします。 この設定では、フィールド ラベルの変更、フィールドの移動、フィールドを必須にする、フィールドを非表示にする権限を拒否します。 設定を保存してから、［組織］の［添付ファイル］を開き、［親オブジェクトから権限を継承］チェック ボックスをオンにします。組織のすべての権限が添付ファイルに適用されます。この例では、フィールド ラベルの変更、フィールドの移動、フィールドを必須にする、フィールドを非表示にする権限が組織に適用されているため、これらの権限は添付ファイルにも適用されます。

6. ［設定の保存］をクリックします。

   設定を役割に割り当てると、その役割のユーザに拡張を定義する権限が付与されます。

参照フィールドの設定

独自の*参照フィールド*を定義してオブジェクトに追加し、製品を拡張したり、ユーザが管理するオブジェクトの情報の入力方法を改善することができます。参照フィールドを定義するときに、既存のオブジェクトを参照したり、新しいオブジェクトを定義できます。

- *既存のオブジェクト*に対する参照フィールドを定義して共通の値セットを基準にし、オブジェクトを定義するときにユーザがそれを選択できるようにします。 たとえばアセットを定義する場合、ユーザがアセットの特定の契約条件を選択し、承認済みの総勘定元帳コードを選択するようにしたい場合があります。 この例では 2 つの参照フィールドを定義し、アセットを定義するときにユーザが選択できる契約条件と総勘定元帳コードを標準化します。
- *新しいオブジェクト*に対する参照フィールドを定義して、ユーザ、会社、およびアセットなどの関係を構築します。 たとえばベンダーを定義して管理する場合、ユーザが各ベンダーに対するサービス評価を割り当てて、品質評価（1 ～ 5 つの星）を選択するようにしたい場合があります。 この例では 1 つの参照フィールドを定義し、ベンダーを定義および管理するときに品質評価を記録します。

モデル、アセット、リーガル ドキュメント、コスト、支払い、モデルの部品と価格、連絡先、会社、組織、ロケーション、およびサイト用に参照フィールドを定義できます。

参照フィールドを定義したら、以下のタスクを実行してフィールドを設定できます。

- 参照フィールドの条件と結果に対してフィールドを追加する (P. 79)
- 参照フィールドの参照条件と結果からフィールドを削除する (P. 81)
- 以前に非表示に設定された参照フィールドを表示する (P. 82)
- 参照フィールドを新しいロケーションに移動する (P. 83)

参照フィールドの定義

独自の*参照フィールド*を定義してオブジェクトに追加し、製品を拡張したり、ユーザが管理するオブジェクトの情報の入力方法を改善することができます。参照フィールドを定義するときに、既存のオブジェクトを参照したり、新しいオブジェクトを定義できます。たとえばアセットを定義する場合、ユーザがアセットの特定の契約条件を選択し、承認済みの総勘定元帳コードを選択するようにしたい場合があります。この例では、既存のオブジェクトに参照フィールドを定義し、アセットを定義するときにユーザが選択できる契約条件と総勘定元帳コードを標準化します。

重要: 以下の手順は、ウィザードを初めて実行して参照フィールドを定義する場合にのみ有効です。参照フィールドを定義する前に、参照する以下の情報が存在することを確認します：テーブル名、ラベル、形式（文字、ブール値、通貨、日付、10 進数、または整数）、フィールド名、属性名、フィールド サイズ、フィールドへの入力が必須かどうか。ウィザードの実行が完了したら、フィールドを追加または削除したり、以前に非表示に設定された参照フィールドを表示したり、参照フィールドを新しいロケーションに移動したりして、参照フィールドを設定できます。

参照フィールドを定義する方法

1. 設定するオブジェクトのタブおよびオプションのサブタブをクリックします。
2. 左側の［設定: オン］をクリックします。

   ページの設定が有効になります。

3. ページの［構成情報］領域で、以下の手順に従います。

   a. 新しいグローバル設定の情報を指定するか、または変更する既存のグローバル設定を選択します。

   b. （オプション）［オブジェクト］ドロップダウン リストで、設定するオブジェクトの一部を選択します。 権限の変更（フィールドの移動権限を拒否するなど）は、オブジェクトのその部分にのみ適用されます。

      たとえば、リーガル ドキュメントを設定する場合は、［オブジェクト］ドロップダウン リストの［リーガル ドキュメント ステータス履歴］を選択します。 オブジェクトの該当する部分（ステータス履歴）に対して、フィールドの移動権限が拒否されます。 権限の変更は、ステータス履歴部分のみに適用され、オブジェクトの他の部分には適用されません。

   重要: グローバル設定用の参照フィールドのみを定義できます。 ローカル設定用の参照フィールドは定義できません。

4. （オプション）［設定の保存］をクリックして、グローバル設定を作成します。

5. ［拡張の追加］をクリックします。

   ウィザードが表示されます。

6. ［参照フィールド］オプションを選択し、画面の指示に従って参照フィールドの情報を入力します。 以下のフィールドについて説明します。

   オブジェクト ラベル

   参照フィールドの条件と結果にフィールドを追加する (P. 79)場合や、以前に非表示に設定された参照フィールドを表示する (P. 82)場合に、デフォルトの参照フィールドのオブジェクト ラベルを表示します。このラベルは要件に合わせて変更できます。たとえば、［Location Extensions］というデフォルトのラベルを［ロケーション］に変更します。

   ラベル

   リスト管理に表示する参照フィールドのラベルを入力します。

   サービス プロバイダ適格

   サービス プロバイダからのフィールド値が参照フィールドに含まれるかどうかを判断します。 このチェック ボックスをオンにすると、参照フィールドに公開データとサービス プロバイダ オブジェクトが含まれます。

基準の既存オブジェクト

定義中の参照フィールドが基準として使用する既存のオブジェクトを選択します。

注: このオプションを選択するときに、そのオブジェクトの参照フィールドはすでに存在し、そのオブジェクトのマルチテナント オプションは適用されています。

オブジェクト テーブル名

参照フィールドのデータベース テーブル名を指定します。

オブジェクト テナンシー

マルチテナントが有効である場合は、以下のいずれかのオプションを選択して、マルチテナントが参照フィールドに対してどのように機能するかを指定します。

テナントなし

テナント属性を使用しないでオブジェクトを定義します。これらのオブジェクト内のデータはすべて公開データであり、すべてのユーザはテナントのない公開データを作成および更新できます。

テナント必須

（DBMS ではなく CA APM によって強制される）null にできないテナント属性でオブジェクトを定義します。これらのオブジェクト内のデータはすべて、個々のテナントに関連付けられます。パブリック データはありません。

テナント任意

null にできるテナント属性でオブジェクトを定義します。 これらのオブジェクトは、「テナントあり」または「パブリック」として作成できます。 テナントのドロップダウン リストでテナントを選択してオブジェクトを作成するとき、そのオブジェクトはテナントのあるオブジェクトになります。ただし、テナントのドロップダウン リストで［公開データ］オプションを選択するとき、そのオブジェクトはテナントのあるパブリック オブジェクトになります。1 つのテナントのみを表示する役割が割り当てられているユーザには、データの入力時に［テナント］ドロップダウン リストが表示されません。

注: マルチテナントが無効である場合は、参照フィールドの［オブジェクト テナンシー］ドロップダウン リストが表示されません。 ただし、［テナント任意］の設定は参照フィールドに適用されます。 製品がこのように動作するのは、マルチテナントが有効である場合に［テナント任意］の設定が参照フィールドに適用されるようにするためです。

7. ［設定の保存］をクリックします。

そのページの参照フィールドはすべてのユーザに表示されます。 新しいオブジェクトに基づいて参照フィールドを定義する場合、参照フィールドはリスト管理を使用して管理できるリスト アイテムとして表示されます。

フィールドの追加

他のフィールドを追加することで、参照フィールドの条件と結果に表示される情報を増やすことができます。 たとえばアセットを追加した場合、モデル名と説明で検索すると、アセットを説明しているモデルを見つけることができます。 モデルの参照フィールドを設定し、［アセット ファミリ］、［クラス］、および［会社名］フィールドを参照フィールドの条件と結果に追加すると、アセットを定義するときにユーザが簡単にモデルを見つけることができます。

注: 割り当てられた役割にオブジェクトの設定権限が付与されている場合、このタスクを完了できます。

参照フィールドの条件と結果に対してフィールドを追加する方法

1. 設定するオブジェクトのタブおよびオプションのサブタブをクリックします。
2. 左側の［設定: オン］をクリックします。

ページの設定が有効になります。

3. ページの［構成情報］領域で、以下の手順に従います。

   a. 新しいグローバルまたはローカル設定の情報を指定するか、または変更する既存の設定を選択します。

   b. （オプション）［オブジェクト］ドロップダウン リストで、設定するオブジェクトの一部を選択します。 権限の変更（フィールドの移動権限を拒否するなど）は、オブジェクトのその部分にのみ適用されます。

      たとえば、リーガル ドキュメントを設定する場合、［オブジェクト］ドロップダウン リストで［リーガル ドキュメント ステータス履歴］を選択します。オブジェクトの該当する部分（ステータス履歴）に対して、フィールドの移動権限が拒否されます。 権限の変更は、ステータス履歴部分のみに適用され、オブジェクトの他の部分には適用されません。

   重要：グローバル設定変更は、ユーザの役割にかかわらずすべてのユーザに影響します。 ローカル設定変更は、選択した設定に割り当てられた役割のユーザのみに影響します。

4. ［設定の保存］をクリックします。
5. フィールドの横にある［ルックアップ フィールド］アイコンをクリックします。

   参照フィールド基準内のフィールドと結果のリストが表示されます。

6. （グローバル設定のみ）［フィールドの追加］をクリックします。

   ［フィールドの追加］ダイアログ ボックスが表示されます。

7. 参照フィールドの条件、結果、またはその両方に追加するフィールドを選択します。
8. ［保存］をクリックします。
9. ［設定の保存］をクリックします。

   参照フィールドの条件と結果に、追加したフィールドが表示されます。

フィールドの削除

特定のフィールドを参照フィールドの条件と結果に含めたくない場合には、フィールドを削除できます。たとえば、以前に［アセット ファミリ］、［クラス］、［会社名］、および［総勘定元帳コード］フィールドを追加して、モデルの参照フィールドを設定したとします。ユーザが機密情報を表示しないようにするには、モデルの参照フィールドから［総勘定元帳コード］フィールドを削除します。

注: 割り当てられた役割にオブジェクトの設定権限が付与されている場合、このタスクを完了できます。

参照フィールドの条件と結果からフィールドを削除する方法

1. 設定するオブジェクトのタブおよびオプションのサブタブをクリックします。
2. 左側の［設定: オン］をクリックします。

   ページの設定が有効になります。
3. ページの［構成情報］領域で、以下の手順に従います。
   a. 新しいグローバルまたはローカル設定の情報を指定するか、または変更する既存の設定を選択します。
   b. （オプション）［オブジェクト］ドロップダウン リストで、設定するオブジェクトの一部を選択します。 権限の変更（フィールドの移動権限を拒否するなど）は、オブジェクトのその部分にのみ適用されます。

      たとえば、リーガル ドキュメントを設定する場合、［オブジェクト］ドロップダウン リストで［リーガル ドキュメント ステータス履歴］を選択します。オブジェクトの該当する部分（ステータス履歴）に対して、フィールドの移動権限が拒否されます。 権限の変更は、ステータス履歴部分のみに適用され、オブジェクトの他の部分には適用されません。

   重要: グローバル設定変更は、ユーザの役割にかかわらずすべてのユーザに影響します。 ローカル設定変更は、選択した設定に割り当てられた役割のユーザのみに影響します。
4. ［設定の保存］をクリックします。
5. フィールドの横にある［ルックアップ フィールド］アイコンをクリックします。

   参照フィールド基準内のフィールドと結果のリストが表示されます。
6. 参照フィールドの条件と結果から削除するフィールドの横にある［削除にマーク］アイコンをクリックします。
7. ［保存］をクリックします。
8. ［設定の保存］をクリックします。

   このフィールドが参照フィールドの条件と結果に表示されなくなります。

以前に非表示に設定された参照フィールドの表示

以前に非表示に設定された参照フィールドをユーザが参照できるようにする必要がある場合は、参照フィールドを表示することができます。 たとえば、以前に［非アクティブ］フィールドを削除して、モデルの参照フィールドを設定したとします。アセットを追加するときに、ユーザが非アクティブ モデルを見つけても選択できないように、モデルの参照フィールドにもう一度フィールドを追加します。

注: 割り当てられた役割にオブジェクトの設定権限が付与されている場合、このタスクを完了できます。

以前に非表示に設定された参照フィールドを表示する方法

1. 設定するオブジェクトのタブおよびオプションのサブタブをクリックします。
2. 左側の［設定: オン］をクリックします。

   ページの設定が有効になります。
3. ページの［構成情報］領域で、以下の手順に従います。
   a. 新しいグローバルまたはローカル設定の情報を指定するか、または変更する既存の設定を選択します。
   b. （オプション）［オブジェクト］ドロップダウン リストで、設定するオブジェクトの一部を選択します。 権限の変更（フィールドの移動権限を拒否するなど）は、オブジェクトのその部分にのみ適用されます。

      たとえば、リーガル ドキュメントを設定する場合、［オブジェクト］ドロップダウン リストで［リーガル ドキュメント ステータス履歴］を選択します。オブジェクトの該当する部分（ステータス履歴）に対して、フィールドの移動権限が拒否されます。 権限の変更は、ステータス履歴部分のみに適用され、オブジェクトの他の部分には適用されません。

   重要: グローバル設定変更は、ユーザの役割にかかわらずすべてのユーザに影響します。 ローカル設定変更は、選択した設定に割り当てられた役割のユーザのみに影響します。
4. ［設定の保存］をクリックします。
5. フィールドの横にある［ルックアップ フィールド］アイコンをクリックします。

   参照フィールド基準内のフィールドと結果のリストが表示されます。
6. ［非表示フィールドの表示］をクリックします。

   ［非表示フィールドの表示］ダイアログ ボックスが表示されます。
7. 参照フィールドの条件、結果、またはその両方に追加するフィールドを選択します。

8. ［保存］をクリックします。
9. ［設定の保存］をクリックします。

   設定を役割に割り当てると、その役割のユーザには参照フィールドの条件と結果に該当するフィールドが表示されます。

参照フィールドの移動

ユーザが参照フィールドを簡単に見つけられるように、参照フィールドを新しいロケーションに移動できます。 たとえばモデルの参照フィールドを設定し、［アセット ファミリ］、［クラス］、および［会社名］フィールドを参照フィールドの条件と結果に追加すると、アセットを定義するときにユーザが簡単にモデルを見つけることができます。 ユーザが特定の会社のモデルを見つけられるように、モデルの参照フィールドの一番上に［会社名］フィールドを移動します。

注: 割り当てられた役割にオブジェクトの設定権限が付与されている場合、このタスクを完了できます。

参照フィールドを新しいロケーションに移動する方法

1. 設定するオブジェクトのタブおよびオプションのサブタブをクリックします。
2. 左側の［設定: オン］をクリックします。

   ページの設定が有効になります。
3. ページの［構成情報］領域で、以下の手順に従います。
   a. 新しいグローバルまたはローカル設定の情報を指定するか、または変更する既存の設定を選択します。
   b. （オプション）［オブジェクト］ドロップダウン リストで、設定するオブジェクトの一部を選択します。 権限の変更（フィールドの移動権限を拒否するなど）は、オブジェクトのその部分にのみ適用されます。

      たとえば、リーガル ドキュメントを設定する場合、［オブジェクト］ドロップダウン リストで［リーガル ドキュメント ステータス履歴］を選択します。オブジェクトの該当する部分（ステータス履歴）に対して、フィールドの移動権限が拒否されます。 権限の変更は、ステータス履歴部分のみに適用され、オブジェクトの他の部分には適用されません。

   重要: グローバル設定変更は、ユーザの役割にかかわらずすべてのユーザに影響します。 ローカル設定変更は、選択した設定に割り当てられた役割のユーザのみに影響します。

4. ［設定の保存］をクリックします。
5. フィールドの横にある［ルックアップ フィールド］アイコンをクリックします。

   参照フィールド基準内のフィールドと結果のリストが表示されます。
6. 参照フィールドを、参照フィールドの条件と結果の新しいロケーションにドラッグアンドドロップします。
7. ［保存］をクリックします。
8. ［設定の保存］をクリックします。

   設定を役割に割り当てると、その役割のユーザには新しいロケーションにあるフィールドが表示されます。

階層の設定

本製品での*階層*とは、オブジェクト フィールドに対する論理的な関係を確立する 1 つの方法です。 階層を定義して製品を拡張すると、オブジェクトに関するさらに多くの情報と詳細を追跡できます。任意のオブジェクトに対して階層を定義できます。

例: アセットを検索するための階層の作成

CA APM でアセットを入力する場合、［ロケーション名］フィールドを使用して、アセットのロケーションに関連する一般的な情報（市区町村や住所）を入力できます。ただし、ハードウェア アセット ファミリの場合は、アセットのロケーションを追跡するためにさらに詳細な方法が必要です。メンテナンスや修復を行うアセットを見つける必要がある場合、特定のオフィスの番号、ビルの番号、フロア番号、およびパーティション番号を検索するできる必要があります。その場合は、以下のような階層を定義します。

ピッツバーグ オフィス
    3 号棟
        4 階
            パーティション 49466

注: 前の階層の各フィールドは、上の階層のフィールドに関連します。 親フィールドの情報 (3 号棟) を変更すると、子フィールドの情報 (4 階およびパーティション 49466) も変更されます。 ただし、子フィールド (4 階) を変更しても親フィールド (3 号棟) は変更されません。

この階層を定義することによって、アセットの正確なロケーションを把握し、追跡できます。 さらに、CA APM は階層に定義するフィールドを管理し、検索とレポートで使用できるようにします。

階層の定義

階層を定義して製品を拡張すると、オブジェクトに関するさらに多くの情報と詳細を追跡できます。 たとえば、アセットのロケーションの階層を定義して、特定のロケーションまでアセットを追跡します。 アセットのロケーションを選択し、そのロケーションに現在のアセット ファミリ用に作成された階層がある場合は、［ロケーション］セクション内にリストが表示されます。 ロケーションの階層の拡張フィールドには、それぞれ 1 つのリストがあります。 選択されたロケーションに階層の値がある場合は、その値がドロップダウン リストに入力されます。

重要: 階層を定義する前に、参照する以下の情報が存在することを確認します：テーブル名、ラベル、形式（文字、ブール値、通貨、日付、10 進数、または整数）、フィールド名、属性名、フィールド サイズ、階層の拡張フィールドへの入力が必須かどうか。

階層を定義する方法

1. 設定するオブジェクトのタブおよびオプションのサブタブをクリックします。
2. 左側の［設定: オン］をクリックします。

   ページの設定が有効になります。
3. ページの［構成情報］領域で、以下の手順に従います。
   a. 新しいグローバル設定の情報を指定するか、または変更する既存のグローバル設定を選択します。
   b. （オプション）［オブジェクト］ドロップダウン リストで、設定するオブジェクトの一部を選択します。 権限の変更（フィールドの移動権限を拒否するなど）は、オブジェクトのその部分にのみ適用されます。

      たとえば、リーガル ドキュメントを設定する場合は、［オブジェクト］ドロップダウン リストの［リーガル ドキュメント ステータス履歴］を選択します。 オブジェクトの該当する部分（ステータス履歴）に対して、フィールドの移動権限が拒否されます。 権限の変更は、ステータス履歴部分のみに適用され、オブジェクトの他の部分には適用されません。

   重要: グローバル設定用の階層のみを定義できます。 ローカル設定用の階層は定義できません。
4. （オプション）［設定の保存］をクリックして、グローバル設定を作成します。
5. ［拡張の追加］をクリックします。

   ウィザードが表示されます。

6. ［階層］オプションを選択し、画面上の指示に従って階層を定義します。 以下のフィールドについて説明します。

オブジェクト ラベル

階層のデフォルトのオブジェクト ラベルを表示します。 このラベルは要件に合わせて変更できます。たとえば、［アセット 拡張子］というデフォルト ラベルを［アセット］に変更します。

オブジェクト テーブル名

階層のデータベース テーブル名を指定します。

オブジェクト テナンシー

マルチテナントが有効である場合は、以下のいずれかのオプションを選択して、マルチテナントが階層に対してどのように機能するかを指定します。 選択したオプションは階層のすべてのレベルに適用されます。

テナントなし

テナント属性を使用しないでオブジェクトを定義します。これらのオブジェクト内のデータはすべて公開データであり、すべてのユーザはテナントのない公開データを作成および更新できます。

テナント必須

（DBMS ではなく CA APM によって強制される）null にできないテナント属性でオブジェクトを定義します。これらのオブジェクト内のデータはすべて、個々のテナントに関連付けられます。パブリック データはありません。

テナント任意

null にできるテナント属性でオブジェクトを定義します。 これらのオブジェクトは、「テナントあり」または「パブリック」として作成できます。 テナントのドロップダウン リストでテナントを選択してオブジェクトを作成するとき、そのオブジェクトはテナントのあるオブジェクトになります。ただし、テナントのドロップダウン リストで［公開データ］オプションを選択するとき、そのオブジェクトはテナントのあるパブリック オブジェクトになります。 ［テナント］ドロップダウン リストは、データを入力するときに 1 つのテナントのみが表示される役割に割り当てられたユーザには表示されません。

既存フィールドで開始

最初の階層レベルのフィールドの基準として、既存のフィールドを選択します。

新規フィールドで開始

定義した新しいフィールドで階層を開始するように選択します。階層には少なくとも 2 つのレベルを定義する必要があります。

7. ［設定の保存］をクリックします。

そのページの該当する階層はすべてのユーザに表示されます。

検索の設定

ユーザがリポジトリ内の情報を検索したり、その結果をエクスポートする方法を簡略化できるように、検索を設定できます。 検索を設定するには、以下のタスクを実行します。

- 検索結果の制限を設定します (P. 88)。
- 役割にデフォルトの検索を割り当てて (P. 89)、検索を簡単にします。
- 以下のタスクを実行して、検索条件の指定を簡略化します。
  - フィールドの追加 (P. 90)
  - フィールドの削除 (P. 91)
  - フィールドの移動 (P. 92)
  - フィールド名の変更 (P. 92)
  - フィールドの置換 (P. 93)
- 以下のタスクを実行して、検索結果内の情報を見つけやすくします。
  - 列の追加 (P. 94)
  - 列の移動 (P. 95)
  - 列ラベルの変更 (P. 96)
  - 列の削除 (P. 96)
  - 並べ替えるフィールドの追加 (P. 97)
  - 重複レコードを非表示にする (P. 97)

- レコードを開けないようにする (P. 98)

- ユーザが検索を保存できるようにする (P. 98) ことで、検索を簡単にします。
- ユーザが検索結果をエクスポートできるようにする (P. 99) ことで、スプレッドシートで検索結果を簡単に使用できるようにします。
- 不要な検索を削除します (P. 101)。

検索結果の制限の設定

オブジェクトを検索した結果、あまりにも多くのオブジェクト レコードが表示され管理するのが困難な場合、制限を設定できます。 たとえばアセットを検索し、2,000 を超えるアセットが検索結果に表示されたとします。 結果のナビゲートが困難で、必要なアセットを見つけることができません。また、パフォーマンスにも悪影響を及ぼします。 そのため、最大 50 のオブジェクト レコードを返すように設定します。

検索結果の制限を設定する方法

1. 設定する検索のタブおよびオプションのサブタブをクリックします。
2. 左側の［検索の管理］をクリックします。

   保存された検索のリストが表示されます。
3. リスト内の検索をクリックします。
4. ［追加設定］の［最大数の検索結果が返されます］領域で、表示するオブジェクトの総数を指定します。

   注: パフォーマンス上の理由により、この値を 500 未満に設定することをお勧めします。
5. ［実行］をクリックします。

   制限された検索結果が表示され、制限を保存する前に結果への影響を確認できます。今後の検索結果はすべて、指定された数または割合に制限されます。

役割に対するデフォルト検索の割り当て

ユーザがタブまたはサブタブをクリックしたときに、役割のすべてのユーザが同じデフォルト検索を使用できるように、役割にデフォルト検索を割り当てることができます。 たとえば、契約、合意契約、およびサービスの確認と交渉を担当するすべてのユーザは、契約およびベンダー管理の役割に属します。 ユーザがデフォルト検索を指定しなくても済むように検索の設定を簡略化するには、デフォルトのリーガル ドキュメント検索を設定します。契約およびベンダー管理の役割のすべてのユーザのデフォルトとして、設定済みのリーガル ドキュメント検索を割り当てます。 この役割のユーザが［リーガル ドキュメント］タブをクリックすると、製品が提供するデフォルトのリーガル ドキュメント検索ではなく、このユーザのデフォルトとして設定されたリーガル ドキュメント検索が表示されます。

役割にデフォルト検索を割り当てる場合は、以下の情報を考慮します。

- 役割にデフォルトの検索割り当てない場合に、役割のユーザがタブまたはサブタブをクリックすると、オブジェクトのデフォルト検索が表示されます。
- 1 つの役割に複数のデフォルトの検索を割り当てることができます。 ただし、特定オブジェクト タイプ（たとえばモデル、アセット、リーガル ドキュメントなど）については、1 つの役割に 1 つのデフォルト検索のみを割り当てることができます。
- ある検索をデフォルトとして保存すると、その役割のデフォルトとして別の検索が割り当てられている場合でも、その検索がそのユーザのデフォルトになります。 たとえば、アセット技術者の役割のユーザには、製品が提供するアセット検索がデフォルトの検索として設定されています。 検索条件にフィールドを追加し、検索結果からフィールドを削除して、デフォルトのアセット検索を設定します。 その後で、ユーザが属するアセット技術者の役割のデフォルトの検索として、設定したアセット検索を割り当てます。 役割のデフォルトとして他の設定済みのアセット検索が割り当てられている場合でも、このデフォルトのアセット検索がそのユーザのデフォルトになります。
- 役割のデフォルトとして検索を割り当てるには、その役割が検索を使用できる必要があります。 たとえば、リーガル ドキュメント検索を作成します。 契約およびベンダー管理の役割で検索を使用できるようにするには、契約およびベンダー管理の役割に検索を割り当てます。 その後で、契約およびベンダー管理の役割のデフォルトとして、リーガル ドキュメント検索を割り当てることができます。

  注: 役割の検索への割り当ての詳細については、「検索のセキュリティ」を参照してください。

役割にデフォルト検索を割り当てる方法

1. ［管理］-［ユーザ/役割管理］をクリックします。
2. 左側の［役割管理］メニューを展開します。
3. ［役割の検索］をクリックします。
4. 役割を検索し選択します。

   役割の詳細が表示されます。
5. ページの［デフォルト検索］領域で、［新規に選択］をクリックします。
6. 役割のデフォルト検索を選択します。

   デフォルト検索が［デフォルト検索］リストに追加されます。
7. ［保存］をクリックします。

   その検索が役割のすべてのユーザのデフォルトとして保存されます。

フィールドの追加

CA APM では、フィールドを追加して、ユーザの検索条件と結果に表示される情報を拡張できます。 たとえば、アセット検索に［DNS 名］フィールドを追加できます。新しい検索や保存された検索にフィールドを追加できます。製品にあらかじめ用意されているデフォルト検索にフィールドを追加することはできません。

フィールドを追加する方法

1. 検索するオブジェクトのタブおよびオプションのサブタブをクリックします。
2. 左側の［検索の管理］をクリックします。

   保存された検索のリストが表示されます。
3. リスト内の検索をクリックします。
4. ページの一番上にある［設定の検索: オン］をクリックします。

   検索の設定が有効になります。
5. ［フィールドの追加］をクリックします。

   ［フィールドの追加］ダイアログ ボックスが表示されます。
6. 検索条件、結果、またはその両方に追加するフィールドを選択します。
7. ページの一番上にある［設定の検索: オフ］をクリックします。

   検索の設定が完了しました。
8. ［保存］をクリックします。

   検索条件と結果内にフィールドが表示されます。

フィールドの削除

特定のフィールドを検索条件に含めない場合には、CA APM を使用してフィールドを削除できます。 たとえば、アセット検索から［DNS 名］フィールドを削除できます。

検索条件からフィールドを削除する方法

1. 検索するオブジェクトのタブおよびオプションのサブタブをクリックします。
2. 左側の［検索の管理］をクリックします。

   保存された検索のリストが表示されます。
3. リスト内の検索をクリックします。
4. 以下の手順を実行します。
   a. ページの一番上にある［設定の検索: オン］をクリックします。

   検索の設定が有効になります。
   b. 検索条件のフィールドの横にある適切なアイコンをクリックします。
   c. ページの一番上にある［設定の検索: オフ］をクリックします。

   これで検索の設定は完了です。
5. （オプション） 以下の手順を実行します。
   a. ページの［検索条件］領域で、［詳細］をクリックします。
   b. ページの一番上にある［設定の検索: オン］をクリックします。

   検索の設定が有効になります。
   c. 検索条件から削除するフィールドで、横にある［削除にマーク］アイコンをクリックします。
   d. ページの一番上にある［設定の検索: オフ］をクリックします。

   これで検索の設定は完了です。
6. ［保存］をクリックします。

   フィールドはページから削除され、検索条件に表示されなくなります。

フィールドの移動

検索条件を簡単に入力できるように、CA APM を使用して検索条件のフィールドを新しいロケーションに移動できます。 たとえば、［バーコード番号］フィールドが［シリアル番号］フィールドの前に表示されるように、［バーコード番号］フィールドを移動することができます。

フィールドを新しいロケーションに移動する方法

1. 検索するオブジェクトのタブおよびオプションのサブタブをクリックします。
2. 左側の［検索の管理］をクリックします。

   保存された検索のリストが表示されます。
3. リスト内の検索をクリックします。
4. ページの一番上にある［設定の検索: オン］をクリックします。

   検索の設定が有効になります。
5. フィールドを検索条件の新しいロケーションにドラッグアンドドロップします。
6. ページの一番上にある［設定の検索: オフ］をクリックします。

   これで検索の設定は完了です。
7. ［保存］をクリックします。

   フィールドの新しいロケーションが保存されます。

フィールド名の変更

検索条件のフィールド名をより使いやすくするために、CA APM を使用してフィールドのラベルを変更できます。 たとえば、［アセット数量］というラベルを［数量］に変更できます。

フィールド名を変更する方法

1. 検索するオブジェクトのタブおよびオプションのサブタブをクリックします。
2. 左側の［検索の管理］をクリックします。

   保存された検索のリストが表示されます。

3. リスト内の検索をクリックします。
4. 以下の手順を実行します。
   a. ページの一番上にある［設定の検索: オン］をクリックします。

   検索の設定が有効になります。

   b. ［検索条件］でフィールド ラベルをクリックし、新しいラベルを入力します。
   c. ページの一番上にある［設定の検索: オフ］をクリックします。

   これで検索の設定は完了です。
5. （オプション） 以下の手順を実行します。
   a. ページの［検索条件］領域で、［詳細］をクリックします。
   b. ページの一番上にある［設定の検索: オン］をクリックします。

   検索の設定が有効になります。

   c. ラベルを変更するフィールドの横にある［レコード編集］アイコンをクリックします。
   d. 新しいフィールド ラベルを入力します。
   e. ［レコード編集を完了］アイコンをクリックします。
   f. ページの一番上にある［設定の検索: オフ］をクリックします。

   これで検索の設定は完了です。
6. ［保存］をクリックします。

   検索条件に新しいフィールド ラベルが表示されます。

フィールドの置換

CA APM を使用して、詳細検索条件の既存のフィールドを別のフィールドに置換することができます。たとえば会社を検索する場合、［*会社 ID*］フィールドを［*会社名*］に置換することができます。

注: フィールドの置換は、作成したカスタム検索でのみ実行できます。製品デフォルト検索のフィールドは置換できません。

フィールドを置換する方法

1. 検索するオブジェクトのタブおよびオプションのサブタブをクリックします。
2. 左側の［検索の管理］をクリックします。

   保存された検索のリストが表示されます。

3. リスト内の検索をクリックします。
4. 以下の手順を実行します。
   a. ページの［検索条件］領域で［詳細］をクリックします。
   b. ページの一番上にある［設定の検索: オン］をクリックします。

   検索の設定が有効になります。
   c. 別のフィールドに置換するフィールドの横にある［検索］アイコンをクリックします。

      ［フィールドの追加］ダイアログ ボックスが表示されます。
   d. 置換するフィールドを選択して、［OK］をクリックします。
   e. ページの一番上にある［設定の検索: オフ］をクリックします。

   検索の設定が完了しました。
5. ［保存］をクリックします。

   検索条件の既存のフィールドが置換されます。

列の追加

検索結果リストで必要な情報を簡単に見つけられるように、CA APM を使用して検索結果に新しい列を追加できます。 たとえば、会社に John Smith という名前のユーザが複数いるとします。 この人たちの姓と名前は同じですが、その他の連絡先情報（電子メール アドレス、スーパバイザ、部門など）は異なります。

連絡先を検索する場合に、名前として「*John*」を指定し、姓として「*Smith*」を指定すると、検索結果には John Smith の 2 つのインスタンスが表示されます。 John Smith の 2 つの一意のインスタンスが表示されるように、以下のように電子メールの列を結果に追加します。

- John Smith（John.Smith1@company.com）
- John Smith（John.Smith2@company.com）

新しい検索および保存済みの検索に列を追加できます。製品が提供するデフォルト検索には列を追加できません。

検索結果に列を追加する方法

1. 検索するオブジェクトのタブおよびオプションのサブタブをクリックします。
2. 左側の［検索の管理］をクリックします。

   保存された検索のリストが表示されます。

3. リスト内の検索をクリックします。
4. ページの一番上にある［設定の検索: オン］をクリックします。

   検索の設定が有効になります。
5. ［フィールドの追加］をクリックします。

   ［フィールドの追加］ダイアログ ボックスが表示されます。
6. 検索結果に追加するフィールドを選択します。
7. ページの一番上にある［設定の検索: オフ］をクリックします。

   これで検索の設定は完了です。
8. ［保存］をクリックします。

   列が検索結果に追加されます。

列の移動

検索結果で必要な情報を簡単に見つけられるように、CA APM を使用して列を新しいロケーションに移動できます。たとえば、［アセット ID］列が［アセット名］列の前に表示されるように、［アセット ID］列を移動することができます。

列を新しいロケーションに移動する方法

1. 検索するオブジェクトのタブおよびオプションのサブタブをクリックします。
2. 左側の［検索の管理］をクリックします。

   保存された検索のリストが表示されます。
3. リスト内の検索をクリックします。
4. ページの一番上にある［設定の検索: オン］をクリックします。

   検索の設定が有効になります。
5. 検索結果リストで、列を新しいロケーションにドラッグアンドドロップします。
6. ページの一番上にある［設定の検索: オフ］をクリックします。

   これで検索の設定は完了です。
7. ［保存］をクリックします。

   列の新しいロケーションが保存されます。

列ラベルの変更

検索結果のラベルをより使いやすくするために、CA APM を使用して列見出しのラベルを変更できます。 たとえば、［*アセット数量*］というラベルを［*数量*］に変更できます。

列見出しのラベルを変更する方法

1. 検索するオブジェクトのタブおよびオプションのサブタブをクリックします。
2. 左側の［検索の管理］をクリックします。

   保存された検索のリストが表示されます。
3. リスト内の検索をクリックします。
4. ページの一番上にある［設定の検索: オン］をクリックします。

   検索の設定が有効になります。
5. 検索結果で列見出しを選択し、新しいラベルを入力します。
6. ページの一番上にある［設定の検索: オフ］をクリックします。

   これで検索の設定は完了です。
7. ［保存］をクリックします。

   検索結果に新しい列ラベルが表示されます。

列の削除

特定の列を検索結果に含めない場合には、CA APM を使用して列を削除できます。たとえば、検索結果から［MAC アドレス］列を削除できます。

列を削除する方法

1. 検索するオブジェクトのタブおよびオプションのサブタブをクリックします。
2. 左側の［検索の管理］をクリックします。

   保存された検索のリストが表示されます。
3. リスト内の検索をクリックします。
4. ページの一番上にある［設定の検索: オン］をクリックします。

   検索の設定が有効になります。
5. 検索結果で、列の横にある適切なアイコンをクリックします。
6. ページの一番上にある［設定の検索: オフ］をクリックします。

   これで検索の設定は完了です。

7. ［保存］をクリックします。

   ページと検索結果から列が削除されます。

並べ替えフィールドの追加

CA APM では、検索結果に並べ替えフィールドを追加し、昇順または降順を使用して 1 つの列のデフォルトの並べ替え機能を拡張することができます。 たとえば、現在はアセット名でアセットを並べ替えているとします。アセット名とアセット ファミリの両方で並べ替えることができるように、並べ替えにアセット ファミリを追加できます。

検索結果を並べ替えるためのフィールドを追加する方法

1. 検索するオブジェクトのタブおよびオプションのサブタブをクリックします。
2. 左側の［検索の管理］をクリックします。

   保存された検索のリストが表示されます。
3. リスト内の検索をクリックします。
4. ［追加設定］の［検索結果の並べ替え］領域で、並べ替え用の追加フィールドを追加します。
5. ［実行］をクリックします。

   拡張された並べ替えを使用した結果が表示され、並べ替えを保存する前に結果への影響を確認できます。 新しいフィールドが追加され、このフィールドを使用して検索結果を並べ替えることができます。

オブジェクト レコードの重複の防止

CA APM では、検索結果に重複したオブジェクト レコードが表示されるのを防ぐことができます。 たとえば、会社に John Smith という名前のユーザが複数いるとします。 この人たちの姓と名前は同じですが、その他の連絡先情報（電子メール アドレス、スーパバイザ、部門など）は異なります。

保存された連絡先の検索があり、その検索結果には連絡先の姓と名前のみが表示されます。保存された連絡先の検索を使用して検索を実行し、名前として「*John*」を指定し、姓として「*Smith*」を指定すると、検索結果には John Smith の 2 つのインスタンスが表示されます。 重複レコードが表示されないようにすると、1 つの John Smith のインスタンスだけが表示されます。

検索結果に重複したオブジェクト レコードが表示されるのを防ぐ方法

1. 検索するオブジェクトのタブおよびオプションのサブタブをクリックします。
2. 左側の［検索の管理］をクリックします。

   保存された検索のリストが表示されます。

3. 重複レコードが表示されるのを防ぐ検索をクリックします。
4. ［追加設定］の［一意の検索特性］領域で、［結果を一意にする］チェック ボックスをオンにします。
5. ［実行］をクリックします。

   重複レコードがない結果が表示され、設定を保存する前に結果への影響を確認できます。 SQL ステートメントに DISTINCT 引数が追加され、検索結果に重複レコードが表示されるのを防ぎます。

レコードのオープンの防止

CA APM では、検索結果から個人レコードを開く機能を無効にすることができます。 たとえば、ユーザに連絡先の検索結果から連絡先情報を開いて表示したくない場合があります。

検索結果からオブジェクト レコードを開けないようにする方法

1. 検索するオブジェクトのタブおよびオプションのサブタブをクリックします。
2. 左側の［検索の管理］をクリックします。

   保存された検索のリストが表示されます。
3. リスト内の検索をクリックします。
4. ［追加設定］の［一意の検索特性］領域で、［結果の選択を許可］チェック ボックスをオフにします。
5. ［保存］をクリックします。

   オブジェクトを開くためのハイパーリンクは検索結果に表示されません。

ユーザに対する検索の保存の許可

［保存］ボタンを表示して検索を保存できるように、ユーザに権限を付与することができます。

ユーザに検索の保存を許可する方法

1. 設定するオブジェクトのタブとサブタブ（オプション）をクリックします。
2. 左側の［設定: オン］をクリックします。

   ページの設定が有効になります。

3. ページの［構成情報］領域で、新しいグローバルまたはローカル設定の情報を指定するか、または変更する既存の設定を選択します。

   重要: グローバル設定の変更は、役割にかかわらず、すべてのユーザに影響します。 ローカル設定の変更は、選択した設定に割り当てられている役割内のユーザのみに影響します。

4. ページの［権限］領域の［権限の許可］リストおよび［権限の拒否］リストで、以下の手順に従います。

   注: 以下の権限の任意の組み合わせを付与すると、ユーザは検索を保存できます。

   a. ログインしている現在のユーザのみに検索の保存を許可するには、［検索の保存（ユーザへの付与）］を［権限の許可］リストに移動します。

   b. ログインしており、固有の設定が割り当てられている現在のユーザに検索の保存を許可するには、［検索の保存（設定への付与）］を［権限の許可］リストに移動します。 この検索は、現在のユーザおよび設定に選択されたすべてのユーザが使用できます。

   c. ログインしており、固有の役割が割り当てられている現在のユーザに検索の保存を許可するには、［検索の保存（役割への付与）］を［権限の許可］リストに移動します。 この検索は、現在のユーザおよび選択した役割のすべてのユーザが使用できます。

5. ［設定の保存］をクリックします。

   設定が保存されます。 設定が役割に適切に割り当てられたことを確認します。

ユーザに対する検索結果のエクスポートの許可

エクスポートした検索結果を保存できるように、ユーザに権限を付与することができます。

検索結果をエクスポートする権限を付与する方法

1. 設定するオブジェクトのタブとサブタブ（オプション）をクリックします。
2. 左側の［設定: オン］をクリックします。

   ページの設定が有効になります。

3. ページの［構成情報］領域で、新しいグローバルまたはローカル設定の情報を指定するか、または変更する既存の設定を選択します。

   重要: グローバル設定の変更は、役割にかかわらず、すべてのユーザに影響します。 ローカル設定の変更は、選択した設定に割り当てられている役割内のユーザのみに影響します。

4. ページの［権限］領域の［権限の許可］リストおよび［権限の拒否］リストで、以下の手順に従います。

   注: 以下の権限の任意の組み合わせを付与すると、ユーザは検索結果をエクスポートできます。

   a. エクスポートされた検索結果の保存をログインしている現在のユーザのみに許可するには、［エクスポート（ユーザへの付与）］を［権限の許可］リストに移動します。

      注: これがユーザに与えられた唯一の権限である場合、検索要求をスケジュールするときに、そのユーザは、検索に割り当てられたすべての設定にエクスポートするチェック ボックス、および検索に割り当てられたすべての役割にエクスポートするチェック ボックスをオンにできません。検索要求のスケジュールの詳細については、ユーザ ガイドを参照してください。 電子メールは現在のユーザのみに送信されます。 電子メールには、エクスポートのタイプに応じて、CSV ファイルへのリンクが含まれるか、データ ベース ビューの名前が指定されます。

   b. ログインしており、固有の設定が割り当てられている現在のユーザに、エクスポートされた検索結果の保存を許可するには、［エクスポート（設定への付与）］を［権限の許可］リストに移動します。 エクスポートは、現在のユーザと、エクスポート時に使用される検索に割り当てられた選択済みの設定のすべてのユーザが使用できます。

      注: この権限がユーザに付与されると、検索要求をスケジュールするときに、そのユーザは、検索に割り当てられたすべての設定にエクスポートするチェック ボックスをオンにできます。 検索要求のスケジュールの詳細については、ユーザ ガイドを参照してください。 電子メールは選択された設定のすべてのユーザに送信されます。電子メールには、エクスポートのタイプに応じて、CSV ファイルへのリンクが含まれるか、データ ベース ビューの名前が指定されます。

c. ログインしており、固有の設定が割り当てられている現在のユーザに、エクスポートされた検索結果の保存を許可するには、［エクスポート（役割への付与）］を［権限の許可］リストに移動します。エクスポートは、現在のユーザと、エクスポート時に使用される検索に割り当てられた選択済みの役割のすべてのユーザが使用できます。

注: この権限がユーザに付与されると、検索要求をスケジュールするときに、そのユーザは、検索に割り当てられたすべての役割にエクスポートするチェック ボックスをオンにできます。 検索要求のスケジュールの詳細については、ユーザ ガイドを参照してください。 電子メールは選択された役割のすべてのユーザに送信されます。電子メールには、エクスポートのタイプに応じて、CSV ファイルへのリンクが含まれるか、データ ベース ビューの名前が指定されます。

5. （オプション）［親オブジェクトから権限を継承］チェック ボックスをオンにすると、最上位の（親）オブジェクトからより下位の（子）オブジェクトに、同じ設定を使用してセキュリティ権限を適用できます。

   たとえば、組織のローカル設定を作成するとします。 この設定では、フィールド ラベルの変更、フィールドの移動、フィールドを必須にする、フィールドを非表示にする権限を拒否します。 設定を保存してから、［組織］の［添付ファイル］を開き、［親オブジェクトから権限を継承］チェック ボックスをオンにします。 組織のすべての権限が添付ファイルに適用されます。 この例では、フィールド ラベルの変更、フィールドの移動、フィールドを必須にする、フィールドを非表示にする権限が組織に適用されているため、これらの権限は添付ファイルにも適用されます。

6. ［設定の保存］をクリックします。

   設定が保存されます。 設定が役割に適切に割り当てられたことを確認します。

検索の削除

保存済みの不要な検索（デフォルトおよびユーザ定義の検索）を削除できます。

保存済みの検索を削除する方法

1. 検索するオブジェクトのタブおよびオプションのサブタブをクリックします。
2. 左側の［検索の管理］をクリックします。

   保存された検索のリストが表示されます。
3. 削除する検索をクリックします。
4. ［削除］をクリックし、検索を削除することを確認します。

   検索が削除されます。

リーガル テンプレートの設定

*リーガル テンプレート*は、特定のタイプのリーガル ドキュメントに属する属性のグループを提供します。一般に、管理者がリーガル テンプレートを設定およびメンテナンスし、そのリーガル テンプレートに基づいてユーザがリーガル ドキュメントのレコードを作成します。リーガル ドキュメント レコードを作成する場合、まずドキュメントのベースとなるリーガル テンプレートを選択します。リーガル ドキュメント レコードは、リーガル テンプレートの属性を継承します。

各リーガル テンプレートには通常、リーガル ドキュメント タイプに適用される*契約条件*が含まれます。 たとえば、インボイス用のリーガル テンプレートには、支払い条件に関する情報が含まれる場合があります。

この製品では、リーガル テンプレートを定義して、リーガル テンプレートの属性を変更できます。リーガル テンプレートに割り当てられた契約条件を変更する場合、契約条件のマスタ リストから該当箇所を削除するか、または新しい契約条件を追加します。

テンプレートに基づくリーガル ドキュメントがすべて削除されるまで、リーガル テンプレートは削除できません。 また、リーガル テンプレート名でリーガル ドキュメントを検索したり、リーガル テンプレート名を使用してレポート内に含めるレコードを選択したりできます。

リーガル テンプレートの定義

特定のタイプのリーガル ドキュメントに属する属性をグループ化するリーガル テンプレートを定義できます。管理者または適切な権限を持ったユーザがリーガル テンプレートを定義できます。

リーガル テンプレートを定義する方法

1. ［ディレクトリ］-［リスト管理］をクリックします。
2. 左側で［リーガル ドキュメント リスト］を展開し、［リーガル テンプレート］をクリックします。

   右側にテンプレートのリストが表示されます。
3. ［新規］をクリックし、テンプレートの名前を入力して、［保存］をクリックします。

   リストに新しいテンプレートが表示されます。
4. 新しいテンプレートの［レコード編集］アイコンをクリックします。

5. ［割り当て済み契約条件の表示］ハイパーリンクをクリックします。
6. ［新規に選択］をクリックし、新しいテンプレートの契約条件を選択します。
7. ［保存］をクリックします。

   ユーザがリーガル ドキュメントを定義するときに、新しいテンプレートを選択できるようになります。

リーガル テンプレートの契約条件の変更

リーガル テンプレートの契約条件を変更できます。 管理者または適切な権限を持ったユーザが契約条件を変更できます。

リーガル テンプレートの契約条件を変更する方法

1. ［ディレクトリ］-［リスト管理］をクリックします。
2. 左側で［リーガル ドキュメント リスト］を展開し、［リーガル テンプレート］をクリックします。

   右側にテンプレートのリストが表示されます。
3. リーガル テンプレートの［レコード編集］アイコンをクリックします。
4. ［割り当て済み契約条件の表示］ハイパーリンクをクリックします。

   リーガル テンプレートのすべての契約条件が表示されます。
5. 以下のいずれかのオプションを選択します。
   - ［新規に選択］をクリックし、テンプレートの契約条件を選択します。
   - ［削除］アイコンをクリックして、テンプレートから契約条件を削除します。
6. ［保存］をクリックします。

   更新された契約条件がテンプレートに適用されます。

イベントおよび通知の設定

*イベント*は、オブジェクトの（デフォルトまたは拡張）フィールドに関連するアクティビティを表します。イベントを定義する場合、イベントが発生するために満たされる必要がある基準を指定します。 たとえば、特定のフィールドのデータが変更されたタイミングを知る必要があるとします。 その場合、データ変更を検出するイベントを定義できます。イベントは*通知*と連携して機能します。ワークフロー プロバイダ（CA Process Automation など）は、重要なイベントが特定のフィールドまたはオブジェクトに対して発生したことをチーム メンバに知らせる場合に通知を作成します。 イベントと通知を使用すると、適切なタスクが適切なタイミングおよび正しい順序で実行されるように、予定されているイベントやヘルプについてユーザに通知できます。

通知は、定義したイベントが発生したときにトリガされます。 たとえば、リーガル ドキュメントの［終了日］フィールドに日付イベントを定義し、法的契約が期限切れになる 15 日前に契約管理者に通知することができます。 契約管理者はその 15 日間を契約の見直しや、より有利な交渉のために活用できます。 定義した日（契約の期限切れの 15 日前）になるとイベントが発生し、ワークフロー プロバイダによって通知プロセスがトリガされます。ワークフロー プロバイダおよび CA APM で指定した設定に基づき、ワークフロー プロバイダは通知を作成、発行、管理します。

CA APM 内のデフォルトの通知方法では、ワークフロー プロバイダによる電子メール通知をサポートしています。ユーザの内部電子メール システム内に定義されているあらゆるユーザ リストまたは配布リストの宛先に電子メール通知を送信できます（宛先が CA APM ユーザでなくてもかまいません）。 さらに、お使いの電子メール システムで許可されている場合、任意の外部電子メール アドレスに電子メールを送信できます。

任意のタイプのプロセスをトリガするように、ワークフロー プロバイダの通知プロセスを設定することもできます。 たとえば、CA APM でイベントが発生したときに別のアプリケーションの特定のアクションを実行するように、通知プロセスを設定できます。 さまざまな通知プロセスの設定については、お使いのワークフロー プロバイダのドキュメントを参照してください。

フィールドまたはオブジェクトへの重要な変更を追跡および管理するために、以下のタイプのイベントを定義できます。

- 日付イベント。 オブジェクトの日付フィールドをモニタし、重要な日付が近いまたは経過した場合にワークフロー プロバイダを使用してユーザに通知します。
- 変更イベント。 オブジェクトのフィールドをモニタし、フィールド値が変更された場合にワークフロー プロバイダを使用してユーザに通知します。
- 監視イベント。 オブジェクトのフィールドをモニタし、タスクの完了が妨げられるおそれがある場合にワークフロー プロバイダを使用してユーザに通知します。

イベントおよび通知を設定する方法

イベントは、ワークフロー プロバイダ（たとえば CA Process Automation）が作成する通知と組み合わせて機能し、重要なイベントやアクティビティに関する情報をチーム メンバに伝えます。イベントおよび通知を設定するには、以下の手順に従います。

1. 管理者は、イベントを管理する権限をユーザに付与します (P. 105)。
2. 適切な権限を持つユーザは、既存の設定を開いて、日付イベント、変更イベント、および監視イベントを定義します。

   注: イベントの定義の詳細については、ユーザ ガイドを参照してください。

3. イベントを定義する場合、すべてのワークフロー プロバイダのプロセス パラメータを CA APM オブジェクトの属性にマップします。

   注: ワークフロー プロバイダのプロセス パラメータのマッピングの詳細については、ユーザ ガイドを参照してください。

4. ワークフロー プロバイダが通知プロセスを開始します。
5. ユーザにはイベントの監査履歴が表示されます。

   注: イベントの監査履歴の表示の詳細については、ユーザ ガイドを参照してください。

イベントを管理する権限の付与

ユーザ インターフェースを設定したり、イベントを定義できるように、ユーザに権限を付与することができます。

イベントを定義する権限を付与する方法

1. 設定するオブジェクトのタブおよびオプションのサブタブをクリックします。
2. 左側の［設定: オン］をクリックします。

   ページの設定が有効になります。

3. ページの［構成情報］領域で、既存のグローバル設定またはローカル設定を選択します。

   重要: グローバル設定変更は、ユーザの役割にかかわらずすべてのユーザに影響します。 ローカル設定変更は、選択した設定に割り当てられた役割のユーザのみに影響します。

4. ページの［許可］領域で、［イベントの管理］を［権限の許可］リストに移動します。
5. （オプション）［親オブジェクトから権限を継承］チェック ボックスをオンにすると、最上位の（親）オブジェクトからより下位の（子）オブジェクトに、同じ設定を使用してセキュリティ権限を適用できます。

   たとえば、組織のローカル設定を作成するとします。 この設定では、フィールド ラベルの変更、フィールドの移動、フィールドを必須にする、フィールドを非表示にする権限を拒否します。 設定を保存してから、［組織］の［添付ファイル］を開き、［親オブジェクトから権限を継承］チェック ボックスをオンにします。 組織のすべての権限が添付ファイルに適用されます。 この例では、フィールド ラベルの変更、フィールドの移動、フィールドを必須にする、フィールドを非表示にする権限が組織に適用されているため、これらの権限は添付ファイルにも適用されます。

6. ［設定の保存］をクリックします。

   設定を役割に割り当てると、その役割のユーザにイベントを定義する権限が付与されます。

リスト管理

管理するオブジェクトの適切な情報をリストから簡単に選択できるように、リストに表示するアイテムを定義できます。たとえば、新しい連絡先を定義する場合、連絡先タイプを指定できます。その連絡先タイプのリストに表示するアイテムを定義します。また、リーガル ドキュメントを定義する場合には、ユーザはリーガル テンプレートを指定する必要があります。 そのリーガル テンプレートのリストに表示するアイテムを定義します。

以下のリスト、および定義した参照フィールドのアイテムを管理できます。

- アセット
- 会社
- 連絡先
- リーガル ドキュメント
- ロケーション
- モデル
- 組織
- 検索
- 正規化

リスト アイテムの管理

オブジェクトを管理する場合に適切な情報をリストから簡単に選択できるように、リスト項目を定義、更新および削除できます。 たとえば、ユーザがコスト センターを簡単に選択できるように、コスト センターの名前と説明を変更できます。また、総勘定元帳コードを削除すると、ユーザがアセットを定義するときにそのコードを選択できなくなります。

重要: リスト項目を削除すると、ユーザがオブジェクトを定義するときにその項目を選択できません。 リスト項目を削除する代わりに、リスト項目を非アクティブにすることができます。 将来リスト項目が必要になった場合は、項目を再度アクティブにすることができます。 項目を再定義る必要はありません。

次の手順に従ってください:

1. ［ディレクトリ］-［リスト管理］をクリックします。
2. 左側で、管理するリストを選択します。

3. **リストを定義します。**
   a. ［新規］をクリックします。
   b. リスト アイテムの情報を入力します。

      注: マルチテナントが有効である場合は、リスト アイテムのテナントを選択します。
4. **リストを更新します。**
   a. 更新するリスト アイテムの横にある［レコード編集］アイコンをクリックします。
   b. リスト アイテムの新しい情報を入力します。

      注: リスト項目を非アクティブにするには、［非アクティブ］チェックボックスをオンにします。
5. **リスト項目を削除します。** 削除するリスト アイテムの横にある［削除にマーク］アイコンをクリックします。
6. ［保存］をクリックします。

アセット ファミリのクラスおよびサブクラスのリストの定義

モデルやアセットを定義する場合に適切な情報を簡単に選択できるように、アセット ファミリのクラスおよびサブクラスのリストを定義できます。 たとえば、クラス「printer」およびサブクラス「laser」を定義できます。 その後、ユーザがプリンタ アセットを作成または検索する場合、この追加情報を使用して正しいアセットを定義または識別できます。

次の手順に従ってください:

1. ［ディレクトリ］-［リスト管理］をクリックします。
2. 左側で、［アセット リスト］-［アセット ファミリ］をクリックします。
3. クラス リストを定義するには、以下の手順に従います。
   a. クラスを定義するアセット ファミリの横にある［レコード編集］アイコンをクリックします。
   b. ［クラス リスト］ハイパーリンクをクリックします。
   c. アセット ファミリのクラス レコードを定義します。
   d. ［保存］をクリックします。

4. サブクラス リストを定義するには、以下の手順に従います。
   a. サブクラスを定義するクラス レコードの横にある［レコード編集］アイコンをクリックします。
   b. ［サブクラス リスト］ハイパーリンクをクリックします。
   c. アセット ファミリのサブクラス レコードを定義します。
   d. ［保存］をクリックします。

リーガル ドキュメントの契約条件の定義

リーガル ドキュメント リストに適用される契約条件を定義できます。 その後、ユーザがリーガル テンプレートまたはリーガル ドキュメントを定義する場合に正しい条件を適用できます。

次の手順に従ってください:

1. ［ディレクトリ］-［リスト管理］をクリックします。
2. 左側で［リーガル ドキュメント リスト］を展開し、［契約条件］を選択します。
3. ［新規］をクリックします。
4. 新しいリスト アイテムの情報を入力します。

   注: 日付固有の契約条件のリストのみに新しいアイテムを適用するには、［日付指定キー］チェック ボックスをオンにします。 新しい項目を日付固有でない契約条件リストのみに適用するには、このチェック ボックスをオフにします。
5. ［保存］をクリックします。

アセット ファミリの除外

アセット ファミリを除外して、ユーザが使用できないようにすることができます。アセット ファミリを除外すると、モデルを作成または変更するユーザはそのアセット ファミリを選択できません。また、除外されたアセット ファミリは、フィルタ、データ インポート、または設定の管理に使用することはできません。たとえば、CA APM が CA Service Desk Manager に統合されると、CA Service Desk Manager のアセット ファミリは CA APM ユーザにも使用可能になります。 CA Service Desk Manager アセット ファミリが必要でない場合は、それらを除外してユーザが使用できないようにできます。

アセット ファミリを除外する前にモデルがすでにそのアセット ファミリに関連付けられていた場合、そのモデルへのアクセスおよび編集は実行できます。また、そのモデルを使用してアセットを作成することもできます。 ただし、そのモデルのアセット ファミリを別の除外されたアセット ファミリに変更することはできません。

注: モデルのアセット ファミリを変更できるのは、モデルにアセットが関連付けられていない場合のみです。

次の手順に従ってください:

1. ［ディレクトリ］-［リスト管理］をクリックします。
2. 左側で、［アセット リスト］または［モデル リスト］下の［アセット ファミリ］を選択します。
3. 除外するファミリの［レコード編集］アイコンをクリックします。
4. ［ITAM］チェック ボックスをオフにし、［レコード編集を完了］アイコンをクリックします。

   重要: ［非アクティブ］チェック ボックスはオンにしないでください。 このアクションを実行すると、CA MDB に統合されたすべての製品のアセット ファミリが非アクティブになります。
5. ［保存］をクリックします。

カスタム関係

カスタム関係は 2 つの関連するオブジェクト間のリンクです。 関係は、オブジェクト間の相互依存に関する情報を記述し提供します。カスタム関係によって、1 つのオブジェクトから別のオブジェクトに移動できます。オブジェクトに関する情報を見つけ、取得し、変更できます。

カスタム関係の管理

2 つのオブジェクト間のカスタム関係を定義および更新できます。 カスタム関係では、オブジェクトの 1 つがプライマリ オブジェクトで、もう 1 つのオブジェクトがセカンダリ オブジェクトになります。

注: 定義して保存したカスタム関係は削除できません。

次の手順に従ってください:

1. カスタム関係を定義します。
   a. カスタム関係を定義するオブジェクトに関連するタブと、必要に応じてサブタブをクリックします。
   b. 検索結果ページから［CONFIGURE: ON］を選択します。
   c. すべてのファミリまたはテンプレートにわたるグローバル設定を選択するか、グローバル設定を作成して保存します。

      注: ローカル設定のカスタム関係は定義できません。
   d. ［カスタム関係の追加］をクリックします。

      ［カスタム関係の追加］ダイアログ ボックスが表示されます。
   e. プライマリ オブジェクト関係とセカンダリ オブジェクト関係の名前を指定します。
   f. セカンダリ オブジェクトを選択します。

      注: アセット、モデル、およびリーガル ドキュメントの場合は、ファミリまたはテンプレートを選択するか、［すべてのタイプ］を選択します。
   g. ［保存］をクリックします。

      新しいカスタム関係は、プライマリおよびセカンダリ オブジェクトの［カスタム関係］メニューに表示されます。
   h. （オプション）単純型フィールドまたは参照拡張フィールドをカスタム関係に追加します。
2. カスタム関係を更新します。
   a. カスタム関係を更新するオブジェクトに関連するタブと、必要に応じてサブタブをクリックします。
   b. 検索結果ページから［CONFIGURE: ON］を選択します。
   c. すべてのファミリまたはテンプレートにわたるグローバル設定を選択します。
   d. ［カスタム関係］メニューで関係を選択します。

e. カスタム関係の情報を変更し、［保存］をクリックします。

第 4 章: ハードウェア アセットの管理

このセクションには、以下のトピックが含まれています。

ハードウェア照合

ハードウェア照合プロセスは、*検出されたアセット*を別の論理リポジトリ内の対応する*所有アセット*と一致させることにより、ビジネス プラクティスに基づいたアセット管理を実現します。 このプロセスを使用して、所有アセットと検出されたアセット間の差異を識別できます。 ハードウェア照合を使用すると、許可されていない、紛失している、あまり使用されていない、または過剰に使用されているアセットを識別して、ハードウェア アセット ベースを最適化できます。

- 所有アセットは、財務および所有権の観点から IT アセット情報を提供します。この製品では、法的情報やコスト情報など、調達から取得、配分、使用、処分に至るまで、所有アセットの全ライフサイクルをサポートします。 所有アセットには、発注書番号、インボイス番号、関連コスト（リース、支払いスケジュール、メンテナンス）、関連契約（契約条件）、ベンダー情報などを含む購入レコードがあります。 所有アセット データは、CA APM ユーザ インターフェース、［管理］タブ、Data Importer を使用して入力およびインポートされます。
- 検出されたアセットは、企業が使用している、または展開済みのアセットに関する情報を提供します。外部検出製品および CA Client Automation の検出コンポーネントは、ネットワーク上のアセットをスキャンし、検出されたアセットとしてそれらを CA MDB 内に保存します。 検出されたアセットには、以下の情報に関する証拠が含まれます。

- アセットは展開され、ユーザのネットワーク上に存在する。
- アセットは使用中でメトリックがある。
- アセットには在庫管理用の最新の設定情報がある。

CA APM ハードウェア照合プロセスは検出されたアセットデータと CA MDB 内に保存された所有アセット データを一致させます。 ハードウェア照合プロセスは、どの所有アセットにも一致しないアセットを検出する場合があります。 ネットワーク内のすべてのアセットを追跡し管理できるように、リポジトリに不一致アセットを追加できます。

ハードウェア照合では、所有権と検出されたデータの同期が自動的に行われます。ハードウェア照合は、CA Client Automation およびサードパーティ製のディスカバリ製品のディスカバリ コンポーネントをサポートしています。これらのコンポーネントおよび製品は、CA Asset Converter および CA Client Automation のアセット コレクタ コンポーネントの組み合わせによってサポートされています。 CA SAM がインストールされるときに、ディスカバリ コネクタは CA SAM リポジトリにディスカバリ データをロードします。次に、ディスカバリ データは CA APM と同期されます。

ハードウェア照合エンジン

*ハードウェア照合エンジン*は、照合プロセス中に以下のタスクを継続的に処理する Windows サービスです。

- 照合ルール (P. 128) を使用して、検出されたアセットと所有アセットを同期する。
- アセット一致基準 (P. 130) に基づき、所有アセットと検出されたアセットを照合する。
- 正規化ルールに基づき、検出データを所有権データにマップする。
- 対応する検出されたアセットの変更に基づき、製品内の選択されたアセット フィールドを更新する。
- 実行中の照合ルールで定義されたアクションを完了する。

照合エンジンが照合ルールを処理する方法

照合ルールが最後に実行された日付および時間によって、次にルールが処理される時期が決まります。ハードウェア照合エンジンは以下の順序で照合ルールを処理します。これにより、複数のハードウェア エンジンに加えて複数のテナントのサポートも考慮することができます。

1. 各ハードウェア照合エンジンは、別のエンジンが処理していない照合ルールを検索し、処理の日付と時刻が最も古いルールを選択します。
2. ハードウェア照合エンジンは、他のエンジンがアクセスできないように照合ルールをロックし、ルールを実行し、ルールの日付と時刻の値を更新して、ルールのロックを解除します。 続いて、日付と時刻の値が最も古く、次に使用可能な照合ルールを検索して、処理を繰り返します。
3. この処理は、引き続きすべてのエンジンを使用して、日付と時刻の値が最も古く、次に使用可能な照合ルールを継続的に操作、検索、および実行します。

照合方法

照合プロセスは、ディスカバリ製品からのデータと CA MDB 内の CA APM 所有権データを比較します。このプロセスはディスカバリおよび所有アセットを照合し、重要なフィールドへの変更を追跡し、見つからないまたは削除されたアセットの結果として生じる差異を追跡します。 照合するには、以下の手順に従います。

1. データの正規化ルール (P. 116) を確立し、ディスカバリ リポジトリと製品間でデータの値をマップします。
2. 照合ルールを定義 (P. 128) し、処理対象のデータの制限方法および検出されたレコードの処理方法を指定します。
3. （オプション）照合更新オプションを定義 (P. 130) し、ハードウェア照合エンジンによって、対応する検出されたアセットで見つかった変更を使用して所有アセットフィールドが自動的に更新されるようにします。
4. 所有アセットと検出されたアセットを一致させるため、照合ルールのアセット一致基準を定義 (P. 130) します。
5. （オプション）照合プロセスから所有アセットを除外します (P. 134)。
6. （オプション）照合プロセスからアセット ファミリを除外します (P. 135)。
7. メッセージ キュー内の照合結果を表示します (P. 137)。
8. （オプション）ネットワーク内のアセットをすべて追跡し管理できるように、リポジトリに不一致アセットを追加 (P. 138) します。

   注: レポートを生成して、照合結果と環境に関する情報を表示できます。 レポートの生成の詳細については、「ユーザ ガイド」を参照してください。

データの正規化

*データの正規化*とは照合処理の 1 つの手順であり、製品とディスカバリ リポジトリのデータを標準化、整理、および統合するためのルールのリストを作成します。正規化によって、発注書用の製品、人材用の製品、調達用の製品、Data Importer などの複数のソースから製品にインポートされる重複データが縮小、削除、および統合されます。

データを正規化すると、データ管理に必要な時間および負担が軽減されます。また、アセット、モデル、およびその他のオブジェクトを定義する場合やレポートを生成する場合に、ユーザが不適切な情報を選択してしまう可能性を低減します。本製品では、正規化の処理について説明し、正規化をさらに効率よく正確に実行できるようにします。照合処理の実行中に、統合済みの検出データは、ユーザが所有するアセットと照合されます。また、照合レポートを使用してこのデータをレポートすることができます。

アセット一致基準 (P. 130)として使用できる、会社、オペレーティング システム、およびシステム モデルの 3 つのフィールドを正規化します。これらのフィールドを正規化するのは、正規化された 1 つの値を表す際に複数の値が存在することが多いためです。たとえば、ディスカバリ ツールによって、1 つの会社の名前のバリエーションが数多く見つかる場合があります。会社名のすべてのバリエーションを 1 つの値に正規化し、アセット一致基準には正規化された会社名が含まれるようにします。これらのフィールドをアセット一致基準に含めることができるように、これらのフィールドが正規化されます。

ハードウェア照合エンジンは、ユーザが定義する以下の正規化ルールを参照して、製品にインポートされるデータを正規化します。

- 会社正規化ルール（P. 117）
- オペレーティング システム正規化ルール（P. 121）
- システム モデル正規化ルール（P. 124）

例: 会社データの正規化

次の例では、CA Client Automation を使用して製品に会社データをインポートするときに、以下のようなさまざまな形式の Document Management Company のバリエーションが検出されました。

- Document Management Company
- Document Management Co
- Doc Management Company
- Doc Management Co

アセットとモデルを定義するとき、および照合レポートを生成するときに適切な会社を選択できるように、会社正規化ルールを定義して、すべてのバリエーションを Document Management Company にマップします。照合プロセスの実行中に、CA MDB でアセットが更新される前に、正規化ルールは以下のように値をマップします。

注: 収集された会社が検出された会社である場合のみ、権限のある（代表の）会社にマップされる収集された会社がハードウェア照合に影響します。

収集されたデータ（権限のない値）	正規化済みのデータ（権限のある値）
Document Management Co	Document Management Company
Doc Management Company	Document Management Company
Doc Management Co	Document Management Company

会社正規化ルール

会社正規化ルールは、たとえば Microsoft、Adobe、Lenovo などのビジネス上の関係を持つ重要な組織を対象としています。

収集された会社

*収集された会社*とは、検出された会社または*製品に定義済みの会社*のいずれかを表します。製品に定義済みの会社は、ユーザ入力と CA MDB を共有する他の製品から収集されます。ハードウェア照合では*検出された*会社のみを照合します。収集された会社は*権限のない*ステータスです。権限のない収集された会社を、正規化された*権限のある*会社にマップします。

重要: *ハードウェア照合の実行中には、収集された会社のうち検出されたもののみが照合され、正規化された会社にマップされます。*

正規化された会社

正規化された会社とは、*CA コンテンツ会社*または製品に定義済み会社のいずれかです。 CA コンテンツ会社は CA APM で提供されています。この会社は*権限のある*ステータスです。 権限のあるステータスの場合は、会社に正規化ルールを持たせることができます。 1 つ以上の収集された会社を権限のある会社にマップする場合に、権限のある正規化された会社に対する正規化ルールを定義します。

製品に定義済みの会社は、最初は権限のないステータスです。 権限のないステータスから権限のあるステータスに製品に定義済みの会社のステータスを変更 (P. 120)できます。その後、収集された会社を製品に定義済みの権限のある会社にマップして、正規化ルールを定義できます。 検出済みの収集された会社の会社正規化ルールのみがハードウェア照合に影響します。

従属会社

正規化ルールでは、権限のない収集された会社を正規化された権限のある会社にマップすると、権限のない会社が権限のある会社に*従属*します。

会社正規化ルールの定義

重要: 正規化ルールは、サービス プロバイダに関連付けられたすべてのテナントと公開データに適用されます。 このタスクを実行するユーザが、照合管理アクセスが有効な役割に属することを確認します。

照合ルールにアセット一致基準 (P. 130)が含まれる場合に必ず照合処理の実行中に適用される、会社正規化ルールを定義できます。 会社情報を含むすべてのアセット一致基準では、自動的に会社正規化ルールが適用されます。

正規化ルールでは、権限のない収集された会社を正規化された権限のある会社にマップすると、権限のない会社が権限のある会社に*従属*します。 従属会社になると、［収集された会社］リストまたは［正規化された会社］リストには表示されません。 従属会社を含む正規化ルールを削除する (P. 127)と、下位の会社が権限のないステータスに戻り、［収集された会社］リストおよび（製品に定義済みの会社である場合は）［正規化された会社］リストに表示されます。

会社正規化ルールを定義する方法

1. ［ディレクトリ］-［リスト管理］をクリックします。
2. 左側で［正規化］を展開し、［会社の正規化］を選択します。

   検出済みの収集された会社の値と正規化された会社の値が表示されます。
3. 正規化された値として使用する条件が［正規化された会社］リストまたは［収集された会社］リストに表示されない場合は、［新規会社］をクリックして会社を追加し、前のステップを繰り返します。
4. （オプション）権限のない会社を正規化された権限のある会社に変更します (P. 120)。
5. ［収集された会社］リストの検出済みの値を［正規化された会社］の値にマップします。

   会社正規化ルールのリストが定義され、照合処理の実行中に参照されます。

関連項目:

会社正規化ルール (P. 117)

会社正規化ルールの更新

重要: 正規化ルールは、サービス プロバイダに関連付けられたすべてのテナントと公開データに適用されます。 このタスクを実行するユーザが、照合管理アクセスが有効な役割に属することを確認します。

検出済みの会社を正規化する方法を変更する場合は、会社正規化ルールを更新します。この更新が照合処理に影響を与える場合があります。会社の正規化ルールを更新するには、ルールを削除して新しいルールを定義します。

製品によって、正規化ルールの更新が監視されます。正規化ルールを変更すると、ハードウェア照合エンジンは、新しいルールを使用してアセットを照合できるように、アセットの照合を処理します。 前のハードウェア照合エンジンの処理によって照合されたすべてのアセットは、新しい正規化ルールに基づいて照合結果を変更する必要があるかどうかを判断するために、もう一度評価されます。

会社正規化ルールを削除すると、従属会社は権限のないステータスに戻り、［収集された会社］リストに表示されます。 従属会社が製品に定義済みの会社であった場合、その会社は［正規化ルール］ページの［正規化された会社］リストにも表示されます。

会社正規化ルールを更新する方法

1. ［ディレクトリ］-［リスト管理］-［会社ルール］をクリックします。
2. 変更する正規化ルールを削除 (P. 127) します。
3. 新しい会社正規化ルールを定義します (P. 118)。

関連項目:

会社正規化ルール (P. 117)

権限のない会社から権限のある正規化された会社への変更

重要: 正規化ルールは、サービス プロバイダに関連付けられたすべてのテナントと公開データに適用されます。 このタスクを実行するユーザが、照合管理アクセスが有効な役割に属することを確認します。

収集された会社は、［会社の正規化］ページの［正規化された会社］リストにある権限のある会社のみにマップできます。［正規化された会社］リストの製品に定義済みの会社は、最初権限のないステータスになっています。［正規化された会社］リストにある製品に定義済みの会社を、権限のある正規化された会社に変更し、その会社に収集された会社をマップすることができます。

注: 検出済みの収集された会社の会社正規化ルールのみがハードウェア照合に影響します。

権限のない会社を権限のある正規化された会社に変更する方法

1. ［ディレクトリ］-［リスト管理］をクリックします。
2. 左側で［正規化］を展開し、正規化のタイプを選択します。

   検出された収集値と正規化された値が表示されます。
3. ［正規化された会社］セクションの［権限レコードのみを表示します］チェック ボックスをオフにします。
4. ［正規化された会社］セクションの［実行］をクリックします。

収集済みで製品に定義済みの会社のうち、権限がなく、まだ権限のある会社にマップされていない会社は正規化済みリストに表示され、会社名の横に［上書き］アイコンが付きます。

5. *正規化済み*リストで、権限のある会社に変更する権限のない会社の左側にある［上書き］アイコンをクリックします。

   権限のない会社が権限のある正規化された会社に変更されます。

6. ［正規化された会社］セクションで他のアクションを実行する前に、新しく権限のある正規化された会社に収集された会社をマップします。

   注: 新しく権限のある会社に、少なくとも 1 つの収集された会社がマップされるまで、その会社は権限のある会社として保存されません。

   新しく権限のある正規化された会社とその正規化ルールが保存されます。

関連項目:

会社正規化ルールの定義 (P. 118)
会社正規化ルール (P. 117)

オペレーティング システム正規化ルール

オペレーティング システム正規化ルールは、ユーザのコンピュータを管理するオペレーティング システム（たとえば Windows XP Professional、Windows Server 2008 Enterprise Edition、Windows Vista Enterprise Edition など）を対象としています。

収集されたオペレーティング システム

収集されたオペレーティング システムとは、常に検出済みのオペレーティング システムを表します。 収集されたオペレーティング システムは権限のないステータスです。 権限のない収集されたオペレーティング システムを、正規化された権限のあるオペレーティング システムにマップします。

正規化されたオペレーティング システム

正規化されたオペレーティング システムとは、常に*製品に定義済みのオペレーティング システム*を表します。 製品に定義済みのオペレーティング システムは、ユーザ入力と CA MDB を共有する他の製品から収集されます。製品に定義済みのオペレーティング システムは、常に権限のあるステータスです。 権限のあるステータスの場合は、オペレーティング システムに正規化ルールを持たせることができます。 1 つ以上の収集されたオペレーティング システムを権限のあるオペレーティング システムにマップする場合に、権限のある正規化されたオペレーティング システムに対する正規化ルールを定義します。

従属オペレーティング システム

正規化ルールでは、権限のない収集されたオペレーティング システムを正規化された権限のあるオペレーティング システムにマップすると、権限のないオペレーティング システムが権限のあるオペレーティング システムに従属します。

オペレーティング システム正規化ルールの定義

重要: 正規化ルールは、サービス プロバイダに関連付けられたすべてのテナントと公開データに適用されます。 このタスクを実行するユーザが、照合管理アクセスが有効な役割に属することを確認します。

照合ルールにアセット一致基準 (P. 130)が含まれる場合に必ず照合処理の実行中に適用される、オペレーティング システム正規化ルールを定義できます。 オペレーティング システム情報を含むすべてのアセットの一致基準では、自動的にオペレーティング システム正規化ルールが適用されます。

正規化ルールでは、権限のない収集されたオペレーティング システムを正規化された権限のあるオペレーティング システムにマップすると、権限のないオペレーティング システムが権限のあるオペレーティング システムに従属します。 従属オペレーティング システムになると、［収集されたオペレーティング システム］リストには表示されません。従属オペレーティング システムを含む正規化ルールを削除する (P. 127)と、従属オペレーティング システムは権限のないステータスに戻り、［収集されたオペレーティング システム］リストに表示されます。

オペレーティング システム正規化ルールを定義する方法

1. ［ディレクトリ］-［リスト管理］をクリックします。
2. 左側で［正規化］を展開し、［オペレーティング システムの正規化］を選択します。

   検出済みの［収集されたオペレーティング システム］の値と、［正規化されたオペレーティング システム］の値が表示されます。
3. 正規化された値として使用する条件が［正規化されたオペレーティング システム］リストまたは［収集されたオペレーティング システム］リストに表示されない場合は、［新規オペレーティング システム］をクリックしてオペレーティング システムを追加し、前のステップを繰り返します。
4. ［収集された OS］リストの検出済みの値を［正規化された OS］の値にマップします。

   オペレーティング システム正規化ルールのリストが定義され、照合処理の実行中に参照されます。

関連項目:

オペレーティング システム正規化ルール (P. 121)

オペレーティング システム正規化ルールの更新

重要: 正規化ルールは、サービス プロバイダに関連付けられたすべてのテナントと公開データに適用されます。 このタスクを実行するユーザが、照合管理アクセスが有効な役割に属することを確認します。

検出済みのオペレーティング システムを正規化する方法を変更する場合は、オペレーティング システム正規化ルールを更新します。 この更新は、アセットの照合時のオペレーティング システムの値に影響する場合があります。オペレーティング システムの正規化ルールを更新するには、ルールを削除して新規ルールを定義します。

製品によって、正規化ルールの更新が監視されます。 ユーザがオペレーティング システム正規化ルールを変更したときに、オペレーティング システムの照合ルールの更新オプションが有効である場合は、ハードウェア照合エンジンによってオペレーティング システムの値が変更され、アセットの照合時に新しく正規化された名前になります。

重要: パブリック テナント データに適用されるオペレーティング システムの正規化ルールを変更すると、アセットが特定のオペレーティング システムを使用しているかどうかに応じて、すべてのテナントの検出済みのアセットに影響する場合があります。

オペレーティング システム正規化ルールを削除すると、従属オペレーティング システムは権限のないステータスに戻り、［正規化ルール］ページの［収集されたオペレーティング システム］リストに表示されます。

オペレーティング システム正規化ルールを更新する方法

1. ［ディレクトリ］-［リスト管理］-［オペレーティング システム ルール］をクリックします。
2. 変更する正規化ルールを削除 (P. 127) します。
3. 新しいオペレーティング システム正規化ルールを定義します (P. 122)。

関連項目:

オペレーティング システム正規化ルール (P. 121)

システム モデル正規化ルール

システム モデル正規化ルールは、コンピュータ（たとえば Lenovo ThinkPad T400、Lenovo ThinkCentre M58 など）のハードウェア デバイスを対象としています。

収集されたシステム モデル

収集されたシステム モデルとは、常に検出済みのシステム モデルを表します。収集されたシステム モデルは権限のないステータスです。権限のない収集されたシステム モデルを、正規化された権限のあるシステム モデルにマップします。

正規化されたシステム モデル

正規化されたシステム モデルとは、常に*製品に定義済みのシステム モデル*を表します。製品に定義済みのシステム モデルは、ユーザ入力と CA MDB を共有する他の製品から収集されます。 製品に定義済みのシステム モデルは、常に権限のあるステータスです。権限のあるステータスの場合は、システム モデルに正規化ルールを持たせることができます。1 つ以上の収集されたシステム モデルを権限のあるシステム モデルにマップする場合に、権限のある正規化されたシステム モデルに対する正規化ルールを定義します。

従属システム モデル

正規化ルールでは、権限のない収集されたシステム モデルを正規化された権限のあるシステム モデルにマップすると、権限のないシステム モデルが権限のあるシステム モデルに従属します。

システム モデル正規化ルールの定義

重要: 正規化ルールは、サービス プロバイダに関連付けられたすべてのテナントと公開データに適用されます。 このタスクを実行するユーザが、照合管理アクセスが有効な役割に属することを確認します。

照合ルールにアセット一致基準 (P. 130)が含まれる場合に必ず照合処理の実行中に適用される、システム モデル正規化ルールを定義できます。システムモデル情報を含むすべてのアセットの一致基準では、自動的にシステム モデル正規化ルールが適用されます。

正規化ルールでは、権限のない収集されたシステム モデルを正規化された権限のあるシステム モデルにマップすると、権限のないシステム モデルが権限のあるシステム モデルに従属します。 従属システム モデルになると、［収集されたシステム モデル］リストには表示されません。従属システム モデルを含む正規化ルールを削除する (P. 127)と、従属システム モデルは権限のないステータスに戻り、［収集システムモデル］リストに表示されます。

システム モデル正規化ルールを定義する方法

1. ［ディレクトリ］-［リスト管理］をクリックします。
2. 左側で［正規化］を展開し、［システム モデル正規化］を選択します。

   検出済みの収集されたシステム モデル名と製造元名の値、および正規化されたシステム モデル名と製造元名の値が表示されます。
3. 正規化された値として使用する条件が［正規化されたシステム モデル］リストまたは［収集されたシステム モデル］リストに表示されない場合は、［新規システム モデル］をクリックしてシステム モデルを追加し、前のステップを繰り返します。
4. ［収集されたシステム モデル］リストの検出済みの値を［正規化されたシステム モデル］の値にマップします。

   システムモデル正規化ルールのリストが定義され、照合処理の実行中に参照されます。

関連項目:

システム モデル正規化ルール (P. 124)

システム モデル正規化ルールの更新

重要: 正規化ルールは、サービス プロバイダに関連付けられたすべてのテナントと公開データに適用されます。 このタスクを実行するユーザが、照合管理アクセスが有効な役割に属することを確認します。

検出済みのシステム モデルを正規化する方法を変更する場合は、システム モデル正規化ルールを更新します。この更新が照合処理に影響を与える場合があります。システム モデルの正規化ルールを更新するには、ルールを削除して新しいルールを定義します。

製品によって、正規化ルールの更新が監視されます。正規化ルールを変更すると、ハードウェア照合エンジンは、新しいルールを使用してアセットを照合できるようにアセットを処理します。前のハードウェア照合エンジンの操作によって照合されたすべてのアセットは、新しい正規化ルールに基づいて照合結果を変更する必要があるかどうかを判断するために、もう一度評価されます。

システム モデル正規化ルールを削除すると、従属システム モデルは権限のないステータスに戻り、［正規化ルール］ページの［収集されたシステム モデル］リストに表示されます。

システム モデル正規化ルールを更新する方法

1. ［ディレクトリ］-［リスト管理］-［システム モデル ルール］をクリックします。
2. 変更する正規化ルールを削除 (P. 127) します。
3. 新しいシステム モデル正規化ルールを定義します (P. 124)。

関連項目:

システム モデル正規化ルール (P. 124)

正規化ルールの表示

重要: 正規化ルールは、サービス プロバイダに関連付けられたすべてのテナントと公開データに適用されます。このタスクを実行するユーザが、照合管理アクセスが有効な役割に属することを確認します。

正規化ルールを検索および表示して、収集された値と正規化された値のマッピングを確認することができます。この情報は、ハードウェア照合処理の実行中に使用されます。

正規化ルールを表示する方法

1. ［ディレクトリ］-［リスト管理］をクリックします。
2. 左側で［正規化］を展開し、表示する正規化ルールのタイプを選択します。
3. 正規化のマッピング ルールを表示する正規化された値または収集された値を検索します。

   各正規化ルールの収集された値、およびそれに対応する正規化された値が、［検索結果］セクション内に表示されます。

正規化ルールの削除

重要: 正規化ルールは、サービス プロバイダに関連付けられたすべてのテナントと公開データに適用されます。 このタスクを実行するユーザが、照合管理アクセスが有効な役割に属することを確認します。

照合処理の実行中にアセット一致基準に正規化処理を適用する必要がなくなった場合、または正規化ルールを変更する場合には、正規化ルールを削除します。会社、オペレーティング システム、またはシステム モデルの正規化ルールを変更するには、ルールを削除して新しいルールを定義します。

会社正規化ルールを削除すると、従属会社は権限のないステータスに戻り、［収集された会社］リストに表示されます。 従属会社が製品に定義済みの会社であった場合、その会社は［正規化ルール］ページの［正規化された会社］リストにも表示されます。オペレーティング システム正規化ルールを削除すると、従属オペレーティング システムは権限のないステータスに戻り、［正規化ルール］ページの［収集されたオペレーティング システム］リストに表示されます。システム モデル正規化ルールを削除すると、従属システム モデルは権限のないステータスに戻り、［正規化ルール］ページの［収集されたシステム モデル］リストに表示されます。

正規化ルールを削除する方法

1. ［ディレクトリ］-［リスト管理］をクリックします。
2. 左側で［正規化］を展開し、削除するルールの正規化ルール タイプを選択します。
3. 正規化ルールを削除する正規化された値または収集された値を検索します。

   各正規化ルールの収集された値、およびそれに対応する正規化された値が、［検索結果］セクション内に表示されます。
4. 削除するルールを選択します。
5. ［ルールの削除］をクリックします。

   正規化ルールが削除されます。 アセット一致基準では、照合処理の実行中にこのルールを適用しません。

正規化ルールの更新

検出済みのシステム モデルまたは会社を正規化する方法を変更する場合は、システム モデル正規化ルールまたは会社正規化ルールを更新します。この更新が照合処理に影響を与える場合があります。検出済みのオペレーティング システムを正規化する方法を変更する場合は、オペレーティング システム正規化ルールを更新します。この更新は、アセットの照合時のオペレーティング システムの値に影響する場合があります。 正規化ルールを更新するには、ルールを削除して新しいルールを定義します。

製品によって、正規化ルールの更新が監視されます。システム モデルまたは会社の正規化ルールを変更すると、ハードウェア照合エンジンは、新しいルールを使用してアセットを照合できるように、アセットの照合処理を実行します。前の操作によって照合されたすべてのアセットは、新しい正規化ルールに基づいて照合結果を変更する必要があるかどうかを判断するために、もう一度評価されます。ユーザがオペレーティング システム正規化ルールを変更したときに、オペレーティング システムの照合ルールの更新オプションが有効である場合、ハードウェア照合エンジンによってオペレーティング システムの値が変更され、アセットの照合時に新しく正規化された名前になります。

会社正規化ルールを削除すると、従属会社は権限のないステータスに戻り、［収集された会社］リストに表示されます。 従属会社が製品に定義済みの会社であった場合、その会社は［正規化ルール］ページの［正規化された会社］リストにも表示されます。オペレーティング システム正規化ルールを削除すると、従属オペレーティング システムは権限のないステータスに戻り、［正規化ルール］ページの［収集されたオペレーティング システム］リストに表示されます。システム モデル正規化ルールを削除すると、従属システム モデルは権限のないステータスに戻り、［正規化ルール］ページの［収集されたシステム モデル］リストに表示されます。

関連項目:

会社正規化ルールの定義 (P. 118)
オペレーティング システム正規化ルールの定義 (P. 122)
システム モデル正規化ルールの定義 (P. 124)
正規化ルールの削除 (P. 127)

照合ルールの定義

重要: このタスクを実行するユーザが、照合管理アクセスが有効な役割に属することを確認します。

照合ルールを使用して、ハードウェア照合エンジンが実行する処理オプションおよびアクションを定義します。テナントごとに 1 つの照合ルールを定義できます。

注: テナントごとに設定できる照合ルールは 1 つのみです。 そのため、ルールを非アクティブにすると、非アクティブ ルールがテナントと関連付けられた唯一の照合ルールになります。 テナントの照合ルールを変更する場合、現在の照合ルールを更新 (P. 139)するか、現在の照合ルールを削除 (P. 140)して新しいルールを定義することができます。 ルールを削除すると、ルールに関連付けられた検出アセットと所有アセット間のアセット一致リンクもすべて削除されます。

照合ルールを定義する方法

1. ［管理］-［照合管理］をクリックします。
2. 左側の［新規照合ルール］をクリックします。
3. 該当する場合は、定義している照合ルールに関連付けられたテナントを選択します。
4. 照合ルール情報を入力して［保存］をクリックします。

   注: 個別のテナントの照合プロセスを一時停止する場合は、［非アクティブ］チェック ボックスをオンにします。［非アクティブ］チェック ボックスをオンにすると、ハードウェア照合エンジンはルールを処理しません（ルールに対してアセット一致またはデータ更新は行われません）。 たとえば、正規化ルールの定義やアセット一致エラーのトラブルシューティングを行う間、ルールを一時的に非アクティブにすることができます。 既存のルールを非アクティブにしたとき、検出アセットや所有アセットがすでに一致している場合は、一致リンクが保存されます。

   ［アセット更新の監視］および［一致アセット］チェック ボックスが選択できるようになります。
5. （オプション）［アセット更新の監視］チェック ボックスをオンにして、ハードウェア照合エンジンで自動的に更新する必要がある照合更新オプションを定義 (P. 130)します。

   ［更新オプション］ペインが開きます。
6. （オプション）［一致アセット］チェック ボックスをオンにして、ハードウェア照合エンジンで適用する必要があるアセット一致基準を定義 (P. 130)します。

   ［一致ルール］ペインが表示されます。

   注: 一致基準を定義しない場合、ハードウェア照合エンジンはデフォルトのアセット一致基準を使用します。その場合、所有シリアル番号を検出シリアル番号に一致させます。
7. ［保存］をクリックします。

   新しい照合ルールが定義されます。

照合の更新オプションの定義

重要: このタスクを実行するユーザが、照合管理アクセスが有効な役割に属することを確認します。

ハードウェア照合エンジンが対応する検出済みのアセット フィールドで新しい値を検出した場合、選択済みの重要な所有アセット フィールドに変更を適用できます。ハードウェア照合エンジンは重要なフィールドを監視します。このフィールドは、対応する検出済みのアセットで変更が検出された場合に選択して更新される所有アセット フィールドです。対応する検出済みのアセットで検出された変更を自動的に更新する所有アセット フィールドを指定します。

照合の更新オプションを定義する方法

1. ［管理］-［照合管理］をクリックします。
2. 左側の［照合ルールの検索］をクリックします。
3. 利用可能な照合ルールのリストを検索して見つけます。
4. 照合の更新オプションを定義する照合ルールをクリックします。
5. ［アセット更新の監視］チェック ボックスをオンにして、ハードウェア照合エンジンに自動更新を適用させます。

   ［更新オプション］ペインが開きます。
6. 自動的に更新するフィールドのチェック ボックスをオンにします。

   注: ［ホスト名］チェック ボックスをオンにして、［ホスト名をアセット名にコピー］更新オプションを有効にして選択します。
7. ［保存］をクリックします。

   照合の新しい更新オプションが定義されます。

アセット一致基準

ハードウェア照合エンジンは、照合ルールに対して定義した*アセット一致基準*に基づき、所有アセットと検出されたアセットを一致させます。 この基準は、CA APM および検出製品の両方のフィールド値のリストに基づき、所有アセットと検出されたアセットの一致要因を定義します。ハードウェア照合エンジンは管理対象のアセットをすべて識別し、照合プロセス中に必要なデータを提供します。

照合ルールに関連付けられたアセット一致基準を変更すると、ハードウェア照合エンジンは、次回ルールを処理するときに、新しい基準を使用して照合済みアセットを再処理します。

以下のアセット フィールド値を一致させることができます。

所有アセットのフィールド	検出されたアセットのフィールド
代替ホスト名	ホスト名
代替ホスト名	レジストリ アセット名
代替 ID	BIOS アセット タグ
アセットの別名	BIOS アセット タグ
アセットの別名	ホスト名
アセット名	ホスト名
クラス	システム タイプ
ホスト名	ホスト名
ホスト名	レジストリ アセット名
MAC アドレス	MAC アドレス
MAC アドレスとホスト名	MAC アドレスとホスト名
製造元	システム ベンダー
モデル名	システム モデル
前のアセット タグ	BIOS アセット タグ
シリアル番号	シリアル番号
サブクラス	システム タイプ

この製品は、所有されたアセットと検出されたアセットのアセット一致フィールドをモニタします。アセット一致に使用される所有アセット フィールド値を変更すると、ハードウェア照合エンジンは次回の照合プロセスで、新しい値を使用して変更済みの所有アセットを再処理します。

同様に、アセット一致に使用できる CA MDB 内の検出されたアセット フィールド値が CA Client Automation またはサードパーティの検出製品の検出コンポーネントによって変更された場合、ハードウェア照合エンジンは次回の照合プロセス中に、新しい値を使用して変更された所有アセットを再処理します。

また、この製品は会社モデルとシステム モデルの正規化ルールの変更もモニタします。 これらのルールは、所有アセットと検出されたアセットのアセット一致に影響します。 いずれかの正規化ルールを変更すると、ハードウェア照合エンジンはアセット一致プロセスを実行し、新しいルールを使用してアセットを一致させます。ハードウェア照合エンジンの前回の実行結果で一致していたアセットはすべて、新しい正規化ルールで一致が変わるかどうかを判断するために再評価されます。

アセット照合時の非アクティブ ステータスの影響

ハードウェア照合処理は、CA APM によって作成された、照合から除外 (P. 134)されないアクティブな所有アセットをすべて処理します。アセット、モデル、アセット ファミリ、または会社が非アクティブである場合、所有アセットと検出済みアセットの間の照合リンクに対して、以下のように影響します。

非アクティブな所有アセット

- ハードウェア照合エンジンがアセットと検出済みのアセットを照合する前に所有アセットが非アクティブである場合、その所有アセットは照合されません。
- アセットの照合後に所有アセットが非アクティブになると、ハードウェア照合エンジンは次に照合ルールを処理するときに、照合リンクを消去します。

非アクティブなモデル

- ハードウェア照合エンジンが検出済みアセットと任意のモデルに基づく所有アセットを照合する前に、そのモデルが非アクティブである場合、その所有アセットは照合されません。
- そのモデルに基づく所有アセットが照合された後にモデルが非アクティブになると、ハードウェア照合エンジンは、次に照合ルールを処理するときに、アセットおよび非アクティブなモデルに基づくその他すべての照合リンクを消去します。

非アクティブなアセット ファミリ

- ハードウェア照合エンジンが検出済みアセットとアセット ファミリ、クラス、またはサブクラスを持つ所有アセットを照合する前に、アセット ファミリ、クラス、またはサブクラスが非アクティブである場合、その所有アセットは照合されません。
- アセット ファミリ、クラス、またはサブクラスを持つ所有アセットが照合された後に、アセット ファミリ、クラス、またはサブクラスが非アクティブになると、ハードウェア照合エンジンは、次に照合ルールを処理するときに、そのアセットおよび非アクティブになったアセット ファミリ、クラス、またはサブクラスに属するその他すべての照合リンクを消去します。

非アクティブな会社

- ハードウェア照合エンジンが検出済みアセットと製造元として会社を持つ所有アセットを照合する前に、その会社が非アクティブである場合、その所有アセットは照合されません。
- 製造元として会社を持つ所有アセットが照合された後に、その会社が非アクティブになると、ハードウェア照合エンジンは、次に照合ルールを処理するときに、そのアセットと非アクティブになった会社に関連するその他すべての照合リンクを消去します。

注: アセット、モデル、アセット ファミリ、および会社を非アクティブにする場合の詳細については、ユーザ ガイドを参照してください。

関連項目:

照合処理からのアセット ファミリの除外 (P. 135)

アセット一致基準の定義

重要: このタスクを実行するユーザが、照合管理アクセスが有効な役割に属することを確認します。

この製品は、照合ルールに対して定義した一致基準に基づき、所有アセットと検出されたアセットを一致させようとします。所有フィールド値が検出フィールド値と一致する場合、ハードウェア照合エンジンはアセット照合を実行します。

アセット一致基準を定義する方法

1. ［管理］-［照合管理］をクリックします。
2. 左側の［照合ルールの検索］をクリックします。

3. 検索して利用可能な照合ルールのリストを見つけます。
4. アセット一致基準を定義する照合ルールをクリックします。

   ［照合ルールの詳細］ページが表示されます。
5. ［一致アセット］チェック ボックスをオンにして、ハードウェア照合エンジンでアセット一致基準を適用します。

   ［一致ルール］ペインが表示されます。
6. 一致させる所有フィールドと検出フィールドを選択し、［基準の追加］をクリックします。

   新しいアセット一致基準レコードが［一致基準］セクションに追加され、新しいトリミング レコードが［トリミング］セクションに追加されます。
7. ［一致基準］セクション内の新しい基準の横にある［レコード編集］アイコンをクリックします。
8. 一致基準オプションを選択します。
9. （オプション）［トリミング］セクションで［レコード編集］アイコンをクリックし、アセット一致基準のトリミング オプションを選択します。 たとえば、あるサイトで検出されたコンピュータ名に 3 文字の地域番号のプレフィックスがあり、所有アセットのコンピュータ名には地域番号がないとします。 この場合、検出されたコンピュータ名の左から 3 文字をトリミングするトリミング レコードをアセット一致基準に対して作成します。
10. （オプション）引き続き、照合ルールに一致基準を追加します。
11. ［保存］をクリックします。

    新しいアセット一致基準が定義され、照合ルールが保存されます。

注: 照合ルールを保存した後に、アセット一致基準内の一致フィールドを別のフィールドに変更する場合、その基準を削除して新しい基準を作成してください。

照合プロセスから所有アセットを除外する

照合プロセスから個々の所有アセットを除外できます。照合からアセットを除外する理由にはいくつかあります。以下に例を示します。

- 所有アセットと一致する検出されたアセットが存在せず、不一致アセットのリストに追加され続けている。 たとえばラップトップなど、ネットワークに一切接続されないアセットや廃止されたアセットの所有データが、CA APM 内に保存されている場合があります。
- 会社で特定のクラスのアセット（たとえばラップトップ）を照合から除外する必要がある。

ハードウェア照合エンジンがアセットを検出されたアセットと一致させる前に所有アセットを照合プロセスから除外すると、所有アセットは一致に使用されません。 アセット一致の実行後に所有アセットが照合プロセスから除外されると、ハードウェア照合エンジンは次回照合ルールを処理するときに、一致のリンクをクリアします。 その所有アセットは一致に使用できなくなります。

注: 除外されたアセットのアセット ファミリがハードウェア照合プロセスの対象に設定されている場合でも、アセットは引き続きプロセスから除外されます。アセット ファミリがハードウェア照合プロセスから除外された (P. 135)場合、除外されたアセット ファミリに属するアセットがすべて除外されます。

照合プロセスから所有アセットを除外する方法

1. ［アセット］-［アセット検索］をクリックします。
2. 検索して利用可能なアセットのリストを見つけます。
3. 照合プロセスから除外するアセットをクリックします。
4. ［基本情報］セクションで、［照合除外］チェック ボックスをオンにします。
5. ［保存］をクリックします。

   今後、その所有アセットは照合の対象外になります。

関連項目:

アセット照合時の非アクティブ ステータスの影響 (P. 132)

照合処理からのアセット ファミリの除外

アセット ファミリのすべての所有アセットを、ハードウェア照合処理から除外できます。アセット ファミリを照合から除外する理由の一部には、以下の例が含まれます。

- アセット ファミリのアセットが一致する検出済みアセットを持っておらず、未照合アセットのリスト内に含まれ続ける場合。 たとえば、サービス アセット ファミリにあるアセットはネットワークに接続されておらず、その所有権データが CA APM 内に保存される場合などです。
- アセット ファミリがソフトウェアである場合。本製品ではソフトウェアの照合を行いません。
- 会社でアセット ファミリを非アクティブにしたいと考えている場合。ハードウェア照合処理は、CA APM によって作成されたアクティブな所有アセットを処理します。

ハードウェア照合エンジンがアセット ファミリの所有アセットと検出済みのアセットを照合する前に、アセット ファミリを照合処理から除外すると、その所有アセットは照合に使用できません。アセット ファミリの所有アセットが照合された後に、アセット ファミリを照合処理から除外すると、ハードウェア照合エンジンは次に照合ルールを処理するときに照合リンクを消去します。その所有アセットは照合に使用できません。

照合処理からアセット ファミリを除外する方法

1. ［ディレクトリ］-［リスト管理］をクリックします。
2. 左側で［アセット リスト］を展開し、［アセット ファミリ］をクリックします。
3. 照合処理から除外するアセット ファミリの［レコード編集］アイコンをクリックします。
4. 以下のいずれかのオプションを実行します。
   - ［ハードウェア照合］チェック ボックスをオフにします。
   - ［ソフトウェア］チェック ボックスをオンにします。
   - ［非アクティブ］チェック ボックスをオンにします。
5. アセット ファミリ オブジェクトの［レコード編集を完了］アイコンを選択します。
6. ［保存］をクリックします。

   除外されたアセット ファミリのアセットは、今後の照合には含まれなくなります。

照合処理からのアセット ファミリ クラスまたはサブクラスの除外

アセット ファミリ クラスまたはサブクラスのすべての所有アセットを、ハードウェア照合処理から除外できます。 たとえば、会社でアセット ファミリ クラスまたはサブクラスを非アクティブにしたい場合には、アセットを除外できます。ハードウェア照合処理は、CA APM によって作成されたアクティブな所有アセットを処理します。

ハードウェア照合エンジンがアセット ファミリ クラスまたはサブクラスの所有アセットと検出済みのアセットを照合する前に、アセット ファミリ クラスまたはサブクラスを照合処理から除外すると、その所有アセットは照合に使用できません。 アセット ファミリ クラスまたはサブクラスの所有アセットが照合された後に、アセット ファミリ クラスまたはサブクラスを照合処理から除外すると、ハードウェア照合エンジンは次に照合ルールを処理するときに照合リンクを消去します。 その所有アセットは照合に使用できません。

照合処理からアセット ファミリ クラスまたはサブクラスを除外する方法

1. ［ディレクトリ］-［リスト管理］をクリックします。
2. 左側で［アセット リスト］を展開し、［アセット ファミリ］をクリックします。
3. 照合処理から除外するクラスまたはサブクラスを持つアセット ファミリの［レコード編集］アイコンをクリックします。
4. ［クラス リスト］をクリックします。
5. 照合処理から除外するクラス（または除外するサブクラスを持つクラス）の［レコード編集］アイコンをクリックします。
6. クラス全体を除外する場合は、［非アクティブ］チェック ボックスをオンにして、アセット ファミリ クラスの［レコード編集を完了］アイコンをクリックします。

   注: 照合処理からクラス全体ではなくサブクラスを除外する場合は、この手順をスキップします。
7. サブクラスを除外する場合は、［サブクラス リスト］をクリックします。
8. 照合処理から除外するサブクラスの［レコード編集］アイコンをクリックします。
9. ［非アクティブ］チェック ボックスをオンにして、アセット ファミリ サブクラスの［レコード編集を完了］アイコンをクリックします。
10. ［保存］をクリックします。

    除外されたアセット ファミリ クラスまたはサブクラスは、今後の照合には含まれなくなります。

照合結果の表示

重要: このタスクを実行するユーザが、照合管理アクセスが有効な役割に属することを確認します。

ハードウェア照合エンジンが照合ルールのアクションを処理するとき、エンジンはデータベース内のメッセージ キューにレコードを書き込みます。その照合ログ メッセージのメッセージ キューを検索できます。 メッセージ キューは設定された日数の間、ログ メッセージを保存します。

注: ハードウェア照合エンジンのロギング レベルを変更すると、メッセージ キューに書き込まれる詳細のレベルを制御できます。また、メッセージ キュー内でのメッセージの保存日数も制御できます。 ロギング レベルとメッセージ キューの保存設定の詳細については、「ハードウェア照合エンジンの設定」を参照してください。

メッセージ キューを表示する方法

1. ［管理］-［照合管理］をクリックします。
2. 左側の［照合メッセージ検索］をクリックします。

   ［検索結果］セクションに、メッセージ キューの照合ログ メッセージが表示されます。
3. （オプション）検索して、メッセージ キュー内のメッセージを見つけます。

注: スプレッドシート アプリケーションで使用されるカンマ区切り値（CSV）ファイルにメッセージ キューをエクスポートできます。 また、レポートを生成して、照合に関係する環境の情報を表示できます。 レポートの生成の詳細については、「ユーザ ガイド」を参照してください。

未照合の検出済みレコードからのアセットの追加

ハードウェア照合プロセスは、どの所有アセットにも一致しないアセットを検出する場合があります。ネットワーク内のすべてのアセットを追跡し管理できるように、リポジトリに不一致アセットを追加できます。 レポートの結果を生成してエクスポートし、Data Importer によってレポート結果をインポートすることにより、未照合のアセットを追加できます。

重要: CA APM にデータをインポートする前に、データを確認して正確性と一意性を保証します。

未照合の検出済みレコードからアセットを追加する方法

1. BusinessObjects Enterprise InfoView にログインします。

   ［レポート］ペインが開きます。
2. ［Document List］をクリックします。
3. ［Public Folder］-［CA Reports］フォルダを展開します。
4. ［CA ITAM］をクリックします。
5. どの所有アセットにも一致しない検出済みアセットを識別するレポートの横にあるアイコンを、ダブルクリックします。
6. レポート用の検索条件を入力します。

   注: レポートを生成する場合に、テナントを 1 つだけ選択します。一度に 1 つのテナントについてデータをインポートできます。

7. ［クエリの実行］をクリックします。
8. エクスポートできるフラット ファイル形式用のリンクをクリックします。

   そのレポートは、ユーザが表示してエクスポートできるドキュメント形式に変換されます。
9. ドキュメントを CSV ファイルとして保存します。
10. 管理者として CA APM にログインします。
11. ［管理］、［Data Importer］、［新規インポート］にナビゲートします。
12. ［データ ファイル］フィールドで CSV ファイル名を指定します。
13. 主なインポート先オブジェクトおよび区切り文字を選択します。

    重要: レポートを生成したときに選択したのと同じテナントを選択します。
14. ［詳細設定］領域で、以下のオプションが選択されていることを確認します。
    - 挿入または更新
    - セカンダリ ルックアップ オブジェクトの作成
    - セカンダリ ルックアップ オブジェクトの更新
    - セカンダリ ルックアップ オブジェクト エラー設定のエラー
15. ［保存］をクリックします。
16. 列マッピングを指定します。
17. ［スケジュール］領域の［サブミットする］をクリックしてインポート プロセスを開始します。

    未照合のアセットがデータ リポジトリに追加されます。

照合ルールの更新

重要: このタスクを実行するユーザが、照合管理アクセスが有効な役割に属することを確認します。

照合ルールの情報を更新できます。

照合ルールに関連付けられたアセット一致基準を変更すると、ハードウェア照合エンジンは、次回ルールを処理するときに、新しい基準を使用して照合済みアセットを再処理します。

照合ルールを更新する方法

1. ［管理］-［照合管理］をクリックします。
2. 左側の［照合ルールの検索］をクリックします。

3. 利用可能な照合ルールのリストを検索して見つけます。
4. 更新する照合ルールをクリックします。
5. 照合ルールの新しい情報を入力します。

   注: 個別のテナントの照合プロセスを一時停止する場合は、［非アクティブ］チェック ボックスをオンにします。［非アクティブ］チェック ボックスをオンにすると、ハードウェア照合エンジンはルールを処理しません（ルールに対してアセット一致またはデータ更新は行われません）。 たとえば、正規化ルールの定義やアセット一致エラーのトラブルシューティングを行う間、ルールを一時的に非アクティブにすることができます。 既存のルールを非アクティブにしたとき、検出アセットや所有アセットがすでに一致している場合は、一致リンクが保存されます。
6. ［保存］をクリックします。

   照合ルールが更新されます。

注: 照合ルールを保存した後に、アセット一致基準内の一致フィールドを別のフィールドに変更する場合、その基準を削除して新しい基準を作成してください。

照合ルールの削除

重要: このタスクを実行するユーザが、照合管理アクセスが有効な役割に属することを確認します。

定義された照合ルールを削除できます。 ルールを削除すると、ルールに関連付けられた検出アセットと所有アセット間のアセット一致リンクもすべて削除されます。

テナントごとに設定できる照合ルールは 1 つのみです。テナントの照合ルールを変更する場合は、現在の照合ルールを更新 (P. 139)するか、現在のルールを削除して新しい照合ルールを定義 (P. 128)します。

注: 個別のテナントの照合プロセスを一時的に停止する場合は、ルールを非アクティブにすることもできます。ルールを非アクティブにするには、ルールを更新 (P. 139)し、［非アクティブ］チェック ボックスをオンにします。 検出アセットや所有アセットがルールとすでに一致している場合は、一致リンクが保存されます。

照合ルールを削除する方法

1. ［管理］-［照合管理］をクリックします。
2. 左側の［照合ルールの検索］をクリックします。

3. 利用可能な照合ルールのリストを検索して見つけます。
4. 削除するルールをクリックします。
5. ［削除］をクリックし、照合ルールを削除することを確認します。

   ルールが削除されます。

照合結果のエクスポート

重要: このタスクを実行するユーザが、照合管理アクセスが有効な役割に属することを確認します。

メッセージ キューを表示した後、スプレッドシート アプリケーションで使用されるカンマ区切り値（CSV）ファイルにキューをエクスポートできます。

メッセージ キューをエクスポートする方法

1. ［管理］-［照合管理］をクリックします。
2. 左側の［照合メッセージ検索］をクリックします。

   ［検索結果］セクションに、メッセージ キューの照合ログ メッセージが表示されます。
3. 検索して、エクスポートする照合ログ メッセージを見つけます。
4. ［CSV へのエクスポート］をクリックします。

   メッセージ キューの検索結果が CSV ファイルにエクスポートされ、CSV ファイルへのリンクが表示されます。

第 5 章: 製品コンポーネントの管理

このセクションには、以下のトピックが含まれています。

製品コンポーネント

CA APM をインストールしたら、手動で多くの製品コンポーネントを設定できます。 さらに、追加のサーバにコンポーネントを追加して、最適なパフォーマンスを維持して拡張を可能にすることができます。 たとえば、ハードウェア照合エンジンまたはその他のコンポーネント サーバを追加できます。柔軟に設定できるため、多くのコンポーネントの設定を変更できます。

注: 各製品コンポーネントの説明については、実装ガイドを参照してください。

製品コンポーネントの設定

重要: このタスクを実行するユーザが、システム設定アクセスが有効な役割に属することを確認します。

製品のインストール中にセットアップされたコンポーネントの設定を変更できます。 たとえば、電子メールを送信するために使用される SMTP サーバの名前を変更できます。

次の手順に従ってください:

1. ［管理］-［システム構成］をクリックします。
2. 左側で、製品コンポーネントを選択します。
3. 次のコンポーネントの新しい設定を入力します。
   - データベース
     - Oracle (P. 144)
     - SQL Server (P. 147)

- Web サーバ (P. 148)
- アプリケーション サーバ (P. 152)
- ハードウェア照合エンジン (P. 153)
- CA EEM (P. 155)
- エクスポート サービス (P. 156)
- Data Importer (P. 157)
- Data Importer エンジン (P. 157)
- LDAP データ インポートおよび同期サービス (P. 159)
- CORA (P. 159)
- ストレージ マネージャ サービス (P. 160)
- イベント サービス (P. 161)
- Common Asset Viewer (P. 164)
- WCF サービス (P. 165)
- SAM - ドライバのインポート (P. 166)
- Software Asset Management （SAM） (P. 166)

4. ［保存］をクリックします。

   設定が保存されます。

Oracle データベースの設定

CA MDB のデータベースとして Oracle を使用している場合、製品をインストールした後に Oracle データベース サーバの設定を変更できます。

以下のフィールドについて説明します。

DBA ユーザ名

ターゲット データベースに接続するためのユーザ名。ユーザ名は特権ユーザ用である必要があります。

デフォルト： sys

リスニング ポート

データベースの接続ポート。

デフォルト： 1521

Oracle サービス名

ターゲット データベース用のサービス名。

デフォルト： orcl

Oracle ネット サービス名

ターゲット データベースのネット サービス名。

デフォルト： orcl

テーブル領域パス

Oracle 表領域のロケーション。

デフォルト： c:¥oracle¥product¥10.2.0¥oradata¥orcl

データ テーブル領域名

データ表領域の名前。

デフォルト： MDB_DATA

データ表領域サイズ

データ表領域に割り当てられるディスク容量。

デフォルト： 400 MB

インデックス テーブル領域名

インデックス表領域の名前。

デフォルト： MDB_INDEX

インデックス表領域サイズ

インデックス表領域に割り当てられるディスク容量。

デフォルト： 100 MB

mdbadmin パスワード

mdbadmin ユーザに関連付けられるパスワード。 新規 CA MDB を作成している場合、これが mdbadmin ユーザに割り当てられるパスワードになります。

コマンド タイムアウト

アプリケーションがデータベースからの応答を待機する時間の最大値。

ストアド プロシージャ コマンド タイムアウト

アプリケーションがデータベース ストアド プロシージャからの応答を待機する時間の最大値。

最大接続プール サイズ

データベースが同時に処理できるリクエストの最大数。

CORA 接続プーリングの有効化

CORA 接続プールを有効にするフラグのプレースホルダ。 現在、CORA は接続プールをサポートしていません。

CORA 接続プールのライフ タイム

CORA 接続プールのライフタイムのプレースホルダ。 現在、CORA は接続プールをサポートしていません。

CORA 接続プール サイズ

CORA 接続プールのサイズのプレースホルダ。 現在、CORA は接続プールをサポートしていません。

最終実行日オプション

インポートされたデータが既存の CA APM データを更新するかどうかを判断します。

注: CA APM は検出されたハードウェア データ インポートを受信し、そのデータを所有権と検出データを一致するために使用します。 CA APM は、在庫の日付を比較することで、インポートされたデータが現在のデータより新しいかどうか判断します。 その後、CA APM はインポートされたデータが既存の CA APM データを更新するかどうか決定します。

デフォルト： 2

注: すべての有効なオプションの説明に関しては以下の表を参照してください。

オプション	定義
1	インポートされたデータで既存の CA APM データを常に更新します。
2	（デフォルト）インポートされたアセットの在庫日付が既存のアセットの在庫日付より新しい場合にのみ既存の CA APM データを更新します。 インポートされたアセットに在庫日付がない場合はエラーが発生し、インポートされたアセット データは既存の CA APM データを更新しません。

オプション	定義
3	インポートされたアセットの在庫日付が既存のアセットの在庫日付より新しい場合にのみ既存の CA APM データを更新します。 インポートされたアセットに在庫日付がない場合、インポートされたデータで既存の CA APM データを更新します。

SQL Server データベースの設定

CA MDB のデータベースとして SQL Server を使用している場合、製品をインストールした後に SQL Server データベース サーバの設定を変更できます。

以下のフィールドについて説明します。

SQL Server ログイン

ターゲット データベースに接続するためのユーザ名。 ユーザ名は SQL Server で割り当てられた sysadmin の役割権限を持つ必要があります。

デフォルト： sa

SQL Server TCP/IP ポート

データベースの接続ポート。

デフォルト： 1433

コマンド タイムアウト

製品がデータベースからの応答を待機する時間の最大値。

ストアド プロシージャ コマンド タイムアウト

製品がデータベース ストアド プロシージャからの応答を待機する時間の最大値。

最大接続プール サイズ

データベースが同時に処理できるリクエストの最大数。

CORA 接続プーリングの有効化

CORA 接続プールを有効にするフラグのプレースホルダ。 現在、CORA は接続プールをサポートしていません。

CORA 接続プールのライフ タイム

CORA 接続プールのライフタイムのプレースホルダ。 現在、CORA は接続プールをサポートしていません。

CORA 接続プール サイズ

CORA 接続プールのサイズのプレースホルダ。 現在、CORA は接続プールをサポートしていません。

SQL Server ホスト名

SQL Server に対して使用されるサーバのホスト名。

最終実行日オプション

インポートされたデータが既存の CA APM データを更新するかどうかを判断します。

注: CA APM は検出されたハードウェア データ インポートを受信し、そのデータを所有権と検出データを一致するために使用します。 CA APM は、在庫の日付を比較することで、インポートされたデータが現在のデータより新しいかどうか判断します。 その後、CA APM はインポートされたデータが既存の CA APM データを更新するかどうか決定します。

デフォルト： 2

注: すべての有効なオプションの説明に関しては以下の表を参照してください。

オプション	定義
1	インポートされたデータで既存の CA APM データを常に更新します。
2	（デフォルト）インポートされたアセットの在庫日付が既存のアセットの在庫日付より新しい場合にのみ既存の CA APM データを更新します。 インポートされたアセットに在庫日付がない場合はエラーが発生し、インポートされたアセット データは既存の CA APM データを更新しません。
3	インポートされたアセットの在庫日付が既存のアセットの在庫日付より新しい場合にのみ既存の CA APM データを更新します。 インポートされたアセットに在庫日付がない場合、インポートされたデータで既存の CA APM データを更新します。

Web サーバの設定

製品をインストールしたら、Web サーバの設定を変更できます。

以下のフィールドについて説明します。

Web サーバまたはロード バランサの IP/ホスト

CA APM インストールでは、デフォルトで、このフィールドに Web サーバのホスト名が設定されます。

- Web サーバが 1 台の環境では、Web サーバのホスト名または IP アドレスを入力できます。
- Web サーバが複数台の環境では、Web サーバのホスト名またはロード バランサの IP アドレスを入力できます。

注: Web サーバをドメイン ネーム システム（DNS）に登録する際、Web サーバ ホスト名として登録されている名前とは別の名前を使用できます。そのような場合、このフィールドにはその別名を指定してください。

認証タイムアウト

ユーザが自動的に製品からログアウトされ、もう一度ログインする必要がある状態になるまでに、ユーザを非アクティブにすることができる時間（ミリ秒）。

デフォルト： 3600000（6 分）

状態データ

ユーザがログオフするまで各ユーザに対してサーバ側で保存される一時ビュー データ。このデータは、データベースまたは Web サーバ ファイル システムに保存できます。状態データの値は、SERVER (FileSystem) または DATABASE です。

キャッシュ タイムアウト

ストアから削除されるキャッシュ ファイルの経過タイムアウト期間。

ユーザがログインすると、ビュー データと一緒にドキュメントがシステム メモリ（キャッシュ）に格納されます。 ユーザがこれらのドキュメントを参照していない場合、ドキュメントは古くなります。 一定時間が経過すると、これらのドキュメントは削除されます。 時間制限は［キャッシュ タイムアウト］です。

オート コンプリート結果数

［オート コンプリート］ドロップダウン リストに表示する値の数。リスト付きのフィールドで、ユーザは値を入力し、製品は一致する値のリストを提供します。 次に、ユーザはこのオート コンプリート リストから値を選択できます。

注: このパラメータの値を小さくした場合、値の大部分を入力しないとリスト内に値が表示されないため、オート コンプリート リストはあまり役に立ちません。 このパラメータの値を大きくした場合、リストの反応が低下する可能性があります。

ホームページ

ログイン後に開くデフォルト CA APM ホーム ページ。

SW Web サービス プロトコル

ストレージ マネージャ サービスにアクセスするために使用されるプロトコル。

［ストレージ マネージャ サービス］は、他の製品コンポーネントへのファイル ストレージ機能を提供します。 他のコンポーネントがストレージ マネージャ サービスと対話する場合、コンポーネントはこのプロトコルを使用します。

SM Web サービス ポート

ストレージ マネージャ サービスが実行されているポート。

このポートは、ストレージ マネージャ サービスがホストされる HTTP ポートです。デフォルトのポート番号は 80 です。［ストレージ マネージャ サービス］が別のポートでホストされるように設定した場合、そのポート番号が表示されます。

EEM バックエンド

CA EEM がインストールされているサーバの名前。 この値はインストール中に入力されます。

レポート Web サービス サーバ

CA Business Intelligence サーバ名およびポート。 この値はインストール中に入力されます。

レポート タイムアウト

CA Business Intelligence （レポート） Web サービスへの接続のタイムアウト（秒単位）。

レポート名

CA Business Intelligence （レポート）エンジンの名前。 この名前は常に「Allegheny Reporting Engine」です。

レポート ユーザ

管理者権限を持った CA Business Intelligence （レポート）ユーザ。

レポート パスワード

レポート ユーザのパスワード。

外部認証ヘッダ

このヘッダは、CA EEM 設定の認証タイプの外部設定と連携して動作します。 外部認証メカニズムは、CA APM Web ページが受信する HTTP ヘッダの情報を設定します。 この情報の一部はユーザ ID です。 外部認証ヘッダは、ユーザ ID 値を設定する変数外部認証の名前です。 外部認証ヘッダ設定は、ユーザ ID 値が提供される外部認証の設定値と一致する必要があります。

送信者アドレス

イベント サービスから送信される通知用の送信者アドレス。

宛先リスト

イベント サービスからの案件に関する電子メール通知を受信する受信者のリスト。

CC リスト

イベント サービスからの案件に関する電子メール通知を受信する CC の受信者のリスト。

BCC リスト

イベント サービスからの案件に関する電子メール通知を受信する BCC の受信者のリスト。

電子メールの件名

イベント サービスが［宛先リスト］、［CC リスト］および［BCC リスト］の受信者に送信する案件に関する電子メール通知の件名行。

注: ［Web サーバ プロトコル］または［Web サーバまたはロード バランサの IP/ホスト］の［管理］、［システム構成］、［Web サーバ］の設定を変更した場合は、CA Asset Portfolio Management – エクスポート サービス用の Windows サービスを再起動する必要があります。

アプリケーション サーバの設定

製品をインストールしたら、アプリケーション サーバの設定を変更できます。

以下のフィールドについて説明します。

アプリケーション サーバまたはロード バランサの IP/ホスト

CA APM インストールでは、デフォルトによって、このフィールドにアプリケーション サーバのホスト名が設定されます。

- アプリケーション サーバが 1 台の環境では、アプリケーション サーバのホスト名または IP アドレスを入力できます。
- アプリケーション サーバが複数台の環境では、アプリケーション サーバのホスト名またはロード バランサの IP アドレスを入力できます。

注: アプリケーション サーバをドメイン ネーム システム（DNS）に登録する際、アプリケーション サーバ ホスト名として登録されている名前とは別の名前を使用できます。 そのような場合、このフィールドにはその別名を指定してください。

認証タイムアウト

ユーザが自動的に製品からログアウトされ、もう一度ログインする必要がある状態になるまでに、ユーザを非アクティブにすることができる時間（ミリ秒）。

デフォルト： 3600000（6 分）

EEM バックエンド

CA EEM がインストールされているサーバの名前。 この値はインストール中に入力されます。

USM Web サービス URL

USM サービスの URL。 製品が CA Service Catalog または CA Service Desk Manager に統合される場合、この値が使用されます。

注: ［Web サービス プロトコル］または［アプリケーション サーバまたはロード バランサの IP/ホスト］の［管理］、［システム構成］、［アプリケーション サーバ］の設定を変更した場合は、次の Windows サービスを再起動する必要があります。

- CA Asset Portfolio Management - エクスポート サービス
- CA Asset Portfolio Management - イベント サービス
- CA Asset Portfolio Management - HW 照合エンジン
- CA Asset Portfolio Management - LDAP インポート サービス

ハードウェア照合エンジンの設定

製品をインストールしたら、ハードウェア照合エンジンの設定を変更できます。

以下のフィールドについて説明します。

メッセージ キューの保存

ハードウェア照合エンジンがパージする前に、レコードがメッセージ キューに残される日数。

デフォルト： 7

レコード ロックのリフレッシュ数

ロック無効化間隔の設定と連携するエンジンのパフォーマンス調整用の設定。照合ルール レコードのロックをリフレッシュする前に、ハードウェア照合エンジンが追加または更新するレコードの数。［ロック無効化間隔］の設定に指定された秒数の時間内にロック リフレッシュが発生しない場合、別のハードウェア照合エンジンが照合ルール レコードを使用できます。

デフォルト： 100

ロック無効化間隔

レコードロックのリフレッシュ数の設定と連携する、エンジンのパフォーマンス調整用の設定。 照合ルールの実行時に、指定された時間（秒）内にロックのリフレッシュが行われなかった場合、他のハードウェア照合エンジンが照合ルールを使用できるようになります。

デフォルト： 600

Web サービス認証タイムアウト

ユーザが自動的にサービスからログアウトされ、もう一度ログインする必要がある状態になるまでに、ユーザを非アクティブにすることができる時間（ミリ秒）。

デフォルト： 3600000（6 分）

処理モード

ハードウェア照合エンジンが継続的に処理を行うかどうかを指定します。 製品では以下のオプションをサポートしています。

0

照合の続行モードで処理を行います。

エンジン一時停止時間

ハードウェア照合エンジンが処理サイクルの間に待機する時間（ミリ秒）。

デフォルト： 300000（5 分）

接続再試行時間

ハードウェア照合エンジンがデータベースへの接続を次に試行するまで待機する時間（ミリ秒）。

デフォルト: 60000（1 分）

エンジンのデバッグ レベル

メッセージ キューのデバッグ レベル。レベルは、Fatal、Error、Warning、情報、および Debug です。

デフォルト： Fatal

Web サービス バッチ サイズ

更新処理のために Web サービスに一度に送信されるレコード数。

デフォルト： 50

変更保留期間

ハードウェア照合エンジンが変更保留のリクエストをパージする前に、それをキューに残しておく日数。 この設定は、ハードウェア照合エンジンが処理するすべてのテナントに影響します。

デフォルト： 7

関連項目:

ハードウェア照合エンジン (P. 114)

CA EEM の設定

製品をインストールしたら、CA EEM の設定を変更できます。

以下のフィールドについて説明します。

認証タイプ

使用できる認証のタイプは以下のとおりです。

- **フォーム**。 ユーザが製品にログインする際、ユーザ名とパスワードの入力を求められます。
- **Windows 統合**。 Windows ドメインにログイン済みのユーザは、追加のログイン認証情報を提供することなく製品にアクセスできます。
- **外部**。 ユーザは外部のアクセス管理システム（たとえば CA SiteMinder）によって認証されます。

デフォルト： フォーム

UAPM 管理者パスワード

UAPM 管理ユーザが Web およびアプリケーション サーバにアクセスするためのパスワード。

エクスポート サービスの設定

製品をインストールしたら、エクスポート サービスの設定を変更できます。

以下のフィールドについて説明します。

オンデマンド リクエスト期間

エクスポート サービスがオンデマンド リクエストの処理サイクルの間に待機する時間（ミリ秒）

デフォルト： 5000 （5 秒）

オン デマンド最大スレッド数

スレッドを処理するオン デマンド スレッドの数。

デフォルト： 2

スケジュールされたリクエスト期間

スケジュールされたリクエストの処理サイクルの頻度（ミリ秒）

デフォルト： 7200000（2 時間）

SMTP Server

電子メール サーバ名。

認証タイムアウト

ユーザが自動的に製品からログアウトされ、もう一度ログインする必要がある状態になるまでに、ユーザを非アクティブにすることができる時間（ミリ秒）。

デフォルト： 360000（6 分）

パージ開始時間

パージ スレッドが開始する時刻（24 時間形式、協定世界時）。

デフォルト： 5 （世界協定時の午前 5 時）

検索バッチ サイズ

1 回のエクスポート リクエストの検索ごとに返されるデータ レコードの最大数。 デフォルト値を変更すると、パフォーマンスに影響する場合があります。 たとえば、低い値を指定すると、Web サービスがすべてのデータを取得する必要があるコール数が増える場合があります。また、高い値を指定すると、すべてのレコードを収集するために長い時間が必要になる場合があります。

デフォルト： 2000

SM Web サービス プロトコル

ストレージ マネージャ サービスにアクセスするために使用されるプロトコル。

SM Web サービス ポート

ストレージ マネージャ サービスが実行されているポート。

エクスポート サービスの電子メール アドレス

エクスポート サービスが通知に使用する電子メール アドレス。

Data Importer の設定

製品をインストールしたら、Data Importer の設定を変更できます。

以下のフィールドについて説明します。

認証タイムアウト

ユーザが自動的にコンポーネントからログアウトされ、もう一度ログインする必要がある状態になるまでに、ユーザを非アクティブにすることができる時間（ミリ秒）。

デフォルト： 3600000（6 分）

最大バッチ レコード サイズ

Data Importer バッチのレコードの最大数。

デフォルト： 50

Data Importer エンジン構成設定

製品をインストールしたら、Data Importer エンジンの設定を変更できます。

以下のフィールドについて説明します。

SMTP サーバ値

電子メール サーバ名。

スケジュールされたリクエスト期間

Data Importer エンジンが保留中のスケジュール済みインポート リクエストを確認するまで待機する時間の最大値。 この値はスケジュールされたデータ インポートのみに適用されます。

デフォルト： 60000 （60 秒）

オンデマンド リクエスト期間

Data Importer エンジンが保留中のオンデマンド インポート リクエストを確認するまで待機する時間の最大値。この値はオンデマンド データ インポートのみに適用されます。

デフォルト： 60000 （60 秒）

最大バッチ レコード サイズ

Data Importer エンジン バッチ内のレコードの最大数。

デフォルト： 100

最大ジョブ スレッド

1 つのインポート ジョブに対して同時に処理できる Data Importer エンジン スレッドの最大数。

デフォルト： 5

最大インポート スレッド

すべてのインポート ジョブに対して同時に処理できる Data Importer エンジン スレッドの最大数。

デフォルト： 5

LDAP データ インポートおよび同期サービスの設定

製品をインストールしたら、LDAP データ インポートおよび同期サービスの設定を変更できます。

以下のフィールドについて説明します。

DB チェック時間

サービスがステータス（アクティブまたはスリープ モード）をチェックする時間（ミリ秒）。 ステータスがアクティブである場合、サービスはデータのインポートを開始します。

EEM バックエンド

CA EEM がインストールされているサーバの名前。 この値はインストール中に入力されます。

<CORA> 構成設定

製品をインストールしたら、CORA （CA APM 登録サービス）の設定を変更できます。

以下のフィールドについて説明します。

注: 共通パラメータへの変更は、Web サーバ、WCF サービス、ハードウェア照合およびアプリケーション サーバ コンポーネントに影響します。登録サービス パラメータへの変更は登録サービス コンポーネントに影響します。

（共通）CORA の有効化

Web サーバ、WCF サービス、ハードウェア照合およびアプリケーション サーバ コンポーネントに対して共通オブジェクト登録 API 機能を有効にします。

デフォルト： False

（共通）CORA ID 生成の有効化

CORA テーブルが Web サーバ、WCF サービス、ハードウェア照合、およびアプリケーション サーバ コンポーネントの新規レコードに対して次の CORA ID を取得することを可能にします。

デフォルト： True

（登録サービス）CORA の有効化

すべての CA APM コンポーネントに対する登録サービスを使用して共通オブジェクト登録 API 機能を有効にします。

デフォルト： True

（登録サービス）CORA ID 生成の有効化

CORA テーブルが、すべての CA APM コンポーネントの登録サービスを使用して新規レコードの次の CORA ID を取得できるようにします。

デフォルト： False

ストレージ マネージャ サービスの設定

製品をインストールしたら、ストレージ マネージャ サービスの設定を変更できます。

以下のフィールドについて説明します。

パージ開始時間

ストレージ マネージャ サービスが未使用のファイルの削除を開始する時刻（24 時間形式）

認証タイムアウト

ユーザが自動的にサービスからログアウトされ、もう一度ログインする必要がある状態になるまでに、ユーザを非アクティブにすることができる時間（ミリ秒）。

デフォルト： 3600000（6 分）

イベント サービスの設定

製品をインストールしたら、イベント サービスの設定を変更できます。

以下のフィールドについて説明します。

プロバイダ URL

ワークフロー プロバイダ（たとえば CA Process Automation）にアクセスするための URL。

例： 次の URL は、デフォルト CA Process Automation ワークフロー Web サービスの URL です。

```
http://<wf_hostname>:<wf_tomcat_port>/itpam/soap
```

プロバイダ認証タイプ

イベント サービスと一緒に使用する認証のタイプ（ユーザまたは CA EEM）。

デフォルト： ユーザ（現在、CA EEM 認証は、イベント サービスではサポートされていません）。

プロバイダ ユーザ名

ワークフロー プロバイダにログインするためのユーザ ID。

プロバイダ パスワード

ワークフロー プロバイダにログインするためのユーザ パスワード。

プロバイダ プロセス パス

ワークフロー プロバイダの開始リクエスト フォームにアクセスするためのパス。 これらのフォームは、CA APM とワークフロー プロバイダとの統合のために利用可能である必要があります。 詳細については、ご使用のワークフロー プロバイダのマニュアルを参照してください。

デフォルト： /

処理対象のイベント数

1 回の Web サービス コールで処理されるイベントの最大数。

デフォルト： 2000

イベント パージの時刻（時間、GMT）

CA APM が削除指定されたイベント定義のパージを開始する時刻（24 時間形式、GMT）。

デフォルト： 5 （GMT の午前 5 時）

必要な CMDB 監査共有

CMDB との監査共有を有効にするインジケータ。

CMDB 共通データベース テーブルは複数のアプリケーションによって使用できます。たとえば、ca_contact テーブルは、統合されるときに CA APM、CA Service Catalog、および CA Service Desk Manager によって使用されます。 監査テーブルは、これらの共通テーブルに加えられる変更を管理します。 CA APM 内の CMDB オブジェクトに変更が加えられ、この値が true に設定されている場合、変更監査が CMDB 監査テーブルにポストされます。

送信者アドレス

イベント サービスから送信される通知用の送信者アドレス。

宛先リスト

イベント サービスからの案件に関する電子メール通知を受信する受信者のリスト。

CC リスト

イベント サービスからの案件に関する電子メール通知を受信する CC の受信者のリスト。

BCC リスト

イベント サービスからの案件に関する電子メール通知を受信する BCC の受信者のリスト。

電子メールの件名

イベント サービスが［宛先リスト］、［CC リスト］および［BCC リスト］の受信者に送信する案件に関する電子メール通知の件名行。

イベント発生のチェック間隔（ミリ秒）

定義済みのイベントに関連するフィールドの変更をデータベースがチェックする間に CA APM が待機する時間（ミリ秒）。

SAM 機能が有効な場合、このパラメータが 30000 に設定されることを検証します。SAM 機能が有効でない場合、この値が［イベント サービス］設定ファイルの設定に一致することを確認します。

デフォルト（CA SAM 実装なし）： 3600000 （1 時間）

デフォルト（CA SAM 実装あり）： 30000 （30 秒）

イベントトリガのチェック間隔（ミリ秒）

ワークフロー プロバイダに送信する必要があるトリガされたイベントのデータベースによるチェック間に CA APM が待機する時間（ミリ秒）。

SAM 機能が有効な場合、このパラメータが 60000 に設定されることを検証します。SAM 機能が有効でない場合、この値が［イベント サービス］設定ファイルの設定に一致することを確認します。

デフォルト（CA SAM 実装なし）： 3600000 （1 時間）

デフォルト（CA SAM 実装あり）： 60000 （60 秒）

トリガされたイベント ステータスの更新間隔（ミリ秒）

ワークフロー プロバイダに送信された、トリガされたイベントのステータスの更新間に CA APM が待機する時間（ミリ秒）。

SAM 機能が有効な場合、このパラメータが 60000 に設定されることを検証します。SAM 機能が有効でない場合、この値が［イベント サービス］設定ファイルの設定に一致することを確認します。

デフォルト（CA SAM 実装なし）： 3600000 （1 時間）

デフォルト（CA SAM 実装あり）： 60000 （60 秒）

アセット連絡先の更新間隔（ミリ秒）

CA CMDB のアセット連絡先の更新間に CA APM が待機する時間（ミリ秒）。

デフォルト： 43200000（12 時間）

CA SAM ステータス更新頻度

MDB 内の CA SAM インポート ジョブのステータスを更新する頻度（ミリ秒）。

デフォルト： 120000 （120 秒）

オン デマンド最大スレッド数

CA APM と CA SAM の間のデータ同期を処理するためのスレッドの最大数。デフォルト（ゼロ）は、システムがシステム ハードウェア設定に応じて必要な数のスレッドを作成することを示します。デフォルト値以外の値はすべて、システム環境設定に関係なく同じ数のスレッドを使用します。

デフォルト： 0

CA SAM イベント通知電子メール

CA SAM データ同期に関する通知を受信するための CA APM 管理者電子メール アドレス。

認証トークン

CA APM イベント サービスと CA SAM インポートおよびエクスポート サービスの間の通信を確立するトークン。 この値は CA SAM インポートおよびエクスポート サービス設定に一致する必要があります。

注: この値を変更する場合、CA SAM サーバ上の CA SAM インポートおよびエクスポート サービスに対する認証トークンの値を、この値に一致するように更新する必要があります。

注: イベントと通知の詳細については、「*ユーザ ガイド*」を参照してください。

Common Asset Viewer

製品をインストールしたら、Common Asset Viewer の設定を変更できます。

重要: CA APM の Tomcat ポート番号は、デフォルトで 9080 です。 CA APM と統合する別の製品がこのポート番号を使用する場合、競合が発生しないように CA APM 内のポート番号を変更してください。

以下のフィールドについて説明します。

Tomcat ポート

Common Asset Viewer を処理している Apache Tomcat サーバが使用するポート。

デフォルト： 9080

注: 本製品の設定を変更する前に、まず Apache Tomcat の設定ファイル内のポートを更新する必要があります。 Apache Tomcat の設定ファイルの更新の詳細については、実装ガイドを参照してください。

WCF サービスの構成設定

製品をインストールしたら、Windows Communications Framework （WCF）サービス コンポーネントの設定を変更できます。

以下のフィールドについて説明します。

WCF サービス サーバまたはロード バランサの IP/ホスト

CA APM インストールでは、デフォルトで、このフィールドに WCF サービス サーバのホスト名が設定されます。

- WCF サービス サーバが 1 台の環境では、WCF サービス サーバのホスト名または IP アドレスを入力できます。
- WCF サービス サーバが複数台の環境では、WCF サービス サーバのホスト名またはロード バランサの IP アドレスを入力できます。

注: WCF サービス サーバをドメイン ネーム システム（DNS）に登録する際、WCF サービス サーバ ホスト名として登録されている名前とは別の名前を使用できます。 そのような場合、このフィールドにはその別名を指定してください。

認証タイムアウト（ミリ秒）

ユーザが自動的にサービスからログアウトされ、もう一度ログインする必要がある状態になるまでに、ユーザを非アクティブにすることができる時間（ミリ秒）。

デフォルト： 3600000（6 分）

操作しきい値

クライアントまたはサーバによって送信できるか、クライアントまたはサーバに戻ったレコードの最大数。 WCF クライアント プログラムから検索メソッドをコールする場合、この値はユーザに返すことができるレコードの最大数を表します。 作成メソッドをコールする場合、この値は一度に送信できるレコードの最大数を表します。

EEM バックエンド

CA EEM がインストールされているサーバの名前。 この値はインストール中に入力されます。

SAM - ドライバのインポートの構成設定

製品をインストールしたら、Data Importer ドライバのインポートの設定を変更できます。

以下のフィールドについて説明します。

サーバ

CA SAM ドライバの インポート コンポーネントがインストールされているサーバの名前。

ユーザ名

Data Importer でレコードを追加、変更、または削除するために必要なユーザ名。

ITAM ルート パス

製品がインストールされているルートへのパス。

ファイル パス

CA SAM エクスポート ファイルがインポートされるルートへのパス。

例： *[ITAM Root Path]*¥ITAM¥Import Driver¥Input

Data Importer 実行可能パス

Data Importer 実行可能ファイル（ITAM Data Importer.exe）へのパス。

例： *[ITAM Root Path]*¥ITAM¥Data Importer¥ITAM Data Importer.exe

CA SAM サーバ名

CA SAM データベースがインストールされているサーバの名前。

ソフトウェア アセット管理の構成設定

製品をインストールしたら、ソフトウェア アセット管理の設定を行うことができます。 これらの設定を行った後、Apache Tomcat Common Asset Viewer サービスを再起動します。

注: 後で以下のいずれかのフィールドのエントリを変更する場合も、Apache Tomcat Common Asset Viewer サービスを再起動します。

- CA SAM Web サービス WSDL URL
- CA SAM Web サービス ログイン
- CA SAM Web サービス パスワード

以下のフィールドについて説明します。

CA SAM Web クライアント URL

CA SAM ホーム ページの URL を指定します。

注: ログインした後、CA SAM ホーム ページから Web クライアントの URL をコピーできます。

CA SAM インポート エクスポート Web サービス URL

CA SAM Web サービスの URL を指定します。以下の形式を使用します。

`http://[CA SAM System Name]:[Port Number]/SAMImportExportService/Service.svc`

- [CA SAM System Name] を CA SAM サーバの名前に置換します。
- [Port Number]を CA SAM インポートおよびエクスポート サービスがホストされるポートの番号に置換します。

SAM 機能の有効化

ソフトウェア アセット管理機能が有効であることを指定します。以前の CA APM ユーザ インターフェースに CA SCM フィールドがあった場合は、このチェック ボックスをオンにした後で削除されます。

CA SAM Web サービス WSDL の URL

CA SAM Web Service Definition Language（WSDL）の URL。この URL は CA SAM Web サービスにアクセスするために使用されます。以下の形式を使用します。

`http://［CA SAM システム名］：［ポート番号］/prod/SOAP/dyn_server.php`

- [CA SAM System Name] を CA SAM サーバの名前に置換します。
- ［ポート番号］を CA SAM Web サービスがホストされるポートの番号に置換します。

CA SAM Web サービス ログイン

CA SAM Web サービスのログイン名。

注: このログイン名と［CA SAM Web サービス パスワード］が config_soap.inc ファイル内のログイン名とパスワードに一致することを確認してください。このファイルは、以下の CA SAM インストール フォルダ パスにあります。

`app¥includes¥prod¥st¥config_soap.inc`

重要: config_soap.inc ファイルのデフォルトの内容は、コメント化されています。 コメント記号（/* */）を削除して、ログイン名とパスワードを設定してください。

CA SAM Web サービス パスワード

CA SAM Web サービスのログイン パスワード。

CA SAM SSO の暗号化アルゴリズム

CA IT Asset Manager の共通ホーム ページから CA SAM へのシングル サインオン アクセスに使用される暗号化アルゴリズムを指定します。

このエントリは、CA SAM システム構成内の security_auth_token_cipher フィールドの エントリと一致する必要があります。

注: CA SAM シングル サインオンの詳細については、 *「CA Software Asset Manager Administration Manual」* のシングル サインオンの説明を参照してください。

CA SAM SSO の認証メカニズム

CA SAM へのログインに使用されるメカニズムを指定します。

このエントリは、CA SAM システム構成内の security_auth_method フィールドの エントリと一致する必要があります。

注: このメカニズムには、auth_token_password を選択することを推奨します。auth_token メカニズムは、ほかの CA SAM ユーザのログインを無効にします。

ユーザ認証のための CA SAM SSO フィールド

ユーザを認証するために使用される一意の識別子（インポート ID または電子メール アドレス）のタイプを指定します。

このエントリは、CA SAM システム構成内の security_auth_token_user_identifier フィールドの エントリと一致する必要があります。

CA SAM SSO 秘密キー

CA APM と CA SAM が共有し、ユーザ認証を暗号化および復号化するために使用されるキーを指定します。 このキーによって、適切に認証されていない CA APM ユーザは CA SAM にアクセスできないようになります。

このエントリは、CA SAM システム構成内の security_auth_token_key フィールドの エントリと一致する必要があります。

コンポーネント サーバの追加

重要: このタスクを実行するユーザが、システム設定アクセスが有効な役割に属することを確認します。

製品をインストールしたら、最適なパフォーマンスを維持し、会社の成長とともに拡張できるようにするために、追加のサーバにコンポーネントを追加できます。1 つ以上のサーバに以下のコンポーネントをインストールできます。

- Web サーバ
- アプリケーション サーバ
- ハードウェア照合エンジン
- Data Importer
- WCF
- Data Importer エンジン

製品コンポーネント サーバを追加する方法

1. ［管理］-［システム構成］をクリックします。
2. 左側で、製品コンポーネントを選択します。
3. コンポーネントの追加セクションで、サーバの管理者のユーザ名やパスワードなど、サーバ接続に必要な情報を指定します。
4. ［追加］をクリックします。

   コンポーネント サーバ リストにサーバが追加されます。
5. 以下の新しいコンポーネント サーバの設定を入力します。
   - Web サーバ
   - アプリケーション サーバ
   - ハードウェア エンジン
   - Data Importer (P. 157)
6. ［保存］をクリックします。

   新しいサーバのコンポーネントの設定が保存されます。

   注: CA APM は追加したサーバにインストールします。***注:*** インストールの詳細については、「実装ガイド」を参照してください。

コンポーネント サービス ログ ファイルのデバッグ レベルの変更

製品コンポーネントには対応する Windows サービスがあります。これらのサービスでは、サービス ステータスを確認し、エラーの詳細を調べることができるログ ファイルが作成されます。ログ ファイル内の詳細情報の量は指定されたデバッグ レベルによって異なります。 サービス ログ ファイルのデフォルトのデバッグ レベルは Fatal です。 Windows サービスのデフォルト レベルを変更するには、各コンポーネントのログ設定ファイルを編集します。

次の手順に従ってください:

1. CA APM がインストールされているアプリケーション サーバ上のコンポーネント フォルダに移動します。

   例：

   [ITAM Root Path]¥ITAM¥Hardware Engine

2. テキスト エディタ（メモ帳など）で logging.config ファイルを開きます。
3. デバッグ レベルの value 文を見つけます。
4. 文を編集してデバッグ レベルを指定します。

   注: ログ設定ファイルには、さまざまなデバッグ レベル値について説明するコメントが含まれています。

5. ログ設定ファイルを保存します。

第 6 章: フィルタで CA APM データを保護する方法

このセクションには、以下のトピックが含まれています。

フィルタで CA APM データを保護する方法

データ フィルタの作成によって CA APM データ セキュリティをセットアップできます。データ フィルタを使用して、ユーザおよびユーザ ロールが表示、作成、または変更できるデータを制限します。 ユーザは、フィルタが指定するデータのみを表示、作成、または変更できます。以下のプライマリ オブジェクトに対するフィルタを作成できます。

- アセット
- モデル
- リーガル ドキュメント
- 連絡先
- 会社
- ロケーション
- 組織
- サイト

  注: [リスト管理] に含まれているセカンダリ オブジェクト用のフィルタは作成できません。 たとえば、特定のコスト センターに属しているアセットのみが表示されるように、コスト センター (セカンダリ オブジェクト) に基づいてアセット (プライマリ オブジェクト) をフィルタできます。 ただし、引き続きすべてのコスト センターにアクセスできます。コスト センター (または他のセカンダリ オブジェクト) へのアクセスを制限するには、これらのオブジェクトへのアクセスを許可しない設定にユーザを割り当てます。

システム管理者として、以下の方法でデータ アクセスを制限するフィルタを定義します。

- 現在のユーザ（連絡先）に基づいてデータを制限します。

  たとえば、連絡先のコスト センターによってアセットを制限するフィルタを定義します。 すべてのユーザにフィルタを適用すると、アセットは各ユーザ コスト センターに基づいて動的にフィルタします。連絡先のコスト センターが変更された場合、新しいコスト センターのアセットが自動的にフィルタされます。

- 固定値に基づいてデータを制限します。

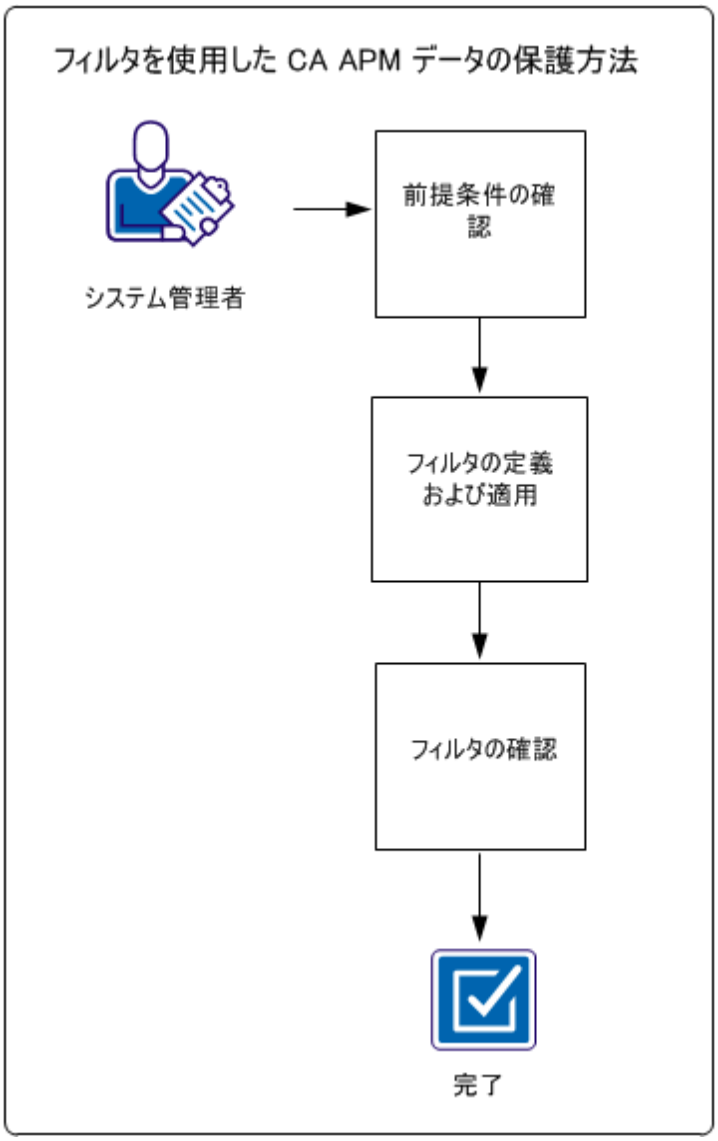
  たとえば、ユーザが 開発コスト センターのアセットを表示できるようにします。 開発は固定値です。 コスト センターが変更された場合、コスト センターはフィルタで自動的に変更されることはありません。

フィルタ ユーザは、フィルタ条件に一致するデータにアクセスできます。

注: また、ユーザ インターフェースの設定によって CA APM セキュリティをセットアップできます。 この設定によって、CA APM の別の機能へのユーザ アクセスを制御できます。

重要: このシナリオでは、システム管理者がフィルタを定義します。 ただし、管理者はフィルタ管理権限を CA APM ユーザ ロールに付与できます。

以下の図は、システム管理者がフィルタによって CA APM データを保護する方法を示しています。



CA APM データをフィルタするには、以下の手順を実行します。

1. 前提条件を確認します (P. 174)。
2. フィルタを定義および適用します (P. 174)。
3. フィルタを確認します (P. 178)。

例: コスト センターによるアセット データのフィルタ

サム (Document Management Company の CA APM システム管理者) は、組織のデータ セキュリティ要件が満たされていることを確認する必要があります。 サムは、ユーザが各自のコスト センター データのみを参照するように、会社のアセット レコードへのユーザ アクセスを制限する必要があります。 サムは、アセット (すべてのファミリ) 用のフィルタを作成して、特定のユーザにそのフィルタを割り当てます。サムは、フィルタによって組織のデータ セキュリティが保証されることを確認します。

前提条件の確認

正常にデータをフィルタできるようにするには、以下の前提条件が完了していることを確認します。

1. ユーザまたは役割によって制限する製品データを特定します。
2. データ アクセスが制限されているユーザおよび役割を特定します。

フィルタの定義および適用

フィルタを定義して、そのフィルタを役割、ユーザ、または役割とユーザの組み合わせに割り当てます。アクセスする権限がユーザに与えられているデータのみが表示されます。

次の手順に従ってください:

1. ［管理］-［フィルタ管理］をクリックします。
2. 左側で、［新規フィルタ］をクリックします。

3. ［フィルタ情報］領域で、必須情報、およびオプション情報（必要な場合）を入力します。 以下のフィールドについて説明します。

   オブジェクト

   フィルタするオブジェクト データを指定します。 選択するオブジェクトによって、［フィルタ条件］領域で条件として使用できるフィールドが決定されます。

   注:［モデル］または［アセット］を選択する場合は、ファミリも選択してください。 ［リーガル ドキュメント］を選択する場合は、テンプレートも選択してください。フィルタは、選択するファミリまたはテンプレートに属しているオブジェクトに適用されます。 たとえば、ハードウェア アセット オブジェクト用のフィルタは他のアセット ファミリには適用されません。

   重要: フィルタ条件を指定した後、またはフィルタを保存した後で、オブジェクト、オブジェクト ファミリ、およびテンプレートを変更することはできません。 フィルタ条件を削除してオブジェクトを変更します。

   ファミリまたはリーガル テンプレート

   モデル オブジェクトまたはアセット オブジェクト用のファミリ、またはリーガル ドキュメント オブジェクト用のテンプレートを指定します。

4. ［フィルタ セキュリティ］領域で、役割またはユーザ セキュリティの情報を入力します。

   重要:［フィルタ セキュリティ］領域で、ユーザまたは役割を選択せずにフィルタを保存すると、フィルタはどのユーザにも適用されません。

5. ［フィルタ条件］領域で［フィールドの追加］をクリックします。
6. ダイアログ ボックスでフィールドを選択して［OK］をクリックします。

   基準が［フィルタ条件］リストに表示されます。

7. 追加した基準の隣の［レコード編集］アイコンをクリックします。
8. 情報を入力して選択したフィールド用のフィルタ基準を定義します。 以下のフィールドについて説明します。

   左かっこ

   条件のグループの最初の基準を指定します。 条件のグループを定義してフィルタのロジックを制御できます。

   注:［左かっこ］を選択してグループの最初の基準を定義する場合は、グループの最後の基準に［右かっこ］を選択してください。

たとえば、アセット名「OE001」、またはアセット ファミリ「コンピュータ」とアセット名「Dell」の両方でアセットをフィルタできます。 この例では、グループは 2 つの基準で構成されます。 ［左かっこ］が最初の基準に選択され、アセット ファミリは「コンピュータ」であることが示されます。 ［右かっこ］が 2 番目の基準に選択され、アセット名は「Dell」であることが示されます。

フィールド名

フィルタするフィールド データを指定します。

演算子

オブジェクト データをフィルタするために使用するフィルタ演算子を指定します。 ［値あり］および［値なし］以外のすべての演算子の場合、［値］フィールドに値を入力します。

たとえば、アセット名が「OE001」と一致せず、かつアセット ファミリが「コンピュータ」と一致するアセットをフィルタできます。

注: ［演算子］および［値］を指定すると、フィルタは［フィールド名］の固定値に基づいてデータを制限します。 このフィルタ タイプでは、［連絡先の値の使用］フィールドは適用されません。

連絡先の値の使用

フィルタが現在のユーザと関連付けられている［フィールド名］の値を使用するように指定します。

たとえば、このチェック ボックスをオンにして、［フィールド名］にコスト センターを選択する場合、ユーザは各自のコスト センターの製品データにのみアクセスできます。 製品のすべてのユーザにフィルタを適用すれば、データは各ユーザ コスト センターに基づいて動的にフィルタします。 コスト センターが変更された場合、新しいコスト センターのデータが自動的にフィルタされます。

注: このチェック ボックスをオンにすると、フィルタは現在のユーザと関連付けられている［フィールド名］の値に基づいてデータを制限します。このフィルタ タイプでは、［演算子］および［値］フィールドは適用されません。

右かっこ

条件のグループの最後の基準を指定します。 条件のグループを定義してフィルタのロジックを制御できます。

注: ［右かっこ］を選択してグループの最後の基準を定義する場合は、グループの最初の基準に［左かっこ］を選択してください。

たとえば、アセット名「OE001」、またはアセット ファミリ「コンピュータ」とアセット名「Dell」の両方でアセットをフィルタできます。 この例では、グループは 2 つの基準で構成されます。 ［左かっこ］が最初の基準に選択され、アセット ファミリは「コンピュータ」であることが示されます。 ［右かっこ］が 2 番目の基準に選択され、アセット名は「Dell」であることが示されます。

結合子

2 つの条件間の結合子を指定します。

- And -- リスト内の現在の基準および次の基準が有効な場合にデータをフィルタします。
- Or -- リスト内の現在の基準または次の基準のいずれかが有効な場合にデータをフィルタします。

たとえば、アセット ファミリが「コンピュータ」およびアセット名が「Dell」のアセットをフィルタできます。

値

フィルタするフィールド値を指定します。 値を指定する場合は、［演算子］フィールドで演算子を選択します。 このフィールドの横に［検索］アイコンが表示される場合、［検索］アイコンをクリックして値を選択することもできます。

たとえば、アセット名が「OE001」のアセットをフィルタできます。

注: ［演算子］および［値］を指定すると、フィルタは［フィールド名］の固定値に基づいてデータを制限します。 このフィルタ タイプでは、［連絡先の値の使用］フィールドは適用されません。

9. ［レコード編集を完了］アイコンをクリックします。
10. （オプション）［フィールドの追加］をクリックして、その他のフィルタ条件を定義します。
11. すべてのフィルタ条件が完了したら、［保存］をクリックします。

フィルタが定義され、ユーザおよび役割に適用されます。フィルタ ユーザは、フィルタ条件に一致するデータにアクセスできます。

例: ユーザ コスト センターによるアセット データのフィルタ

サムはシステム管理者として、ユーザを各自のコスト センターのアセット データに制限するフィルタを定義します。 このフィルタを定義するために、サムは以下の選択を行います。

1. ［フィルタ情報］領域では、［オブジェクト］フィールドで［アセット］、および［ファミリ］フィールドで［（すべてのファミリ）］を選択します。
2. ［フィルタ セキュリティ］領域では、フィルタと関連付けられているユーザを選択します。
3. ［フィルタ条件］領域では、以下の手順を実行して基準を作成します。
   a. ［フィールド名］フィールドで［コスト センター］を選択します。
   b. ［連絡先の値の使用］チェック ボックスをオンにします。
4. フィルタを保存します。

フィルタの確認

フィルタによって組織のデータ セキュリティが保証されることを確認します。

次の手順に従ってください:

1. フィルタに割り当てられたユーザとして製品にログインします。
2. フィルタがユーザに対して許可しているデータの一部を表示します。
3. フィルタがユーザに対して許可していないデータの表示を試行します。

   たとえば、フィルタ ユーザに対して許可されていないデータにアクセス権がある別のユーザとしてログインします。フィルタ ユーザがアクセスできないデータが表示されるページの URL をコピーします。フィルタ ユーザのブラウザにこの URL を貼り付けます。

   エラー メッセージが表示されます。
4. フィルタがユーザに対して許可していないデータの変更を試行します。

   たとえば、ページ上のテキスト入力フィールドを特定します。 ユーザがアクセスできないデータ（フィルタが許可していない特定の会社名など）を入力して、［保存］をクリックします。

   エラー メッセージが表示されます。

例: データ フィルタによるアセット データ制限の確認

サムは、アセット（すべてのファミリ）データ用のフィルタを作成して、特定のユーザにそのフィルタを割り当てました。フィルタによって、ユーザはユーザ コスト センター内のアセットにのみアクセスできます。その後、サムは以下の手順を実行して、フィルタが機能することを確認します。

1. 割り当てられたユーザとしてログインし、アセットが［アセット検索］ページに表示されることを検証します。
2. 最初のユーザ コスト センター外にあるアセットへのアクセス権を持つ別のユーザとしてログインします。
3. 最初のユーザ コスト センター外にあるアセットを表示して、このアセットの URL をコピーします。
4. 最初のユーザ（フィルタを割り当てられたユーザ）としてログインして、コピーしたアセットの URL をブラウザに貼り付けます。

   エラー メッセージで、アセットが存在しないことが示されます。

第 7 章: CA APM から未使用のファイルを削除する方法

このセクションには、以下のトピックが含まれています。

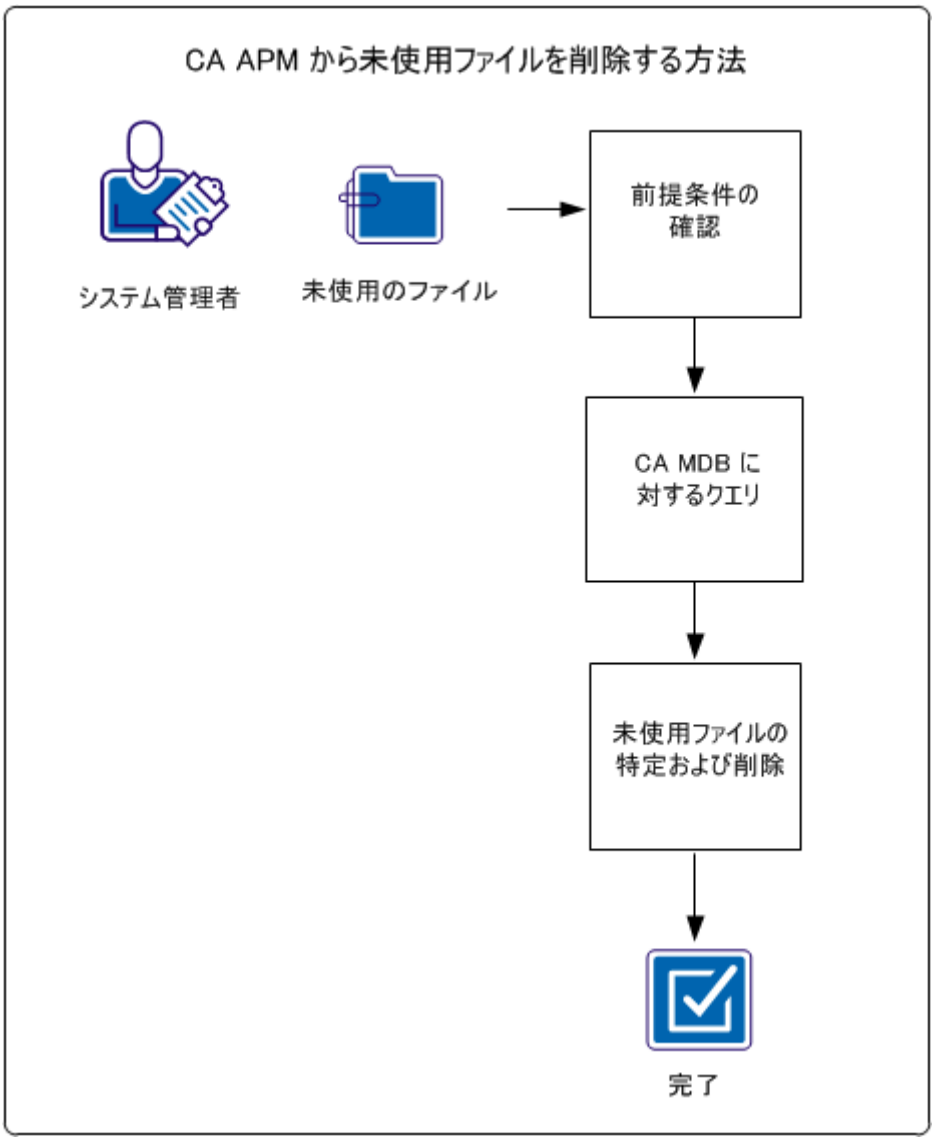
CA APM から未使用のファイルを削除する方法

製品で使用するファイルは、ストレージ マネージャ サービスがインストールされている CA APM アプリケーション サーバに格納されています。これらのファイルには添付ファイル、Data Importer ソース データ ファイルおよびレガシー マップ ファイルが含まれます。

添付ファイルを削除する場合は、オブジェクト レコード内の添付ファイルへの参照のみを削除します。削除された添付ファイルがファイルである場合、そのファイルは CA APM アプリケーション サーバ上のファイル システムに残ります。同様に、特定のデータ ファイルを使用するインポートを削除するときは、CA APM サーバからデータ ファイルを削除しません。

特定の添付ファイル（インポート データ ファイルまたはレガシー マップ ファイル）が不要になった場合、CA APM サーバからファイルを削除できます。 ファイルを削除する前に、ファイルに関連付けがないことを確認します。

以下の図は、システム管理者が CA APM アプリケーション サーバから未使用のファイルを削除する方法を示しています。



未使用のファイルを削除するには、以下の手順を実行します。

1. 前提条件を確認します (P. 183)。
2. CA MDB にクエリを実行します (P. 183)。
3. 未使用のファイルを特定して削除します (P. 183)。

前提条件の確認

正常に未使用のファイルを削除できるように、削除する未使用のファイルの名前を特定します。

CA MDB に対するクエリの実行

特定の添付ファイル（インポート データ ファイルまたはレガシー マップ ファイル）が不要になった場合、CA APM アプリケーション サーバからファイルを削除できます。 ファイルを削除する前に、CA APM 内にそのファイルの関連付け（たとえば、リーガル ドキュメントに添付されたファイル、またはデータ インポートに関連付けられたインポート データ ファイル）がないことを確認します。

次の手順に従ってください:

1. CA APM インストールと関連付けられている CA MDB にアクセスします。
2. al_file_storage テーブルをクエリして、ファイル名および関連するテナント（該当する場合）を検索します。 以下のステートメントはクエリ例です。

   ```
   select COUNT(0) from al_file_storage where attachment_url = 'filename.txt'
   ```

   レコードが返されない場合、指定されたファイル名と関連付けられたレコードはありません。 ファイルを削除できます。

未使用ファイルの特定および削除

CA APM 内にファイルの関連付けがないことを確認したら、ファイルを特定して削除できます。

次の手順に従ってください:

1. ストレージ マネージャ サービスがインストールされている CA APM アプリケーション サーバ上で、マルチテナントを使用するかどうかに応じて以下のいずれかの場所に移動します。

   ```
   [ITAM Root Path]/Storage/Common Store/Attachments
   ```

   ```
   [ITAM Root Path]/Storage/Tenant_Name/Attachments
   ```

   ```
   [ITAM Root Path]/Storage/Common Store/Import
   ```

   ```
   [ITAM Root Path]/Storage/Tenant_Name/Import
   ```

2. 未使用のファイルを特定して削除します。

第 8 章: データのインポート方法

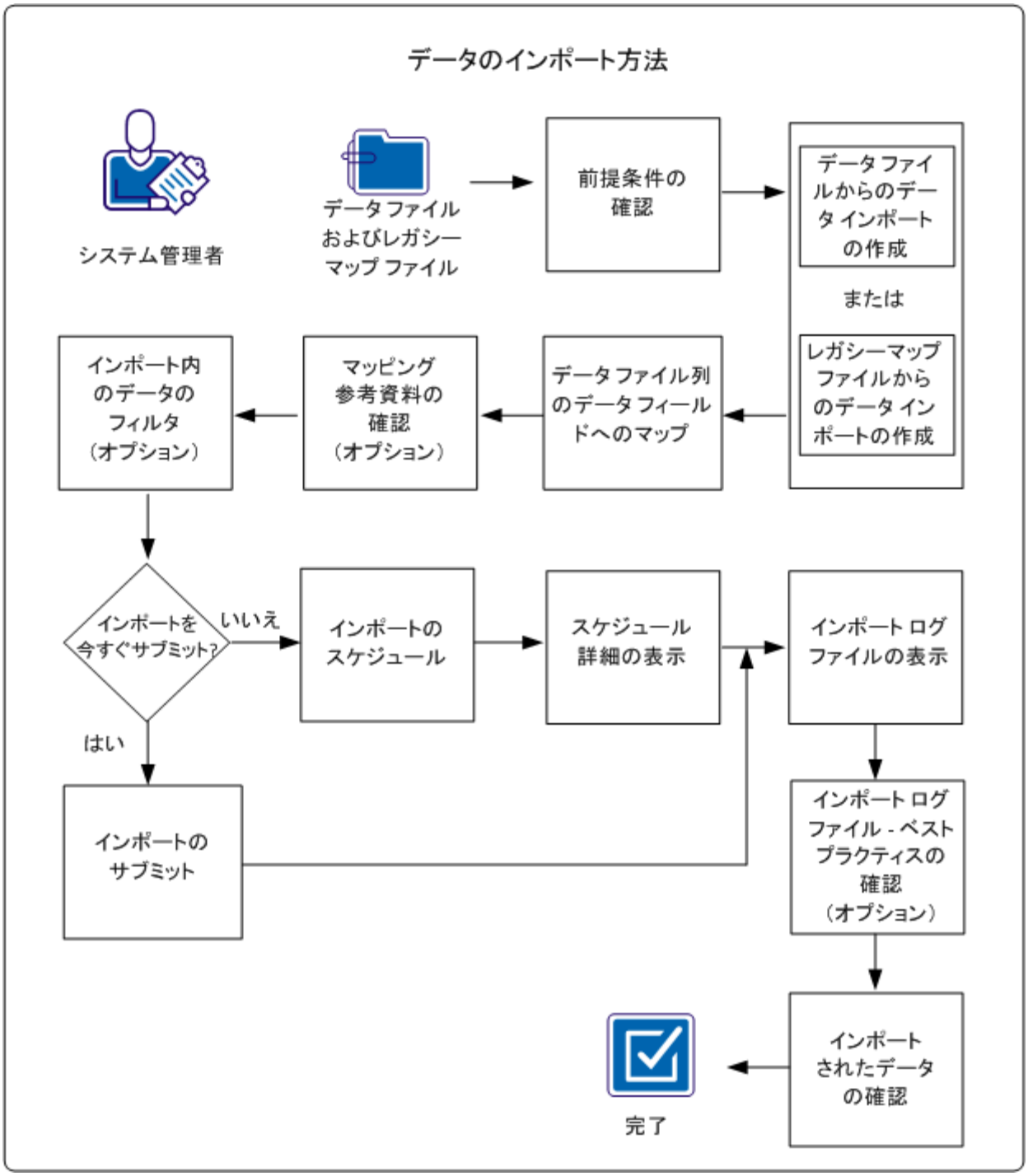
このセクションには、以下のトピックが含まれています。

データのインポート方法

データを追加または更新するときは、Data Importer を使用して、CA APM へそれをインポートします。 CA MDB で、インポートするデータが 挿入されるか、または既存のデータを更新します。

重要: このシナリオで、システム管理者はデータ インポートを実行します。ただし、管理者は Data Importer ユーザ アクセスまたは Data Importer 管理者アクセスを任意の CA APM ユーザ役割へ付与できます。 ユーザ アクセスにより、ユーザはインポートの作成、自分のインポートの変更または削除、別のユーザによって作成されたインポートの表示が可能になります。 管理者アクセスにより、ユーザはインポートの作成、任意のユーザによって作成されたインポートの変更または削除が可能になります。

以下の図は、システム管理者がデータをインポートする方法を示しています。



CA APM データをインポートするには、以下の手順に従います。

1. 前提条件を確認します (P. 188)。
2. データ ファイルからデータ インポートを作成する (P. 189) か、またはレガシー マップ ファイルからデータ インポートを作成します (P. 194)。
3. ［データ ファイル］列を［データ］フィールドにマップします (P. 195)。
4. マッピング参考資料を確認します (P. 198)。
   - プライマリおよびセカンダリ ルックアップの組み合わせ (P. 198)
   - ハードコードされた値 (P. 201)
   - 1 つのフィールドに対する複数の値 (P. 202)
5. インポート内のデータをフィルタします (P. 202)。
6. インポートをサブミットします (P. 204)。
7. インポートをスケジュールします (P. 205)。
8. ［スケジュールの詳細］を表示します (P. 207)。
9. インポート ログ ファイルを表示します (P. 207)。
10. インポート ログ ファイル ベスト プラクティスを確認します (P. 208)。
11. インポートされたデータを確認します (P. 209)。

例: 新入社員のインポート

Document Management Company の CA APM システム管理者であるサムは、新入社員のグループをインポートしたいと思っています。新入社員は、この製品を使用してハードウェア アセットを管理します。サムは、社員情報が含まれるカンマ区切り値（CSV）ソース データ ファイルを人事から受信しました。新規アセット マネージャ社員は全員 IT 部門に属し、会社本部で働いています。 ただし、ソース データ ファイルには、他の場所で勤務し IT 部門に属さない新入社員に関するデータも含まれています。

サムは、本部にいる IT 社員のデータのみをインポートしたいと思っています。Data Importer とソース データ ファイルを使用して、サムは、データ インポートを作成し新入社員を CA MDB に組み込みます。本部の IT 部門の社員のみが確実にインポートされるように、サムは除外フィルタを作成します。 サムはインポートを実行した後、インポートが成功したことを確認するためにインポート統計およびインポート ログ ファイルとユーザ インターフェースを確認します。

前提条件の確認

正常にデータをインポートできたことを確認するには、以下のタスクが完了したことを確認します。

- 区切られたテキスト形式（たとえばタブまたはカンマ）でソース データ ファイルを準備します。このファイルには、インポートするデータが含まれます。

  注: ソース データ ファイルの名前に主なインポート先オブジェクトを含めることを推奨します。 このファイル命名規則は、インポートを作成したときにデータ ファイルを見つけるのに役立ちます。

  注: ソース データ ファイルに存在する NULL は、対応するインポート先フィールド値をクリアします。ソース データ ファイル内のフィールドが空の場合、対応するインポート先フィールド値は変更されません。

  重要: ソース データ ファイル内のデータ値に選択された区切り文字が含まれている場合、データ値を二重引用符で囲む必要があります。 たとえば、会社をインポートする際に区切り文字としてカンマを選択したとします。 また、ソース データ ファイルに Document Management Company, Inc. というデータ値を入力するとします。 この場合、このデータ値を二重引用符で囲みます。

  例： "Document Management Company, Inc"。

- （オプション）ソース データ ファイルをローカル サーバから以下のいずれかの場所にコピーします。ストレージ マネージャ サービスがインストールされている CA APM アプリケーション サーバ上でこれらの場所にアクセスできます。 この場所は、マルチテナントを使用しているかどうかによって異なります。

  `[ITAM Root Path]¥Storage¥Common Store¥Import`

  `[ITAM Root Path]¥Storage¥`*`Tenant_Name`*`¥Import`

  注: インポートを作成する前にデータ ファイルをコピーした場合は、インポートを作成するときにファイル名を指定できます。データ ファイルを最初にコピーしない場合は、インポートを作成するときにローカル サーバからファイルをアップロードできます。

- （オプション）ローカル サーバから旧製品リリース（これらのファイルがある場合）からレガシー マップ ファイルを以下のいずれかの場所にコピーします。ストレージ マネージャ サービスがインストールされている CA APM アプリケーション サーバ上でこれらの場所にアクセスできます。 この場所は、マルチテナントを使用しているかどうかによって異なります。

  `[ITAM Root Path]¥Storage¥Common Store¥Import`

  `[ITAM Root Path]¥Storage¥`*`Tenant_Name`*`¥Import`

データ ファイルからのデータ インポートの作成

インポートするデータが含まれるソース データ ファイル（区切られたテキスト ファイル）を使用して、データ インポートを作成します。 ファイルを選択し、インポート パラメータを設定し、ファイル内のデータを区切る区切り文字（カンマ、タブなど）を指定します。

以前の製品リリースからのレガシー マップ ファイルを使用して、データ インポートを作成することもできます。 詳細については、「レガシー マップ ファイルからのデータ インポートの作成 (P. 194)」を参照してください。

次の手順に従ってください:

1. 管理者として CA APM にログインします。

   重要: このシナリオで、システム管理者はデータ インポートを実行します。ただし、管理者は Data Importer ユーザ アクセスまたは Data Importer 管理者アクセスを任意の CA APM ユーザ役割へ付与できます。 ユーザ アクセスにより、ユーザはインポートの作成、自分のインポートの変更または削除、別のユーザによって作成されたインポートの表示が可能になります。 管理者アクセスにより、ユーザはインポートの作成、任意のユーザによって作成されたインポートの変更または削除が可能になります。

2. ［管理］-［Data Importer］をクリックします。
3. ［新規インポート］をクリックします。
4. ［基本情報］領域に必要な情報を入力し、必要に応じオプションの情報を提供します。 以下のフィールドについて説明します。

   データ ファイル

   インポートするソース データ ファイルを指定します。

   このファイルが CA APM アプリケーション サーバで利用可能な場合は、データ ファイルを検索および選択します。 このファイルがアプリケーション サーバで利用可能でない場合は、ファイルをアップロードします。

   ファイルのアップロード

   ローカル サーバ上で、インポートするソース データ ファイル、またはマッピングを作成するために使用するレガシー マップ ファイルを参照します。 このファイルは CA APM アプリケーション サーバにアップロードされます。

   重要: ファイル サイズは、製品の環境設定によって制限されます。 詳細については、管理者にお問い合わせください。

   主なインポート先オブジェクト

インポートのための主なオブジェクトを指定します。

アセットおよびモデル オブジェクトは、それぞれに対応するファミリと共にリスト表示されます。［すべてのファミリ］を指定することもできます。 リーガル ドキュメントのオブジェクトは、リーガル テンプレートに従ってリスト表示されます。［すべてのテンプレート］を指定することもできます。 オブジェクトには、インポートできるオブジェクトがすべて含まれます。

注: 複数のアセット ファミリ タイプを含むアセットまたはモデル、もしくは複数のリーガル テンプレートを含むリーガル ドキュメントの場合は、このフィールドに以下の選択を使用します。 ソース データ ファイルの各レコードの特定のファミリまたはテンプレートを指定します。

- アセットでは、［アセット］（すべてのファミリ）を選択します。
- モデルでは、［モデル］（すべてのファミリ）を選択します。
- リーガル ドキュメントでは、［リーガル ドキュメント］（すべてのテンプレート）を選択します。

重要: インポートに対し正しい主なインポート先オブジェクトを選択していることを確認してください。 インポートを保存またはコピーした後で主なインポート先オブジェクトを変更することはできません。

最初の行を列名にする

ソース データ ファイルの最初の行に列名を含めるかどうかを指定します。最初の行に列名を含めない場合、名前は「フィールド 1」や「フィールド 2」などの一般的な名前で表示されます。

テナント

インポートに適用されるテナントを指定します（マルチテナントを使用している場合）。

テナントを選択できるのは、CA APM でマルチテナントが有効になっていて、さまざまなテナントにアクセスする権限が与えられているときだけです。 公開データへのアクセス権があり、複数のテナントを持っている場合は、すべてのテナントを選択できます。

注: すべてのテナントを指定した場合は、ソース データ ファイルには［テナント名］フィールドにマップする［テナント名］列が必要です。

重要: 1 つのテナントを指定する場合は、ソース データ ファイル内のすべてのデータが選択したテナントに属していることを確認してください。 複数のテナント用のデータがある場合、選択したテナントにはすべてのテナントのデータがインポートされます。

データ区切り文字

ソース データ ファイルで使用した区切り文字（たとえばカンマまたはタブ）を指定します。

重要: ソース データ ファイル内のデータ値に選択された区切り文字が含まれている場合、データ値を二重引用符で囲む必要があります。 たとえば、会社をインポートする際に区切り文字としてカンマを選択したとします。また、ソース データ ファイルに Document Management Company, Inc. というデータ値を入力するとします。 この場合、このデータ値を二重引用符で囲みます。

例： "Document Management Company, Inc"

データ ファイルのロケール

ソース データ ファイルのロケールを選択します。 この設定は、日付および時刻の形式を指定します。

5. ［詳細設定］領域に必要な情報を入力し、必要に応じオプションの情報を提供します。 以下のフィールドについて説明します。

最大エラーしきい値（%）

インポートを停止するためのエラーの回数を定義します。 しきい値は、処理されたレコードのパーセンテージに基づきます。 15 パーセント以上のしきい値を推奨します。

注: Data Importer は、エラーしきい値に達した場合、計算する前の管理、システム構成、Data Importer（［最大バッチ レコード サイズ］フィールド）上で指定されるレコードの数を処理します。

プライマリ ルックアップ オブジェクト処理タイプ

インポート アクティビティ（たとえば、挿入または更新）のタイプを指定します。

セカンダリ ルックアップ オブジェクトの作成

インポート プロセス中に新しいセカンダリ ルックアップ オブジェクトを作成します。 このオプションが選択されておらず、セカンダリ オブジェクトが存在しない場合、エラーが発生します。

セカンダリ ルックアップ オブジェクトの更新

インポート プロセス中に既存のセカンダリ ルックアップ オブジェクトを更新します。 セカンダリ オブジェクトが存在しない場合、エラーが発生します。

セカンダリ ルックアップ オブジェクト エラー設定のエラー

セカンダリ オブジェクト プロセスが失敗した場合に、Data Importer がプライマリ オブジェクトの挿入または更新を処理しないことを示します。 このチェック ボックスがオンの場合にセカンダリ オブジェクトの挿入または更新プロセスが失敗すると、プライマリ オブジェクトへの挿入または更新も失敗します。 このチェック ボックスがオフの場合、プライマリ オブジェクトは作成または更新されます（そのオブジェクトがセカンダリ オブジェクトに依存していない限りにおいて）。ただし、セカンダリ オブジェクト値は作成または変更されません。 いずれの状況でも、セカンダリ オブジェクト エラーはインポート ログ ファイルに記録されます。

例： ロケーションをインポートし、そのロケーションには国があるとします。インポートが国オブジェクトの更新試行中に失敗し、かつこのチェック ボックスがオンの場合、ロケーション レコードは作成されません。 このチェック ボックスがオフの場合、ロケーション レコードは作成されますが、国の情報は更新されません。

正規化の動作

データを正規化するか、またはデータを正規化せずにログ ファイルにエラー メッセージを書き込むかどうかを指定します。

注: このフィールドは、正規化ルールを定義している場合にのみ表示されます。

正規化エラー

インポートしているデータの中に正規化できるデータが見つかったときに、エラー メッセージを Data Importer ログ ファイルに書き込みます。該当のデータはインポートされません。ログ ファイル エラー メッセージには、データに関する詳細が含まれます。

たとえば、データに会社名 Microsoft が含まれるとします。 作成した会社正規化ルールによって、Microsoft は収集（非権限）値として識別され、Microsoft Corporation が正規化された（権限）値として指定されます。データのインポート時にこのオプションを選択すると、会社名 Microsoft を含むオブジェクトはインポートされず、エラー メッセージがログ ファイルに書き込まれます。

エラーなしで正規化を適用

正規化ルールを使用して、インポートするデータを正規化します。正規化できるデータが見つかった場合、データは正規化され、インポートされます。 データに関するエラー メッセージはログ ファイルに書き込まれません。

たとえば、データに会社名 Microsoft が含まれるとします。 作成した会社の正規化ルールによって、Microsoft は収集（非権限）値として識別され、Microsoft Corporation が正規化された（権限）値として指定されます。データのインポート時にこのオプションを選択すると、会社名 Microsoft を含むオブジェクトは正規化されます。 この例では、会社名が Microsoft Corporation に変更され、関連のあるオブジェクトがインポートされます。

6. ［保存］をクリックします。

   インポートが保存されます。 ページの［マッピング］、［例外フィルタ］および［スケジュール］領域に入力できるようになりました。

例: データ ファイルからの新入社員のデータ インポートの作成

CA APM システム管理者であるサムはデータ インポートを作成するために以下のアクションを行います。

1. ［管理］-［Data Importer］に移動して、［新規インポート］をクリックします。
2. ［データ ファイル］フィールドに「新入社員.csv」と入力します。

   この CSV ファイルは、サムが人事から受信した新入社員情報を含むソース データ ファイルです。
3. 主なインポート先オブジェクトの連絡先とデータ区切り文字としてカンマを選択します。
4. ［プライマリ ルックアップ オブジェクト処理タイプ］フィールドで［挿入または更新］を選択し、［保存］をクリックします。

レガシー マップ ファイルからのデータ インポートの作成

以前の CA APM リリースからのレガシー マップ ファイルを使用して、データ インポートを作成できます。 マップ ファイルは対応するデータ ファイルおよびインポート パラメータ設定を定義します。

注: データ インポートを作成する前に、CA APM アプリケーション サーバにレガシー マップ ファイルおよび対応するデータ ファイルをコピーすることをお勧めします。 ただし、必要な場合、レガシー マップ ファイルをアップロードするオプションの手順を使用できます。

また、データ ファイルのみを使用して、データ インポートを作成することもできます。 詳細については、「データ ファイルからのデータ インポートの作成 (P. 189)」を参照してください。

次の手順に従ってください:

1. ［管理］-［Data Importer］-［新規インポート］をクリックします。
2. ［マップの検索およびロード］をクリックして、CA APM アプリケーション サーバに存在するレガシー マップ ファイル名を選択します。

   重要: 対応するデータ ファイルは、CA APM アプリケーション サーバで利用可能である必要があります。

   レガシー マップ ファイルが CA APM アプリケーション サーバに存在しない場合は、［ファイルのアップロード］フィールドを使用してファイルをアップロードします。
3. （オプション） 以下の手順に従って、CA APM アプリケーション サーバに存在しないレガシー マップ ファイルをアップロードします。

   a. ［ファイルのアップロード］フィールドで、ローカル サーバを参照し、レガシー マップ ファイルを選択します。

      レガシー マップ ファイルがアップロードされ、［ファイルのアップロード］フィールドに表示されます。

   b. ［マップの検索およびロード］をクリックして、アップロードしたレガシー マップ ファイルを選択します。

      レガシー マップ ファイルが［レガシー マップ ファイル］フィールドに表示されます。

      基本情報がロードされます。

   注: ソース データ ファイルに関する警告が表示されたら、［ファイルのアップロード］フィールドを使用してファイルをアップロードします。

4. ［詳細設定］を指定して、［保存］をクリックします。

   例外フィルタおよびマッピング データ マッピングがロードされます。ページの［マッピング］、［例外フィルタ］および［スケジュール］領域に入力できるようになりました。 ［マッピング］および［例外フィルタ］領域には、レガシー マップ ファイルのデータが表示されます。

   注: ［詳細設定］への指定の詳細については、「データ ファイルからのデータ インポートの作成 (P. 189)」を参照してください。

データ ファイル列のデータ フィールドへのマップ

CA APM 内のフィールドにソース データ ファイル内の列をマップできます。 列マッピングを実行して、ソース データがどこにインポートされるかを指定します。列マッピング中に、ほとんどのオブジェクトおよび関連するフィールドをインポート先フィールドとして選択できます。

注: レガシー マップ ファイルからデータ インポートを作成した場合は、列マッピングが存在します。値を変更したい場合は、既存のマッピング ルールを編集できます。 また、マッピング ルールおよびフィルタを追加または削除できます。

ログイン時に、管理者が割り当てたユーザ役割によって参照および使用できるオブジェクトおよびフィールドが決定されます。 役割によって、オブジェクト フィールドの権限がないことを指定される場合、フィールドはマッピングに使用できません。マッピングの作成およびデータのインポートができるのは、権限のあるオブジェクトとフィールドについてだけです。

注: データをマップする前に、CA APM ユーザ インターフェースを見直して、マッピングの作成に必要な情報を確認することをお勧めします。 たとえば、［アセット］ページを見直すと、アセット名、アセット ファミリ、モデル、およびクラスが必要であることがわかります。アセットの作成にはモデルが必要なので、［モデル］ページを見直すと、モデル名とアセット ファミリが必要であることがわかります。 マッピングを作成する前にユーザ インターフェースを見直すことで、マッピングの作成に必要なすべての情報が揃っているかを確認できます。

次の手順に従ってください:

1. 選択したインポートの［マッピング］領域の［Data Importer］ページ、［管理］タブで［新規］をクリックするか、［ソース フィールドのロード］をクリックします。

   - ［新規］をクリックすると、ソース データ ファイルからソース フィールドを個別に選択できます。
   - ［ソース フィールドのロード］をクリックすると、ソース データ ファイルからソース フィールドをすべて追加します。

   注: 既存のマッピングがある場合、［ソース フィールドのロード］をクリックすると、これらのマッピングをソース データ ファイルのソース フィールドに置換できます。また、このオプションを使用すると、マッピングにないソース データ ファイルからソース フィールドを追加することもできます。

   a. ［ソース フィールドのロード］をクリックした場合は、フィールドの隣の［レコード編集］アイコンをクリックします。

2. ［ソース フィールド］の隣の［選択］アイコンをクリックして（このフィールドが空の場合）、データ ソースから列を選択し、［OK］をクリックします。

   （すべてのソース フィールドをロードしたことにより）このフィールドにすでにソース フィールドが含まれる場合は、この手順をスキップできます。

   注: 列名前後に表示されるパーセント記号は、ソース データ ファイル内の列ヘッダとしての名前を識別します。また、ソース データ ファイル内のすべてのレコードに適用する［ソース フィールド］でハードコードされた値を指定できます。 その後、ハードコードされた値を［インポート先フィールド］にマップできます。ハードコードされた値は、ソース データ ファイルの列名と区別できるように、パーセント記号で表示されません。 詳細については、「ハードコードされた値 (P. 201)」を参照してください。

3. ［インポート先フィールド］の隣の［選択］アイコンをクリックして、選択された［ソース フィールド］に［インポート先フィールド］を選択し、［OK］をクリックします。

   表示されるインポート先フィールドは、選択した主なインポート先オブジェクトに基づきます。

   注: インポート先フィールドは階層順に表示されます。 たとえば、［アセット タイプ］階層の下に一覧表示されるフィールドには、［アセット ファミリ］、［クラス］、および［サブクラス］があります。 リスト内でのフィールドの順序は、フィールド階層を表します。 マッピング ルールを指定するときは、フィールド階層に従います。たとえば、［アセット タイプ］階層の場合、［サブクラス］のルールを指定する前に、［クラス］のルールを指定します。

4. 必要に応じて、［プライマリ ルックアップ］および［セカンダリ ルックアップ］チェック ボックスをオンにします。

   a. プライマリ オブジェクトの検索に使用する各インポート先フィールドの［プライマリ ルックアップ］チェック ボックスをオンにします。 このチェック ボックスをオンにするときは、以下のガイドラインに従います。

      - インポート用の列マッピング内の［プライマリ ルックアップ］チェック ボックスを 1 つ以上オンにします。
      - ［インポート先フィールド］が［特記事項テキスト］（［特記事項］オブジェクトの下）である場合は、このチェック ボックスをオフにします。 ［特記事項テキスト］フィールドのデータベース データ タイプは、ルックアップ フィールドとして機能することができません。

   b. セカンダリ オブジェクトの検索に使用する各インポート先フィールドの［セカンダリ ルックアップ］チェック ボックスをオンにします。 このチェック ボックスをオンにするときは、以下のガイドラインに従います。

      - インポート先フィールドが、セカンダリ オブジェクト用のルックアップ フィールドでない場合は、このチェック ボックスをオフにします。
      - ［インポート先フィールド］が［特記事項テキスト］（［特記事項］オブジェクトの下）である場合は、このチェック ボックスをオフにします。 ［特記事項テキスト］フィールドのデータベース データ タイプは、ルックアップ フィールドとして機能することができません。

5. ［レコード編集を完了］アイコンをクリックします。

6. 再度［新規］をクリックするか、別のソース フィールドの隣の［レコード編集］アイコンをクリックして、その他のマッピング ルールを指定します。

   注: マップされた列のリストから特定のマッピング ルールを削除するには、マッピング ルールの隣の［削除］アイコンをクリックします。 列マッピング ルールがリストから削除されます。

7. ［保存］をクリックします。

   列マッピングが保存されます。

例: データ ファイル列のデータ フィールドへのマップ

サムはソース データ ファイル内のデータ ファイル列を CA APM データ フィールドにマップするために以下の手順を行います。

1. ［インポート詳細］ページの［マッピング］領域で［新規］をクリックします。
2. ［ソース フィールド］の隣の［選択］アイコンをクリックしダイアログ ボックスからこの項目を選択することにより、［ソース フィールド］内の［%ログイン ID%］を選択します。

   ダイアログ ボックスに一覧表示される項目はソース データ ファイルの列です。
3. ［インポート先フィールド］の隣の［選択］アイコンをクリックしダイアログ ボックスからこのオブジェクトを選択することにより、［インポート先フィールド］内の［ユーザ ID］を選択します。
4. ［プライマリ ルックアップ］チェック ボックスをオンにします。
5. 引き続き CA APM データ フィールドがあるソース データ ファイル内の残りの列をマップし、終了時に［保存］をクリックします。

マッピング参考資料の確認

データのインポートまたは削除のために列マッピングをセットアップするときは以下の情報を参照します。

プライマリおよびセカンダリ ルックアップの組み合わせ

列マッピング内でプライマリおよびセカンダリ ルックアップとして選択するフィールドは、製品データベース内のデータを検索するために使用されます。

単純なマッピング

単純なマッピングでは、プライマリ ルックアップのみを指定します。たとえば、一連の会社レコードをテキスト ファイルから製品データベースにインポートしたりまたは削除するとします。プライマリ ルックアップとして［会社名］を指定します。特定の名前を持つ会社がデータのインポートを行っているデータベース内に存在しない場合は、その会社のレコードが作成されます。 以下の表に、単純なマッピング用のルックアップの例を示します。

ソース フィールド	インポート先フィールド	プライマリ ルックアップ	セカンダリ ルックアップ
%会社名%	会社.会社名	はい	いいえ

参照フィールド マッピング

参照フィールド マッピングでは、プライマリおよびセカンダリ ルックアップ値を指定します。 一意のオブジェクトを検索するには、複数のプライマリ ルックアップを指定します。たとえば、会社を検索するには、プライマリ ルックアップ値として［会社名］、［親会社］および［会社タイプ］を指定できます。 この例では、Data Importer は指定した名前と指定した親会社を持つ、指定した会社タイプの会社を検索します。オブジェクトが存在せず、データをインポートしている場合は、（［詳細設定］で選択した［挿入または更新］オプションに応じて）レコードが作成されます。以下の表に、参照フィールド マッピング用のルックアップの例を示します。

ソース フィールド	インポート先フィールド	プライマリ ルックアップ	セカンダリ ルックアップ
%会社名%	会社.会社名	はい	いいえ
%親会社%	会社.親会社.会社名	はい	はい
%会社タイプ%	会社.会社タイプ.値	はい	はい

このマッピングは［親会社］と［会社タイプ］について選択された［プライマリ ルックアップ］および［セカンダリ ルックアップ］チェックボックスの両方がオンになっています。 Data Importer は、［会社名］を使用して親会社を検索し、［親会社］を使用して会社名を検索します。

セカンダリ オブジェクト マッピング

マッピング ルールがセカンダリ オブジェクトのプロパティにマップされる場合、プライマリ ルックアップ値がセカンダリ オブジェクトとその参照フィールドとの関係を確立します。 以下の表に、セカンダリ オブジェクト マッピング用のルックアップの例を示します。

ソース フィールド	インポート先フィールド	プライマリ ルックアップ	セカンダリ ルックアップ
%コメント%	リーガル ドキュメント.法的関係者.コメント	いいえ	はい
%リーガル ドキュメント ID%	リーガル ドキュメント.ドキュメント識別子	はい	いいえ
%会社名%	リーガル ドキュメント.法的関係者.法的関係者.会社名	はい	はい
%リーガル テンプレート%	リーガル ドキュメント.リーガル テンプレート.テンプレート	はい	はい

最初のマッピング ルールで、［リーガル ドキュメント］はプライマリ オブジェクトで、［法的関係者］はセカンダリ オブジェクトです。 コメントは［法的関係者］のプロパティです。

3 番目のマッピング ルールで、［リーガル ドキュメント］はプライマリ オブジェクトで、［法的関係者］はセカンダリ オブジェクトです。 さらに、［法的関係者］は［会社］テーブル内に参照フィールドを持っています。 ［セカンダリ ルックアップ］チェック ボックスは、［会社名］が会社オブジェクトを検索するために使用されることを示します。［プライマリ ルックアップ］チェック ボックスは、会社オブジェクトが法的関係者オブジェクトを検索するために使用されることを示します。

ハードコードされた値

列マッピングでは、列名前後に表示されるパーセント記号は、ソース データ ファイル内の列ヘッダとしての名前を識別します。 また、ソース データ ファイル内のすべてのレコードに適用する［ソース フィールド］でハードコードされた値を指定できます。 その後、ハードコードされた値を［インポート先フィールド］にマップできます。 ハードコードされた値は、ソース データ ファイルの列名と区別するために、パーセント記号で表示されません。

1. ソース データ ファイルの列ヘッダ
2. ハードコードされた値

［ソース フィールド］でハードコードされた値を定義して、ソース データを展開し、必須フィールドがすべて含まれることを確認できます。 ハードコードされた値は通常、値の先頭と最後にパーセント記号（%）は付きません。 パーセント記号を含むハードコードされた値があると、その値はソース データ ファイルのフィールド名に一致しません。

例: アセット ファミリでのハードコードされた値の使用

この例では、ソース データ ファイル内のアセットにはアセットを作成するときに必要であるアセット ファミリが含まれません。 .ハードコードされた値をマッピングに追加できます。 アセットがすべてハードウェアである場合、［ソース フィールド］に「ハードウェア」と入力できます。この値を［アセット ファミリ］フィールドにマップできます。 アセットが別のファミリに属している場合は、データをインポートまたは削除する前に対応するアセット ファミリを持つソース データ ファイルに列を追加します。

以下の情報は、ソース データ ファイルからの値とハードコードされた値によって追加される値の差を示します。

- ソース データ ファイルに[アセット ファミリ]列があります。[ソース フィールド］内の選択内容は「%アセット ファミリ%」です。
- ソース データ ファイルに［アセット ファミリ］列がありません。 ただし、アセットはすべてハードウェア アセットです。［ソース フィールド］でハードウェアのハードコードされた値を指定します。

  注: また、［主なインポート先オブジェクト］を使用して、ソース データ ファイル内のすべてのレコードは特定のファミリまたはテンプレートに属していることを指定することができます。 たとえば、［主なインポート先オブジェクト］のアセット（ハードウェア）選択内容は、すべてのソース レコードはハードウェア アセット ファミリに属していることを指定します。

1 つのフィールドに対する複数の値

1 つの［インポート先フィールド］にマップされる複数の［ソース フィールド］値を持つマッピングを追加できます。

例: 1 つのフィールドに対して複数の値を使用する

データ ソースに［製造元］と［カタログ名］という名前の 2 つの列があります。［ソース フィールド］で両方の列を選択してこれらの列を組み合わせます。この例では、［ソース フィールド］選択内容は「%製造元% %カタログ名%」です。

また、［ソース フィールド］に複数のハードコードされた値を入力できます（たとえば、ドキュメント管理会社 %モデル名% IT 部門など）。

インポートでのフィルタ データ

インポートから除外するソース データ ファイル内のレコードのサブセットを識別できます。Data Importer 除外フィルタにより、除外フィルタ ルールを使用して、データ ソースの一部をフィルタすることができます。

例: 返却されたアセットを処理する例外フィルタの定義

ハードウェア ベンダーから受け取る CSV ファイルには、ベンダーに対して注文および返却されたアセットが含まれます。返品されたアセットだけを処理したいので、データをインポートして、それらのレコードのみを更新します。 例外フィルタを定義して、ステータスが［返却済み］でないレコードを除外します。

次の手順に従ってください:

1. 選択したインポートの［例外フィルタ］領域の［Data Importer］ページ、［管理］タブで［フィルタ タイプ］を選択します。

   AND

   指定したすべてのルールがレコードに有効な場合にのみ、ソース データ ファイルからレコードを除外します。

   OR

   指定したルールのいずれかがレコードに有効な場合に、ソース データ ファイルからレコードを除外します。

2. ［新規］をクリックします。
3. ［ソース フィールド］の隣の［選択］アイコンをクリックして、ソース データ ファイルから列を選択し、［OK］をクリックします。

   注: 列名前後のパーセント記号は、ソース データ ファイルからの列としての名前を識別します。

4. ［演算子］を選択します。

   注:「等しくない」を指定するには、「<>」演算子を選択します。

5. ルールのフィルタ値を入力します。

   注: フィルタ値には特殊文字およびワイルドカードを使用できます。 ルールは、テキスト、数値、日付のフィールドを処理できます。

6. ［レコード編集を完了］アイコンをクリックします。
7. （オプション）［新規］をクリックして、その他の例外フィルタ ルールを指定します。
8. ［保存］をクリックします。

   除外フィルタ ルールが保存され、インポート プロセス時に適用されます。

例: 例外フィルタの作成

サムは除外フィルタを作成するために以下の手順を実行します。フィルタはデータ インポートから非 IT 社員、および会社本部以外で勤務している社員を除外します。

1. ［インポート詳細］ページの［例外フィルタ］領域で［フィルタ タイプの And］を選択し［新規］をクリックします。
2. ［ソース フィールド］に［%部門%］を選択します。
3. 演算子として［<>］を選択します。
4. フィルタ値に「IT」と入力します。

5. ［レコード編集を完了］アイコンをクリックし、［新規］をクリックします。
6. ［ソース フィールド］に［%ロケーション%］を選択します。
7. 演算子として［<>］を選択します。
8. フィルタ値に「本社」と入力します。
9. ［レコード編集を完了］アイコンをクリックして、［保存］をクリックします。

インポートのサブミット

インポートをすぐに開始するには、ページの［スケジュール］領域の［サブミットする］をクリックします。 選択されたインポート用のデータ ファイルからのデータ ソース レコードが処理されます。

注: 別のファイルを使用する場合、デフォルト以外のデータ ファイル（［基本情報］から）を指定できます。

また、特定の曜日および時間に対するインポートをスケジュールできます。 詳細については、「インポートのスケジュール (P. 205)」を参照してください。

現在の選択されたインポート用のインポート ジョブを表示するには、ページの左側にある［関連ジョブ］をクリックします。 すべてのインポート用のインポート ジョブをすべて表示するには、ページの左側にある［インポート ジョブ］をクリックします。 表示されるインポート ジョブのリストで［ステータス メッセージ］をクリックして、インポートのステータスを表示します。

インポート アクティビティの詳細については、ログ ファイルでも確認できます。 インポート ジョブのリストで、選択されたインポートの［ログの表示］をクリックします。

インポートのスケジュール

インポートを特定の時間にスケジュールできます。また、インポートの間隔（日単位や週単位など）を指定できます。 複数のインポートを同時に処理するようにスケジュールできます。

次の手順に従ってください:

1. 選択したインポートの［スケジュール］領域の［Data Importer］ページ、［管理］タブで［スケジュール済み］チェック ボックスをオンにします。
2. スケジュールの情報を提供します。 以下のフィールドについて説明します。

実行時刻

インポートを処理する時間を 24 時間の形式で指定します。 インポートをスケジュールするときは、CA APM アプリケーション サーバのローカル タイム ゾーンを使用してください。

間隔日

間隔タイプ中にインポートを処理する日を指定します。たとえば、［間隔タイプ］が［月］で、［間隔日］が「1」である場合、インポートは月の 1 日に処理されます。

データ ファイル

別のファイルを使用したい場合は、デフォルト（基本情報からの）以外のデータ ファイル名を指定します。

このファイルがアプリケーション サーバで利用可能な場合は、ファイルを検索および選択できます。 このファイルがアプリケーション サーバで利用可能でない場合は、ファイルを見つけてアップロードできます。

データ ファイルのアップロード

インポートするソース データ ファイルを参照します。このファイルはアプリケーション サーバにアップロードされます。

初回実行日

最初のインポート処理を開始する日を指定します。

間隔タイプ

インポートの間隔のタイプ（日、月、四半期、週、または年）を指定します。

間隔

インポートを処理する頻度を指定します。 この間隔は、指定された［期間タイプ］に基づきます。たとえば、［間隔タイプ］が［週］で、［間隔］が「2」である場合、インポートは 2 週間ごとに処理されます。

間隔の最終日

インポートが選択された間隔タイプの最終日に処理されるように指定します。 このチェック ボックスをオンにすると、［間隔日］フィールドに追加した前の値は削除され、［間隔日］フィールドは無効になります。

3. ［サブミット］をクリックします。

データ インポートが指定された日付と時刻にスケジュールされます。

例: スケジュール設定の使用

以下の例では、スケジュール設定の使い方を示します。

- ［間隔タイプ］で［日］を選択し、［間隔］に「2」を指定します。インポートは 1 日ごとに処理されます。
- ［間隔タイプ］で［週］を選択し、［間隔日］に「1」、［間隔］に「3」を指定します。 インポートは、3 週間ごとに週の最初の日（日曜日）に処理されます。
- ［間隔タイプ］で［月］を選択し、［間隔日］に「15」、［間隔］に「2」を指定します。 インポートは、2 か月ごとに月の 15 日に処理されます。
- ［間隔タイプ］で［四半期］を選択し、［間隔の最終日］を選択します。 インポートは、各四半期（3 か月ごと）の最終月の最終日に処理されます。
- ［間隔タイプ］で［年］を選択し、［間隔日］に「1」、［間隔］に「1」を指定します。 インポートは、毎年 1 月 1 日に処理されます。

現在の選択されたインポート用のインポート ジョブを表示するには、ページの左側にある［関連ジョブ］をクリックします。 すべてのインポート用のインポート ジョブをすべて表示するには、ページの左側にある［インポート ジョブ］をクリックします。 表示されるインポート ジョブのリストで［ステータス メッセージ］をクリックして、インポートのステータスを表示します。

インポート アクティビティの詳細については、ログ ファイルでも確認できます。インポート ジョブのリストで、選択されたインポートの［ログの表示］をクリックします。

スケジュールの詳細の表示

スケジュールされた作成済みのインポート ジョブのスケジュール詳細を表示できます。

まず、インポート ジョブのリストを開きます。

- 現在の選択されたインポート用のスケジュールされたインポート ジョブを表示するには、ページの左側にある［関連ジョブ］をクリックし、［スケジュール済み］チェック ボックスをオンにして、［実行］をクリックします。
- すべてのインポート用のすべてのインポート ジョブを表示するには、ページの左側にある［インポート ジョブ］をクリックし、［実行］をクリックします。

表示されるインポート ジョブのリストで、選択されたインポートの［スケジュールの詳細］をクリックします。

インポート ログ ファイルの表示

Data Importer ログ ファイルを表示して、完了した CA が提供するインポートおよびユーザ定義インポートすべての詳細を参照することができます。 Data Importer は、実行する各インポートのログ ファイルを作成します。これには、すぐにサブミットされたインポートと、将来実行されるようにスケジュールされたインポートが含まれます。 すべてのインポート アクティビティはログ ファイルに保存されます。

ログ ファイルを表示するには、まずインポート ジョブのリストを開きます。

- 現在の選択されたインポート用のインポート ジョブを表示するには、ページの左側にある［関連ジョブ］をクリックします。
- すべてのインポートのすべてのインポート ジョブを表示するには、［インポート ジョブ］をクリックします。

インポート ジョブのリストで、選択されたインポートの［ログの表示］をクリックします。複数のログ ファイルが使用可能な場合（たとえばスケジュールされたインポートがすでに数回完了している場合）、すべてのファイルはそれらの対応する作成日とともにリスト表示されます。

使用可能な LDAP インポート同期ログ ファイルはすべて表示できます。 ［LDAP データ インポートおよび同期］ページ（［管理］-［ユーザ/役割管理］）の［LDAP データ インポートおよび同期の開始］をクリックすると、インポート ジョブ ID が表示されます。 このジョブ ID を使用して、Data Importer のインポート ジョブ リストでジョブを探します。次に、そのジョブの［ログを表示］をクリックします。

注: また、CA APM アプリケーション サーバ上の以下のロケーションにインポート ログ ファイルを置き表示できます。

```
[ITAM Root Path]¥Storage¥Common Store¥Import¥Logs
```

インポート ログ ファイルの表示 - ベスト プラクティス

Data Importer ログ ファイルには、インポート ジョブの処理に関する情報およびエラー メッセージが含まれます。 インポートの結果を理解しエラーをトラブルシュートするには、このログ ファイルの情報を使用します。このセクションには Data Importer ログ ファイルでの動作に関する推奨ベスト プラクティスが含まれます。

データ ファイル内の行番号とログ ファイル内のエラー メッセージを一致させます。

ログ ファイル エラー メッセージは、データ ファイルからの対応する行番号を識別します。 また、ログ ファイル内のエラー メッセージより上の、またはそのエラー メッセージより下の行にあるデータ ファイル行番号を検索できます。

ログ ファイル内のエラー メッセージがデータ ファイル行番号を表示しない場合があります。この場合、実際のデータ ファイル値はログ ファイル内のエラー メッセージの直後に表示されます。

ログ ファイル内のエラー メッセージの数を数えます。

1. ログ ファイル内で以下のフレーズを検索し、ファイル内のエラー メッセージを検索します。 これらのフレーズはエラー メッセージに含まれています。

   Web サービスから例外がスローされました

   レコードのエラー

2. エラー メッセージのタイプを検索した後、ログ ファイル内でそのエラーを検索し、発生数を数えます。
3. ログ ファイルに表示されるさらなるエラー タイプを識別および検索し、発生数を数えます。
4. ログ ファイルのすべてのエラーの数を Data Importer が関連するインポートに対して生成した統計と比較します。 これらの統計を表示するには、［関連ジョブ］リストまたは［インポート ジョブ］リスト上の［ステータス メッセージ］をクリックします。 この比較により、すべての関連するエラーを明らかにし、有効でなく無視できるエラー メッセージを識別することができます。

インポートされたデータの確認

CA APM 内のデータを表示し、Data Importer 統計を確認することでデータ インポートが成功したことを確認します。

- **Data Importer 統計を確認します。** 現在の選択されたインポートの統計を確認するには、ページの左側にある［関連ジョブ］をクリックします。 表示されるインポート ジョブのリストで、インポートの［ステータス メッセージ］をクリックします。

  インポート アクティビティの詳細については、ログ ファイルでも確認できます。 インポート ジョブのリストで、選択されたインポートの［ログの表示］をクリックします。

- **CA APM 内のインポートされたデータを表示します。** インポートされたデータを表示するには、インポートしたオブジェクト（たとえばアセット、会社または連絡先）のタブおよびサブタブ（必要に応じ）に移動します。インポートしたオブジェクトを検索し、オブジェクトが利用可能であることを確認します。

例: 新入社員のデータ インポートの確認

サムはインポートを実行した後、以下の手順を実行して新入社員のデータ インポートを確認します。

1. インポート統計を確認します。
   - ［Data Importer］ページの左側にある［関連ジョブ］または［インポート ジョブ］をクリックします。
   - インポートの［ステータス メッセージ］をクリックし、統計を確認します。
2. インポート ログ ファイルおよびユーザ インターフェースを表示します。
   - インポート ジョブのリストで［ログの表示］をクリックして、ログ ファイルの内容を確認します。
   - CA APM ユーザ インターフェース上の［ディレクトリ］、［連絡先］に移動します。 新入社員を検索します。 非 IT 社員、および会社本部以外で勤務している社員が利用可能でないことを確認します。

第 9 章: Data Importer でデータを削除する方法

このセクションには、以下のトピックが含まれています。

Data Importer を使用したデータの削除方法

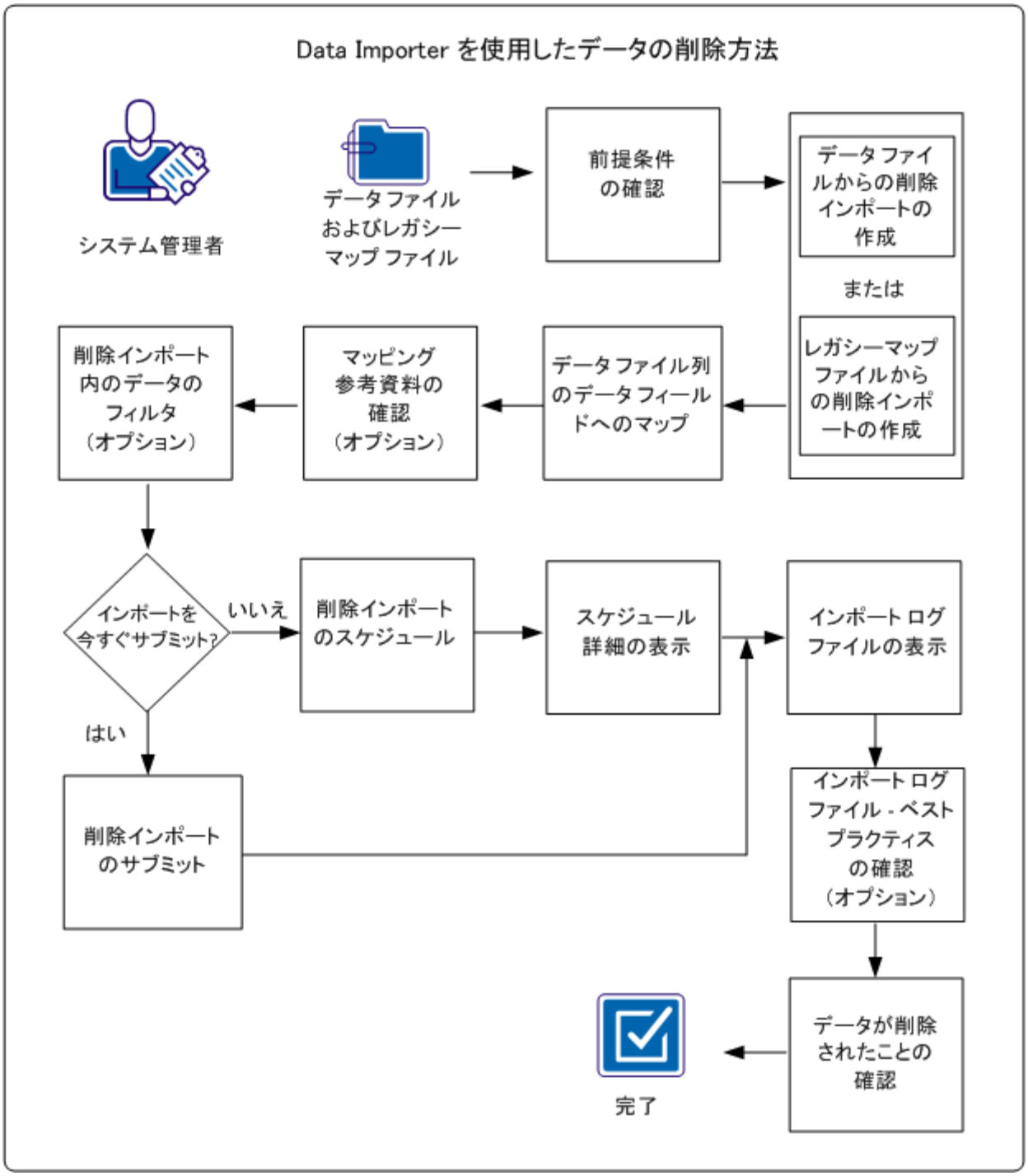
データが実装に対して無効になった場合、Data Importer を使用して CA APM からデータを削除します。 ただしほとんどの場合、非アクティブのステータスを持つリポジトリでデータを保持することは、IT アセット管理の推奨プラクティスです。この方法によって、履歴および監査の目的でデータにアクセスできます。ただし、場合によっては、データが誤って作成されることがあります。このような場合は、データを削除する必要があります。

重要: このシナリオでは、システム管理者がデータ削除を実行します。 ただし、管理者は Data Importer ユーザ アクセスまたは Data Importer 管理者アクセスを任意の CA APM ユーザ役割へ付与できます。 ユーザ アクセスにより、ユーザはインポートの作成、自分のインポートの変更または削除、別のユーザによって作成されたインポートの表示が可能になります。 管理者アクセスにより、ユーザはインポートの作成、任意のユーザによって作成されたインポートの変更または削除が可能になります。

プライマリ オブジェクトを削除でき、それらのセカンダリ オブジェクトとの関係を削除できます。 たとえば、アセット（プライマリ オブジェクト）を削除し、そのアセットのリーガル ドキュメント（セカンダリ オブジェクト）との関係を削除します。

プライマリ オブジェクトおよびそのセカンダリ オブジェクトとの関係を削除する場合、セカンダリ オブジェクトは削除されません。 プライマリ オブジェクトが削除され、プライマリ オブジェクトとセカンダリ オブジェクトとの関係が削除されます。 たとえば、アセットおよびその関連するリーガル ドキュメントとの関係を削除すると、アセットは削除されますが、リーガル ドキュメントは削除されません。 アセットとリーガル ドキュメントとの関係だけが削除されます。

以下の図は、システム管理者がデータを削除する方法を示しています。



CA APM データを削除するには、以下の手順を実行します。

1. 前提条件を確認します。 (P. 214)
2. データ ファイルから削除インポートを作成 (P. 215) またはレガシー マップ ファイルから削除インポートを作成 (P. 220) します。
3. ［データ ファイル］列を［データ］フィールドにマップします。 (P. 221)
4. マッピング参考資料を確認します。 (P. 198)
   - プライマリおよびセカンダリ ルックアップの組み合わせ (P. 198)
   - ハードコードされた値 (P. 201)
   - 1 つのフィールドに対する複数の値 (P. 202)
5. 削除インポートのデータをフィルタします (P. 228)。
6. 削除インポートをサブミット (P. 229) または削除インポートをスケジュール (P. 230) します。
7. ［スケジュールの詳細］を表示します (P. 207)。
8. インポート ログ ファイルを表示します。 (P. 207)
9. インポート ログ ファイル - ベスト プラクティスを確認します (P. 208)。
10. データが削除されたことを確認します (P. 234)。

例: ラップトップの削除

ミリアム（Document Management Company の CA APM システム管理者）は、廃止およびリサイクルされた複数のラップトップを削除する必要があります。ミリアムは、これらのラップトップに対して作成されたリーガル ドキュメントとの関連も削除する必要があります。 ミリアムは、ラップトップ名、製造元およびモデル名を識別するデータ ファイルを持っています。 Data Importer およびソース データ ファイルを使用して、ミリアムは削除インポートを作成します。インポートの実行後に、ミリアムはインポート統計、インポート ログ ファイルおよびユーザ インターフェースを表示して削除を確認します。

前提条件の確認

正常にデータを削除できるようにするには、以下のタスクが完了していることを確認します。

- 削除するデータを含む区切られたテキスト形式（たとえば、タブ区切りまたはカンマ区切り）のソース データ ファイルを準備します。

  注: ソース データ ファイルの名前に主なインポート先オブジェクトを含めることを推奨します。 このファイル命名規則は、インポートを作成したときにデータ ファイルを見つけるのに役立ちます。

  注: ソース データ ファイルに存在する NULL は、対応するインポート先フィールド値をクリアします。ソース データ ファイル内のフィールドが空の場合、対応するインポート先フィールド値は変更されません。

  重要: ソース データ ファイル内のデータ値に選択された区切り文字が含まれている場合、データ値を二重引用符で囲む必要があります。 たとえば、会社をインポートする際に区切り文字としてカンマを選択したとします。 また、ソース データ ファイルに Document Management Company, Inc. というデータ値を入力するとします。 この場合、このデータ値を二重引用符で囲みます。

  例： "Document Management Company, Inc"。

- （オプション）ソース データ ファイルをローカル サーバから以下のいずれかの場所にコピーします。ストレージ マネージャ サービスがインストールされている CA APM アプリケーション サーバ上でこれらの場所にアクセスできます。 ロケーションは、ユーザがマルチテナントを使用しているかどうかに依存します。

  ```
  [ITAM Root Path]¥Storage¥Common Store¥Import
  ```

  ```
  [ITAM Root Path]¥Storage¥Tenant_Name¥Import
  ```

  注: インポートを作成する前にデータ ファイルをコピーした場合は、インポートを作成するときにファイル名を指定できます。データ ファイルを最初にコピーしない場合は、インポートを作成するときにローカル サーバからファイルをアップロードできます。

- （オプション）ローカル サーバから旧製品リリース（これらのファイルがある場合）からレガシー マップ ファイルを以下のいずれかの場所にコピーします。ストレージ マネージャ サービスがインストールされている CA APM アプリケーション サーバ上でこれらの場所にアクセスできます。ロケーションは、ユーザがマルチテナントを使用しているかどうかに依存します。

  ```
  [ITAM Root Path]¥Storage¥Common Store¥Import
  ```

  ```
  [ITAM Root Path]¥Storage¥Tenant_Name¥Import
  ```

データ ファイルからの削除インポートの作成

削除するデータを含むソース データ ファイル（区切られたテキスト ファイル）を使用して、データを削除できます。 ファイルを選択し、インポート パラメータを設定し、ファイル内のデータを区切る区切り文字（たとえばカンマ）を指定します。

以前の製品リリースのレガシー マップ ファイルを使用して、削除インポートを作成することもできます。 詳細については、「レガシー マップ ファイルから削除インポートを作成する (P. 220)」を参照してください。

次の手順に従ってください:

1. 管理者として CA APM にログインします。

   重要: このシナリオでは、システム管理者が削除インポートを実行します。ただし、管理者は Data Importer ユーザ アクセスまたは Data Importer 管理者アクセスを任意の CA APM ユーザ役割へ付与できます。 ユーザ アクセスにより、ユーザはインポートの作成、自分のインポートの変更または削除、別のユーザによって作成されたインポートの表示が可能になります。 管理者アクセスにより、ユーザはインポートの作成、任意のユーザによって作成されたインポートの変更または削除が可能になります。

2. ［管理］-［Data Importer］をクリックします。
3. ［新規インポート］をクリックします。
4. ［基本情報］領域に必要な情報を入力し、必要に応じオプションの情報を提供します。 以下のフィールドについて説明します。

   データ ファイル

   ソース データ ファイルを指定します。

   このファイルが CA APM アプリケーション サーバで利用可能な場合は、データ ファイルを検索および選択します。 このファイルがアプリケーション サーバで利用可能でない場合は、ファイルをアップロードします。

   ファイルのアップロード

   ローカル サーバ上で、ソース データ ファイル、またはマッピングを作成するために使用するレガシー マップ ファイルを参照します。このファイルは CA APM アプリケーション サーバにアップロードされます。

   重要: ファイル サイズは、製品の環境設定によって制限されます。 詳細については、管理者にお問い合わせください。

主なインポート先オブジェクト

削除インポート用の主なオブジェクトを指定します。

アセットおよびモデル オブジェクトは、それぞれに対応するファミリと共にリスト表示されます。［すべてのファミリ］を指定することもできます。 リーガル ドキュメントのオブジェクトは、リーガル テンプレートに従ってリスト表示されます。［すべてのテンプレート］を指定することもできます。 オブジェクトには、インポートまたは削除できるすべてのオブジェクトが含まれます。

注: 複数のアセット ファミリ タイプを含むアセットまたはモデル、もしくは複数のリーガル テンプレートを含むリーガル ドキュメントの場合は、このフィールドに以下の選択を使用します。 ソース データ ファイルの各レコードの特定のファミリまたはテンプレートを指定します。

- アセットでは、［アセット］（すべてのファミリ）を選択します。
- モデルでは、［モデル］（すべてのファミリ）を選択します。
- リーガル ドキュメントでは、［リーガル ドキュメント］（すべてのテンプレート）を選択します。

重要: 必ず正しい主なインポート先オブジェクトを選択してください。インポートを保存またはコピーした後で主なインポート先オブジェクトを変更することはできません。

最初の行を列名にする

ソース データ ファイルの最初の行に列名を含めるかどうかを指定します。最初の行に列名を含めない場合、名前は「フィールド 1」や「フィールド 2」などの一般的な名前で表示されます。

テナント

インポートに適用されるテナントを指定します（マルチテナントを使用している場合）。

テナントを選択できるのは、CA APM でマルチテナントが有効になっていて、さまざまなテナントにアクセスする権限が与えられているときだけです。 公開データへのアクセス権があり、複数のテナントを持っている場合は、すべてのテナントを選択できます。

すべてのテナントを指定する場合、ソース データ ファイルには［テナント名］フィールドにマップするテナント名の列が必要です。

注: 1 つのテナントを指定する場合は、ソース データ ファイル内のすべてのデータが選択したテナントに属していることを確認してください。複数のテナントのデータがある場合、すべてのテナントのデータが選択したテナントに適用されます。

データ区切り文字

ソース データ ファイルで使用した区切り文字（たとえばカンマまたはタブ）を指定します。

重要: ソース データ ファイル内のデータ値に選択された区切り文字が含まれている場合、データ値を二重引用符で囲む必要があります。 たとえば、会社をインポートする際に区切り文字としてカンマを選択したとします。また、ソース データ ファイルに Document Management Company, Inc. というデータ値を入力するとします。 この場合、このデータ値を二重引用符で囲みます。

例： "Document Management Company, Inc"

データ ファイルのロケール

ソース データ ファイルのロケールを選択します。 この設定は、日付および時刻の形式を指定します。

5. ［詳細設定］領域に必要な情報を入力し、必要に応じオプションの情報を提供します。

以下のフィールドについて説明します。

最大エラーしきい値（%）

インポートを停止するためのエラーの回数を定義します。 しきい値は、処理されたレコードのパーセンテージに基づきます。 15 パーセント以上のしきい値を推奨します。

注: Data Importer は、エラーしきい値に達した場合、計算する前の管理、システム構成、Data Importer（［最大バッチ レコード サイズ］フィールド）上で指定されるレコードの数を処理します。

プライマリ ルックアップ オブジェクト処理タイプ

インポート アクティビティのタイプを指定します。 以下のいずれかのオプションを選択します。

プライマリ オブジェクトおよび関連する関係の削除

プライマリ オブジェクトと、それらに関連付けられているセカンダリ オブジェクトとの関係を削除するには、このオプションを選択します。 たとえば、会社（プライマリ オブジェクト）を削除し、関連付けられているアセット配置（セカンダリ オブジェクト）との関係を削除します。

このオプションを選択するときは、マッピング ルールでプライマリ オブジェクトだけが指定されていることを確認してください。 セカンダリ オブジェクトのマッピング ルールは一切含めないでください。

注: プライマリ オブジェクトに関連付けられているセカンダリ オブジェクトは削除されません。 プライマリ オブジェクトとセカンダリ オブジェクトとの関係が削除されます。 たとえば、プライマリ オブジェクト Company1 と、関連付けられている被買収会社 Company2 （セカンダリ オブジェクト）があるとします。 Company1 を削除すると、Company2 に対する関係が削除されます。セカンダリ オブジェクト Company2 は削除されません。

関係のみの削除（Delete Relationships Only）

セカンダリ オブジェクトとそのプライマリ オブジェクトとの関係を削除するには、このオプションを選択します。このオプションを選択するときは、マッピング ルールでプライマリ オブジェクトとセカンダリ オブジェクトだけが指定されていることを確認してください。 セカンダリ オブジェクトのマッピング ルールを含めますが、そのルールの［プライマリ ルックアップ］チェック ボックスをオンにしないでください。

注: プライマリ オブジェクトに関連付けられているセカンダリ オブジェクトは削除されません。 プライマリ オブジェクトとセカンダリ オブジェクトとの関係が削除されます。

正規化の動作

データを正規化するか、またはデータを正規化せずにログ ファイルにエラー メッセージを書き込むかどうかを指定します。

注: このフィールドは、正規化ルールを定義している場合にのみ表示されます。

正規化エラー

削除するデータ内に正規化できるデータが見つかった場合、エラー メッセージを Data Importer ログ ファイルに書き込みます。該当のデータは削除されません。 ログ ファイル エラー メッセージには、データに関する詳細が含まれます。

たとえば、データに会社名 Microsoft が含まれるとします。 作成した会社正規化ルールによって、Microsoft は収集（非権限）値として識別され、Microsoft Corporation が正規化された（権限）値として指定されます。データの削除時にこのオプションを選択すると、会社名 Microsoft を含むオブジェクトは削除されず、エラー メッセージがログ ファイルに書き込まれます。

エラーなしで正規化を適用

正規化ルールを使用して、削除するデータを正規化します。正規化できるデータが見つかった場合、そのデータは正規化および削除されます。 データに関するエラー メッセージはログ ファイルに書き込まれません。

たとえば、データに会社名 Microsoft が含まれるとします。 作成した会社の正規化ルールによって、Microsoft は収集（非権限）値として識別され、Microsoft Corporation が正規化された（権限）値として指定されます。データの削除時にこのオプションを選択すると、会社名 Microsoft を含むオブジェクトは正規化されます。この例では、会社名が Microsoft Corporation に変更され、関連のあるオブジェクトが削除されます。

6. ［保存］をクリックします。

削除インポートが保存されます。ページの［マッピング］、［例外フィルタ］および［スケジュール］領域に入力できるようになりました。

例: データ ファイルからの削除インポートの作成

ミリアム（CA APM システム管理者）は以下のアクションを実行して削除インポートを作成します。

1. ［管理］-［Data Importer］に移動して、［新規インポート］をクリックします。
2. ［データ ファイル］フィールドに「Hardware Deletions.csv」と入力します。

この CSV ファイルは、ラップトップ削除を含むソース データ ファイルです。

3. ［主なインポート先オブジェクト］には［アセット（ハードウェア）］、および［データ区切り文字］にはカンマを選択します。
4. ［プライマリ ルックアップ オブジェクト処理タイプ］フィールドで［プライマリ オブジェクトおよび関連する関係の削除］を選択して、［保存］をクリックします。

レガシー マップ ファイルからの削除インポートの作成

以前の CA APM リリースのレガシー マップ ファイルを使用して、削除インポートを作成できます。 マップ ファイルは対応するデータ ファイルおよびインポート パラメータ設定を定義します。

注: 削除インポートを作成する前に、CA APM アプリケーション サーバにレガシー マップ ファイルおよび対応するデータ ファイルをコピーすることをお勧めします。ただし、必要な場合、レガシー マップ ファイルをアップロードするオプションの手順を使用できます。

データ ファイルのみを使用して、削除インポートを作成することもできます。詳細については、「データ ファイルから削除インポートを作成する (P. 215)」を参照してください。

次の手順に従ってください:

1. ［管理］-［Data Importer］-［新規インポート］をクリックします。
2. ［マップの検索およびロード］をクリックして、CA APM アプリケーション サーバに存在するレガシー マップ ファイル名を選択します。

   重要: 対応するデータ ファイルは、CA APM アプリケーション サーバで利用可能である必要があります。

   レガシー マップ ファイルが CA APM アプリケーション サーバに存在しない場合は、［ファイルのアップロード］フィールドを使用してファイルをアップロードします。

3. （オプション） 以下の手順に従って、CA APM アプリケーション サーバに存在しないレガシー マップ ファイルをアップロードします。

   a. ［ファイルのアップロード］フィールドで、ローカル サーバを参照し、レガシー マップ ファイルを選択します。

      レガシー マップ ファイルがアップロードされ、［ファイルのアップロード］フィールドに表示されます。

   b. ［マップの検索およびロード］をクリックして、アップロードしたレガシー マップ ファイルを選択します。

      レガシー マップ ファイルが［レガシー マップ ファイル］フィールドに表示されます。

      基本情報がロードされます。

   注: ソース データ ファイルに関する警告が表示されたら、［ファイルのアップロード］フィールドを使用してファイルをアップロードします。

4. ［詳細設定］を指定して、［保存］をクリックします。

   例外フィルタおよびマッピング データ マッピングがロードされます。ページの［マッピング］、［例外フィルタ］および［スケジュール］領域に入力できるようになりました。 ［マッピング］および［例外フィルタ］領域には、レガシー マップ ファイルのデータが表示されます。

   注: ［詳細設定］への値の設定については、「データ ファイルからの削除インポートの作成 (P. 215)」を参照してください。

データ ファイル列のデータ フィールドへのマップ

ソース データ ファイル内の列を製品フィールドにマップできます。 列マッピングを実行して削除するデータを指定します。 列マッピング中に、ほとんどのオブジェクトおよび関連するフィールドをインポート先フィールドとして選択できます。

注: レガシー マップ ファイルから削除インポートを作成した場合に、列マッピングが存在します。 値を変更する場合、既存のマッピング ルールを編集できます。新しいマッピング ルールを追加することもできます。

ログイン時に、管理者が割り当てたユーザ役割によって参照および使用できるオブジェクトおよびフィールドが決定されます。 役割によって、オブジェクト フィールドの権限がないことを指定される場合、フィールドはマッピングに使用できません。 マッピングの作成、および権限のあるオブジェクトおよびフィールドのデータのインポートまたは削除のみ可能です。

次の手順に従ってください:

1. 選択した削除インポートの［マッピング］領域の［Data Importer］ページ、［管理］タブで［新規］をクリックするか、［ソース フィールドのロード］をクリックします。

   - ［新規］をクリックすると、ソース データ ファイルからソース フィールドを個別に選択できます。
   - ［ソース フィールドのロード］をクリックすると、ソース データ ファイルからソース フィールドをすべて追加します。

   注: 既存のマッピングがある場合、［ソース フィールドのロード］をクリックすると、これらのマッピングをソース データ ファイルのソース フィールドに置換できます。また、このオプションを使用すると、マッピングにないソース データ ファイルからソース フィールドを追加することもできます。

   a. ［ソース フィールドのロード］をクリックした場合は、フィールドの隣の［レコード編集］アイコンをクリックします。

2. ［ソース フィールド］の隣の［選択］アイコンをクリックして（このフィールドが空の場合）、データ ソースから列を選択し、［OK］をクリックします。

   （すべてのソース フィールドをロードしたことにより）このフィールドにすでにソース フィールドが含まれる場合は、この手順をスキップできます。

3. ［インポート先フィールド］の隣の［選択］アイコンをクリックして、選択された［ソース フィールド］に［インポート先フィールド］を選択し、［OK］をクリックします。

   表示されるインポート先フィールドは、選択した主なインポート先オブジェクトに基づきます。

   注: インポート先フィールドは階層順に表示されます。 たとえば、［アセット タイプ］階層の下に一覧表示されるフィールドには、［アセット ファミリ］、［クラス］、および［サブクラス］があります。フィールドの順序は、フィールド階層を表します。マッピング ルールを指定するときは、フィールド階層に従います。 たとえば、［アセット タイプ］階層の場合、［サブクラス］のルールを指定する前に、［クラス］のルールを指定します。

4. 必要に応じて、［プライマリ ルックアップ］および［セカンダリ ルックアップ］チェック ボックスをオンにします。

   a. プライマリ オブジェクトの検索に使用する各インポート先フィールドの［プライマリ ルックアップ］チェック ボックスをオンにします。 このチェック ボックスをオンにするときは、以下のガイドラインに従います。

      - インポート用の列マッピング内の［プライマリ ルックアップ］チェック ボックスを 1 つ以上オンにします。
      - ［インポート先フィールド］が［特記事項テキスト］（［特記事項］オブジェクトの下）である場合は、このチェック ボックスをオフにします。 ［特記事項テキスト］フィールドのデータベース データ タイプは、ルックアップ フィールドとして機能することができません。

   b. セカンダリ オブジェクトの検索に使用する各インポート先フィールドの［セカンダリ ルックアップ］チェック ボックスをオンにします。 このチェック ボックスをオンにするときは、以下のガイドラインに従います。

      - インポート先フィールドが、セカンダリ オブジェクト用のルックアップ フィールドでない場合は、このチェック ボックスをオフにします。
      - ［インポート先フィールド］が［特記事項テキスト］（［特記事項］オブジェクトの下）である場合は、このチェック ボックスをオフにします。 ［特記事項テキスト］フィールドのデータベース データ タイプは、ルックアップ フィールドとして機能することができません。

5. ［レコード編集を完了］アイコンをクリックします。
6. （オプション）再度［新規］をクリックするか、別のソース フィールドの隣の［レコード編集］アイコンをクリックして、その他のマッピング ルールを指定します。

   注: マップされた列のリストから特定のマッピング ルールを削除するには、マッピング ルールの隣の［削除］アイコンをクリックします。 列マッピング ルールがリストから削除されます。

7. ［保存］をクリックします。

   列マッピングが保存されます。

例: データ ファイル列のデータ フィールドへのマップ

ミリアムは、以下の手順を実行してソース データ ファイルの列を CA APM データ フィールドにマップします。

1. ［インポート詳細］ページの［マッピング］領域で［新規］をクリックします。
2. ［ソース フィールド］の隣の［選択］アイコンをクリックし、ダイアログ ボックスからこの項目を選択することによって、［ソース フィールド］で［% ハードウェア名 %］を選択します。

   ダイアログ ボックスに一覧表示される項目はソース データ ファイルの列です。
3. ［インポート先フィールド］の隣の［選択］アイコンをクリックし、ダイアログ ボックスからオブジェクトを選択することによって、［インポート先フィールド］で［アセット名］を選択します。
4. ［プライマリ ルックアップ］チェック ボックスをオンにします。
5. ［レコード編集を完了］アイコンをクリックして、［保存］をクリックします。

マッピング参考資料の確認

データのインポートまたは削除のために列マッピングをセットアップするときは以下の情報を参照します。

プライマリおよびセカンダリ ルックアップの組み合わせ

列マッピング内でプライマリおよびセカンダリ ルックアップとして選択するフィールドは、製品データベース内のデータを検索するために使用されます。

単純なマッピング

単純なマッピングでは、プライマリ ルックアップのみを指定します。たとえば、一連の会社レコードをテキスト ファイルから製品データベースにインポートしたりまたは削除するとします。プライマリ ルックアップとして［会社名］を指定します。特定の名前を持つ会社がデータのインポートを行っているデータベース内に存在しない場合は、その会社のレコードが作成されます。 以下の表に、単純なマッピング用のルックアップの例を示します。

ソース フィールド	インポート先フィールド	プライマリ ルックアップ	セカンダリ ルックアップ
%会社名%	会社.会社名	はい	いいえ

参照フィールド マッピング

参照フィールド マッピングでは、プライマリおよびセカンダリ ルックアップ値を指定します。 一意のオブジェクトを検索するには、複数のプライマリ ルックアップを指定します。たとえば、会社を検索するには、プライマリ ルックアップ値として［会社名］、［親会社］および［会社タイプ］を指定できます。 この例では、Data Importer は指定した名前と指定した親会社を持つ、指定した会社タイプの会社を検索します。オブジェクトが存在せず、データをインポートしている場合は、（［詳細設定］で選択した［挿入または更新］オプションに応じて）レコードが作成されます。以下の表に、参照フィールド マッピング用のルックアップの例を示します。

ソース フィールド	インポート先フィールド	プライマリ ルックアップ	セカンダリ ルックアップ
%会社名%	会社.会社名	はい	いいえ
%親会社%	会社.親会社.会社名	はい	はい
%会社タイプ%	会社.会社タイプ.値	はい	はい

このマッピングは［親会社］と［会社タイプ］について選択された［プライマリ ルックアップ］および［セカンダリ ルックアップ］チェックボックスの両方がオンになっています。 Data Importer は、［会社名］を使用して親会社を検索し、［親会社］を使用して会社名を検索します。

セカンダリ オブジェクト マッピング

マッピング ルールがセカンダリ オブジェクトのプロパティにマップされる場合、プライマリ ルックアップ値がセカンダリ オブジェクトとその参照フィールドとの関係を確立します。 以下の表に、セカンダリ オブジェクト マッピング用のルックアップの例を示します。

ソース フィールド	インポート先フィールド	プライマリ ルックアップ	セカンダリ ルックアップ
%コメント%	リーガル ドキュメント.法的関係者.コメント	いいえ	はい
%リーガル ドキュメント ID%	リーガル ドキュメント.ドキュメント識別子	はい	いいえ
%会社名%	リーガル ドキュメント.法的関係者.法的関係者.会社名	はい	はい
%リーガル テンプレート%	リーガル ドキュメント.リーガル テンプレート.テンプレート	はい	はい

最初のマッピング ルールで、［リーガル ドキュメント］はプライマリ オブジェクトで、［法的関係者］はセカンダリ オブジェクトです。 コメントは［法的関係者］のプロパティです。

3 番目のマッピング ルールで、［リーガル ドキュメント］はプライマリ オブジェクトで、［法的関係者］はセカンダリ オブジェクトです。 さらに、［法的関係者］は［会社］テーブル内に参照フィールドを持っています。 ［セカンダリ ルックアップ］チェック ボックスは、［会社名］が会社オブジェクトを検索するために使用されることを示します。［プライマリ ルックアップ］チェック ボックスは、会社オブジェクトが法的関係者オブジェクトを検索するために使用されることを示します。

ハードコードされた値

列マッピングでは、列名前後に表示されるパーセント記号は、ソース データ ファイル内の列ヘッダとしての名前を識別します。 また、ソース データ ファイル内のすべてのレコードに適用する［ソース フィールド］でハードコードされた値を指定できます。 その後、ハードコードされた値を［インポート先フィールド］にマップできます。 ハードコードされた値は、ソース データ ファイルの列名と区別するために、パーセント記号で表示されません。

1. ソース データ ファイルの列ヘッダ
2. ハードコードされた値

［ソース フィールド］でハードコードされた値を定義して、ソース データを展開し、必須フィールドがすべて含まれることを確認できます。 ハードコードされた値は通常、値の先頭と最後にパーセント記号（%）は付きません。 パーセント記号を含むハードコードされた値があると、その値はソース データ ファイルのフィールド名に一致しません。

例：アセット ファミリでのハードコードされた値の使用

この例では、ソース データ ファイル内のアセットにはアセットを作成するときに必要であるアセット ファミリが含まれません。 .ハードコードされた値をマッピングに追加できます。 アセットがすべてハードウェアである場合、［ソース フィールド］に「ハードウェア」と入力できます。この値を［アセット ファミリ］フィールドにマップできます。 アセットが別のファミリに属している場合は、データをインポートまたは削除する前に対応するアセット ファミリを持つソース データ ファイルに列を追加します。

以下の情報は、ソース データ ファイルからの値とハードコードされた値によって追加される値の差を示します。

- ソース データ ファイルに[アセット ファミリ]列があります。[ソース フィールド］内の選択内容は「%アセット ファミリ%」です。
- ソース データ ファイルに［アセット ファミリ］列がありません。 ただし、アセットはすべてハードウェア アセットです。［ソース フィールド］でハードウェアのハードコードされた値を指定します。

  注: また、［主なインポート先オブジェクト］を使用して、ソース データ ファイル内のすべてのレコードは特定のファミリまたはテンプレートに属していることを指定することができます。 たとえば、［主なインポート先オブジェクト］のアセット（ハードウェア）選択内容は、すべてのソース レコードはハードウェア アセット ファミリに属していることを指定します。

1 つのフィールドに対する複数の値

1 つの［インポート先フィールド］にマップされる複数の［ソース フィールド］値を持つマッピングを追加できます。

例: 1 つのフィールドに対して複数の値を使用する

データ ソースに［製造元］と［カタログ名］という名前の 2 つの列があります。［ソース フィールド］で両方の列を選択してこれらの列を組み合わせます。この例では、［ソース フィールド］選択内容は「%製造元% %カタログ名%」です。

また、［ソース フィールド］に複数のハードコードされた値を入力できます（たとえば、ドキュメント管理会社 %モデル名% IT 部門など）。

削除インポートのデータのフィルタ

削除インポートから除外するソース データ ファイル内のレコードのサブセットを特定できます。Data Importer 除外フィルタにより、除外フィルタ ルールを使用して、データ ソースの一部をフィルタすることができます。

例: 返却されたアセットを処理する例外フィルタの定義

ハードウェア ベンダーから受け取る CSV ファイルには、ベンダーに対して注文および返却されたアセットが含まれます。ベンダーに返却されたアセットを削除するために、それらのレコードのみを処理する必要があります。 例外フィルタを定義して、ステータスが［返却済み］でないレコードを除外します。

次の手順に従ってください:

1. 選択した削除インポートの［管理］-［Data Importer］-［例外フィルタ］で、［フィルタ タイプ］を選択します。

   AND

   指定したすべてのルールがレコードに有効な場合にのみ、ソース データ ファイルからレコードを除外します。

   OR

   指定したルールのいずれかがレコードに有効な場合に、ソース データ ファイルからレコードを除外します。

2. ［新規］をクリックします。
3. ［ソース フィールド］の隣の［選択］アイコンをクリックして、ソース データ ファイルから列を選択し、［OK］をクリックします。

   注: 列名の前後のパーセント記号によって、ソース データ ファイルの列として名前を識別します。

4. ［演算子］を選択します。

   注:「等しくない」を指定するには、「<>」演算子を選択します。

5. ルールのフィルタ値を入力します。

   注: フィルタ値には特殊文字およびワイルドカードを使用できます。 ルールは、テキスト、数値、日付のフィールドを処理できます。

6. ［レコード編集を完了］アイコンをクリックします。
7. （オプション）［新規］をクリックして、その他の例外フィルタ ルールを指定します。
8. ［保存］をクリックします。

   例外フィルタ ルールが保存され、削除インポートの処理時に適用されます。

削除インポートのサブミット

削除インポートをすぐに開始するには、ページの［スケジュール］領域で［サブミットする］をクリックします。選択した削除インポート用のデータ ファイルのデータ ソース レコードが処理されます。

注: 別のファイルを使用する場合、デフォルト以外のデータ ファイル（［基本情報］から）を指定できます。

特定の曜日および時間に削除インポートをスケジュールすることもできます。詳細については、「削除インポートのスケジュール (P. 230)」を参照してください。

現在選択されている削除インポートのインポート ジョブを表示するには、ページの左側にある［関連ジョブ］をクリックします。すべてのインポートのすべてのインポート ジョブを表示するには、［インポート ジョブ］をクリックします。表示されるインポート ジョブのリストで[ステータス メッセージ]をクリックして、インポートのステータスを表示します。

インポート アクティビティの詳細については、ログ ファイルでも確認できます。インポート ジョブのリストで、選択されたインポートの［ログの表示］をクリックします。

削除インポートのスケジュール

特定の時間に削除インポートをスケジュールできます。また、削除インポートの間隔（日単位または週単位など）を指定できます。 複数の削除インポートを同時に処理するようにスケジュールできます。

次の手順に従ってください:

1. 選択した削除インポートの［管理］-［Data Importer］-［スケジュール］で、［スケジュール済み］チェック ボックスをオンにします。
2. スケジュールの情報を提供します。 以下のフィールドについて説明します。

   実行時刻

   削除インポートを処理する時刻を 24 時間形式で指定します。インポートをスケジュールするときは、CA APM アプリケーション サーバのローカル タイム ゾーンを使用してください。

   間隔日

   間隔タイプ内で削除インポートを処理する日を指定します。 たとえば、［間隔タイプ］が［月］で、［間隔日］が「1」である場合、インポートは月の 1 日に処理されます。

データ ファイル

別のファイルを使用したい場合は、デフォルト（基本情報からの）以外のデータ ファイル名を指定します。

このファイルがアプリケーション サーバで利用可能な場合は、ファイルを検索および選択できます。 このファイルがアプリケーション サーバで利用可能でない場合は、ファイルを見つけてアップロードできます。

データ ファイルのアップロード

ソース データ ファイルを参照します。このファイルはアプリケーション サーバにアップロードされます。

初回実行日

最初の削除インポート処理を開始する日付を指定します。

間隔タイプ

削除インポートの期間タイプ（日、月、四半期、週、または年）を指定します。

間隔

削除インポートを処理する頻度を指定します。 この間隔は、指定された［期間タイプ］に基づきます。 たとえば、［間隔タイプ］が［週］で、［間隔］が「2」である場合、インポートは 2 週間ごとに処理されます。

間隔の最終日

削除インポートが選択された間隔タイプの最終日に処理されるように指定します。 このチェック ボックスをオンにすると、［間隔日］フィールドに追加した前の値は削除され、［間隔日］フィールドは無効になります。

3. ［サブミット］をクリックします。

削除インポートは指定された日時にスケジュールされました。

例: スケジュール設定の使用

以下の例では、スケジュール設定の使い方を示します。

- ［間隔タイプ］で［日］を選択し、［間隔］に「2」を指定します。インポートは 1 日ごとに処理されます。
- ［間隔タイプ］で［週］を選択し、［間隔日］に「1」、［間隔］に「3」を指定します。インポートは、3 週間ごとに週の最初の日（日曜日）に処理されます。
- ［間隔タイプ］で［月］を選択し、［間隔日］に「15」、［間隔］に「2」を指定します。インポートは、2 か月ごとに月の 15 日に処理されます。
- ［間隔タイプ］で［四半期］を選択し、［間隔の最終日］を選択します。インポートは、各四半期（3 か月ごと）の最終月の最終日に処理されます。
- ［間隔タイプ］で［年］を選択し、［間隔日］に「1」、［間隔］に「1」を指定します。インポートは、毎年 1 月 1 日に処理されます。

現在選択されている削除インポートのインポート ジョブを表示するには、ページの左側にある［関連ジョブ］をクリックします。すべてのインポートのすべてのインポート ジョブを表示するには、［インポート ジョブ］をクリックします。表示されるインポート ジョブのリストで[ステータス メッセージ]をクリックして、インポートのステータスを表示します。

インポート アクティビティの詳細については、ログ ファイルでも確認できます。インポート ジョブのリストで、選択されたインポートの［ログの表示］をクリックします。

スケジュールの詳細の表示

スケジュールされた作成済みのインポート ジョブのスケジュール詳細を表示できます。

まず、インポート ジョブのリストを開きます。

- 現在の選択されたインポート用のスケジュールされたインポート ジョブを表示するには、ページの左側にある[関連ジョブ]をクリックし、［スケジュール済み］チェック ボックスをオンにして、［実行］をクリックします。
- すべてのインポート用のすべてのインポート ジョブを表示するには、ページの左側にある［インポート ジョブ］をクリックし、［実行］をクリックします。

表示されるインポート ジョブのリストで、選択されたインポートの［スケジュールの詳細］をクリックします。

インポート ログ ファイルの表示

Data Importer ログ ファイルを表示して、完了した CA が提供するインポートおよびユーザ定義インポートすべての詳細を参照することができます。 Data Importer は、実行する各インポートのログ ファイルを作成します。これには、すぐにサブミットされたインポートと、将来実行されるようにスケジュールされたインポートが含まれます。 すべてのインポート アクティビティはログ ファイルに保存されます。

ログ ファイルを表示するには、まずインポート ジョブのリストを開きます。

- 現在の選択されたインポート用のインポート ジョブを表示するには、ページの左側にある［関連ジョブ］をクリックします。
- すべてのインポートのすべてのインポート ジョブを表示するには、［インポート ジョブ］をクリックします。

インポート ジョブのリストで、選択されたインポートの［ログの表示］をクリックします。複数のログ ファイルが使用可能な場合（たとえばスケジュールされたインポートがすでに数回完了している場合）、すべてのファイルはそれらの対応する作成日とともにリスト表示されます。

使用可能な LDAP インポート同期ログ ファイルはすべて表示できます。 ［LDAP データ インポートおよび同期］ページ（［管理］-［ユーザ/役割管理］）の［LDAP データ インポートおよび同期の開始］をクリックすると、インポート ジョブ ID が表示されます。 このジョブ ID を使用して、Data Importer のインポート ジョブ リストでジョブを探します。次に、そのジョブの［ログを表示］をクリックします。

注: また、CA APM アプリケーション サーバ上の以下のロケーションにインポート ログ ファイルを置き表示できます。

```
[ITAM Root Path]¥Storage¥Common Store¥Import¥Logs
```

インポート ログ ファイルの表示 - ベスト プラクティス

Data Importer ログ ファイルには、インポート ジョブの処理に関する情報およびエラー メッセージが含まれます。 インポートの結果を理解しエラーをトラブルシュートするには、このログ ファイルの情報を使用します。このセクションには Data Importer ログ ファイルでの動作に関する推奨ベスト プラクティスが含まれます。

データ ファイル内の行番号とログ ファイル内のエラー メッセージを一致させます。

ログ ファイル エラー メッセージは、データ ファイルからの対応する行番号を識別します。 また、ログ ファイル内のエラー メッセージより上の、またはそのエラー メッセージより下の行にあるデータ ファイル行番号を検索できます。

ログ ファイル内のエラー メッセージがデータ ファイル行番号を表示しない場合があります。この場合、実際のデータ ファイル値はログ ファイル内のエラー メッセージの直後に表示されます。

ログ ファイル内のエラー メッセージの数を数えます。

1. ログ ファイル内で以下のフレーズを検索し、ファイル内のエラー メッセージを検索します。 これらのフレーズはエラー メッセージに含まれています。

   Web サービスから例外がスローされました

   レコードのエラー

2. エラー メッセージのタイプを検索した後、ログ ファイル内でそのエラーを検索し、発生数を数えます。
3. ログ ファイルに表示されるさらなるエラー タイプを識別および検索し、発生数を数えます。
4. ログ ファイルのすべてのエラーの数を Data Importer が関連するインポートに対して生成した統計と比較します。 これらの統計を表示するには、［関連ジョブ］リストまたは［インポート ジョブ］リスト上の［ステータス メッセージ］をクリックします。 この比較により、すべての関連するエラーを明らかにし、有効でなく無視できるエラー メッセージを識別することができます。

データが削除されたことの確認

CA APM のデータを表示して Data Importer 統計を確認することによって、削除インポートが成功したことを確認します。

- **Data Importer 統計を確認します。** 現在選択されている削除インポートの統計を表示するには、ページの左側にある［関連ジョブ］をクリックします。 表示されるインポート ジョブのリストで、インポートの［ステータス メッセージ］をクリックします。

  インポート アクティビティの詳細については、ログ ファイルでも確認できます。 インポート ジョブのリストで、選択されたインポートの［ログの表示］をクリックします。

- **CA APM のデータを表示します。** CA APM のデータを表示するには、必要に応じて、削除したオブジェクト（たとえば、アセット、会社または連絡先）のタブおよびサブタブに移動します。 削除したオブジェクトを検索して、そのオブジェクトが利用不可であることを確認します。

例: ラップトップの削除の確認

ミリアムは削除インポートの実行後に、以下の手順を実行してラップトップが削除されたことを確認します。

1. インポート統計を確認します。
   - ［Data Importer］ページの左側にある［関連ジョブ］または［インポート ジョブ］をクリックします。
   - 削除インポート用の［ステータス メッセージ］をクリックして、統計を確認します。
2. インポート ログ ファイルおよびユーザ インターフェースを表示します。
   - インポート ジョブのリストで［ログの表示］をクリックして、ログ ファイルの内容を確認します。
   - ［アセット］タブに移動します。 削除したラップトップを検索して、そのラップトップが利用不可であることを確認します。

第 10 章: 製品提供されたデータ インポートの管理

このセクションには、以下のトピックが含まれています。

製品提供されたデータ インポート タイプ

製品は、すでにすべてのマッピングと設定を含んでいる一連の事前定義済みデータ インポートを提供します。これらのインポートは、データ管理を開始するのに役立ちます。製品提供された 2 種類のデータ インポートによって、以下の機能を実行できます。

- 読み取り専用データ インポート - 連絡先の LDAP 同期インポートなどの内部システム機能をモニタできます。
- オブジェクト インポート - ロケーション、連絡先、およびアセットなどの共通オブジェクトのインポートを実行できます。

製品提供されたデータ インポートではマッピングと設定を変更できません。ただし、インポートをコピーし、コピーを変更することはできます。

製品提供された読み取り専用データ インポートのステータスのモニタ

読み取り専用データ インポートは内部システム関数を実行します。読み取り専用インポートのステータスはモニタできますが、これらのインポートをサブミットすることはできません。 読み取り専用インポートをコピーし、コピーを変更して独自のインポートを作成できます。

次の手順に従ってください:

1. ［管理］-［Data Importer］に移動します。
2. 製品提供された読み取り専用データ インポート（オブジェクト データ インポートではない）の 1 つをクリックします。 以下のフィールドについて説明します。

   CA APM - LDAP **同期インポート**

   CA EEM が生成したデータ ファイルを持つデータ インポートをサブミットします。 このデータ インポートは LDAP Sync コンポーネントによって連絡先を作成します。

   CA APM - **デバイス削除インポート**

   CA SAM が生成したデータ ファイルを持つデータ インポートをサブミットします。 このデータ インポートは、削除された検出済みアセットに関連付けられた情報を削除します。

   CA APM - **デバイスの挿入または更新インポート**

   CA SAM が生成したデータ ファイルを持つデータ インポートをサブミットします。 このデータ インポートは、検出されたアセットに関連付けられた情報を追加または更新します。
3. ページの左側で［関連ジョブ］をクリックします。
4. インポート ジョブのリスト内の［ステータス メッセージ］をクリックしてインポートのステータスを表示します。

製品提供されたオブジェクト データ インポートのサブミット

製品提供されたオブジェクト データ インポートは、共通オブジェクトのインポートを実行します。 これらのインポートをサブミットし、これらのインポートのステータスをモニタできます。 製品提供されたオブジェクト データ インポートをサブミットするには、データが関連するデータ ファイルに追加されたことを確認します。 また、独自のデータ ファイルを指定できます。 ただし、データ ファイル内の列ヘッダは製品提供されたデータ ファイル内の列ヘッダと一致する必要があります。

また、これらのインポートをコピーし、コピーを変更して独自のインポートを作成できます。

注: マルチテナント環境では、これらのインポートは［公開データ］テナントにデータを追加するか、既存のデータを更新します。

次の手順に従ってください:

1. ［管理］-［Data Importer］に移動します。
2. 製品提供されたオブジェクト データ インポート（読み取り専用インポートではない）の 1 つをクリックします。 以下のフィールドについて説明します。

   CA APM - **会社インポート**

   会社を作成および更新します。

   CA APM - **コスト センター インポート**

   コスト センターを作成および更新します。

   CA APM - **ロケーション インポート**

   ロケーションを作成および更新します。

   CA APM - **連絡先インポート**

   連絡先を作成および更新します。

   注: マルチテナントを使用している場合は、このインポートをサブミットできません。 このインポートをコピーし、テナントのマッピングを追加し、新しい連絡先インポートをサブミットします。

   CA APM - HW **モデル インポート**

   ハードウェア モデルを作成および更新します。

CA APM - HW アセット インポート

ハードウェア アセットを作成および更新します。

CA APM - 照合済みでない検出済みアセット インポート

検出されたアセットを作成および更新します。

注: 照合済みでない検出されたアセットに関する CA Business Intelligence レポートは、このデータ インポートの入力を提供します。 この CA Business Intelligence レポートには［クラス］および［ステータス］フィールドは含まれていません。 これらのフィールドは、このインポートに対応するデータ ファイルに追加します。

3. ［スケジュール］領域に自分のデータ ファイルを指定するか、製品提供のデータ ファイルを使用します。

   注: 製品提供のデータ ファイルにはデータは含まれていません。 インポートをサブミットする前に、製品提供のデータ ファイルにインポートするデータを追加します。 製品提供のデータ ファイルは、ストレージ マネージャ サービスがインストールされている CA APM アプリケーション サーバ上の以下の場所にあります。

   ```
   [ITAM Root Path]¥Storage¥Common Store¥Import
   ```

4. ［サブミット］をクリックします。

第 11 章: コマンド ラインを使用してデータ インポートをサブミットする方法

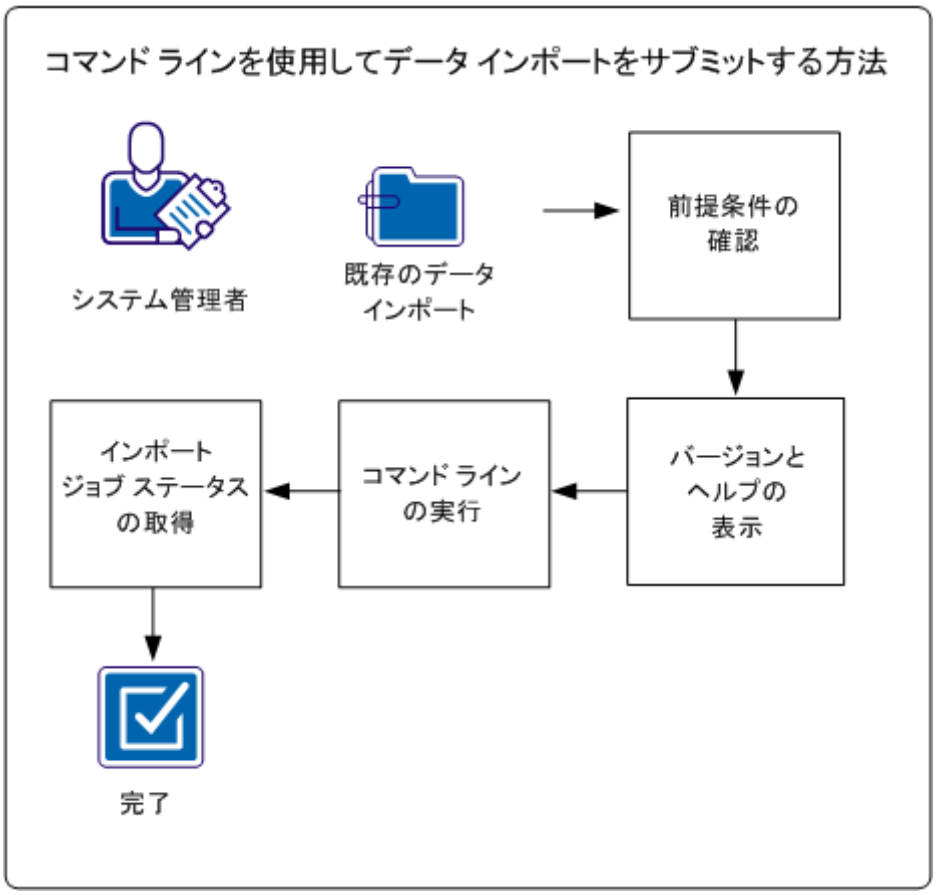
このセクションには、以下のトピックが含まれています。

コマンド ラインを使用してデータ インポートをサブミットする方法

CA APM ユーザ インターフェースを使用する代わりに、コマンド ラインを使用して処理用に Data Importer データ インポートをサブミットできます。 製品がインストールされているアプリケーション サーバ上の Import Processor フォルダからコマンド ラインを実行できます。また、別のコンピュータに Import Processor フォルダをコピーすることもできます。そのコンピュータのユーザもコマンド ラインを実行できます。

データ インポートはすぐにサブミットされ、CA APM ユーザ インターフェースからその他のインポート ジョブと共に Data Importer エンジンによって実行されます。 データ インポートをコマンド ラインを使用して特定の時刻に実行するようにスケジュールすることはできません。 ただし、スケジューラ（オペレーティング システム スケジューラなど）を使用してデータ インポートを実行する日時を指定できます。

以下の図は、システム管理者がコマンド ラインを使用してデータ インポートをサブミットする方法を示しています。



コマンド ラインを使用してデータ インポートをサブミットするには、以下の手順に従います。

1. 前提条件を確認します (P. 243)。
2. （オプション）バージョンおよびヘルプを表示します (P. 243)。
3. コマンド ラインを実行します (P. 244)。
4. インポート ジョブのステータスを取得します (P. 245)。

例: 新しいハードウェア デバイスのインポート

Document Management Company の CA APM システム管理者であるサムは、データ リポジトリに新しいハードウェア デバイスを追加する既存のデータ インポートを行っています。サムはそのデータ インポートを毎日実行したいと考えています。また、サブミットされたインポート ジョブのステータスを確認したいと思っています。 ただし、毎日その他の製品機能を必ずしも実行するとは限らないので、インポートを実行するために製品にログインしたくありません。 サムは、コマンド ラインを使用してデータ インポートをサブミットし、ステータスを確認します。

前提条件の確認

コマンド ラインを使用して正常にデータ インポートをサブミットできることを確認するには、以下の前提条件を満たしていることを確認します。

1. コマンド ラインを実行するコンピュータに Microsoft .NET Framework 4.0 がインストールされていることを確認します。
2. CA APM ユーザ インターフェースですべてのマッピングおよび設定を含むデータ インポートを定義します。
3. （オプション）インポート サービス URL を変更する場合は、新しい URL を反映するために ImportProcessor.exe.config ファイルを変更します。ImportProcessor.exe.config ファイルは Import Processor フォルダにあります。エンドポイントのアドレス値を更新します。

   例 : 以下のステートメントは、インポート サービス URL を変更するために修正するエンドポイントのアドレス値の例を示しています。

   ```
   <endpoint address="http://localhost/ImportService/ImportService.svc"
       binding="basicHttpBinding"
       bindingConfiguration="BasicHttpBinding_ImportService"
       contract="IImportService" name="BasicHttpBinding_ImportService" />
   ```

バージョンおよびヘルプの表示

コマンド ライン バージョンおよび使用法のヘルプを表示するためのコマンド ライン パラメータを指定します。

次の手順に従ってください:

1. CA APM をインストールしたアプリケーション サーバ、または Import Processor フォルダがあるコンピュータにログインします。
2. Import Processor フォルダにアクセスします。

   注: アプリケーション サーバでは、Import Processor フォルダは CA APM インストール パスにあります。

3. コマンド プロンプト ウィンドウを開いて、以下のコマンドを実行します。

   ```
   importerprocessor -H | -V
   ```

   -H

   コマンド ライン パラメータのコマンド ライン バージョン番号および使用法のヘルプを表示します。

   -V

   コマンド ライン バージョン番号を表示します。

コマンド ラインの実行

データ インポートをサブミットするためのコマンド ライン パラメータを指定します。

次の手順に従ってください:

1. CA APM をインストールしたアプリケーション サーバ、または Import Processor フォルダがあるコンピュータにログインします。
2. Import Processor フォルダにアクセスします。

   注: アプリケーション サーバでは、Import Processor フォルダは CA APM インストール パスにあります。
3. コマンド プロンプト ウィンドウを開いて、以下のコマンドを実行します。

   ```
   importerprocessor -usr "user_name" -pwd "password" -i "import_name"
   –df  "data_file_absolute_path" -t "tenant_name" –ts -c
   ```

   -usr

   CA APM ログイン ユーザ名を指定します。

   -pwd

   CA APM ログイン パスワードを指定します。

   -i

   CA APM ユーザ インターフェースで以前に作成されたデータ インポートの名前を指定します。

   -df

   データ インポートに関連付けられたデータ ファイルの絶対パスを指定します。 Data Importer エンジンは、このファイルを使用してインポートを処理します。

-t

（マルチテナントでは必須）データ インポートに関連付けられたテナントの名前を指定します。

-ts

（オプション）コマンド ライン パラメータが Import Processor ログ ファイルに記録されるように指定します。

注: Import Processor ログ ファイルは Import Processor フォルダにあります。

-c

（オプション）データ インポートが製品で提供されたか、またはユーザによって作成されたかを指定します。

有効な値： 1 （製品提供）または 0 （ユーザによって作成）

デフォルト： 0

インポート ジョブのステータスの取得

インポート ジョブのステータスを確認するためのコマンド ライン パラメータを指定します。

次の手順に従ってください:

1. CA APM をインストールしたアプリケーション サーバ、または Import Processor フォルダがあるコンピュータにログインします。
2. Import Processor フォルダにアクセスします。

   注: アプリケーション サーバでは、Import Processor フォルダは CA APM インストール パスにあります。
3. コマンド プロンプト ウィンドウを開いて、以下のコマンドを実行します。

   ```
   importerprocessor -usr "user_name" -pwd "password" -j "job_id" – ts
   ```

   -usr

   CA APM ログイン ユーザ名を指定します。

   -pwd

   CA APM ログイン パスワードを指定します。

-j

インポート ジョブ ID を指定します。

-ts

（オプション）コマンド ライン パラメータが Import Processor ログ ファイルに記録されるように指定します。

注: Import Processor ログ ファイルは Import Processor フォルダにあります。

第 12 章: プロセス ワークフローを使用してデータ インポートをサブミットする方法

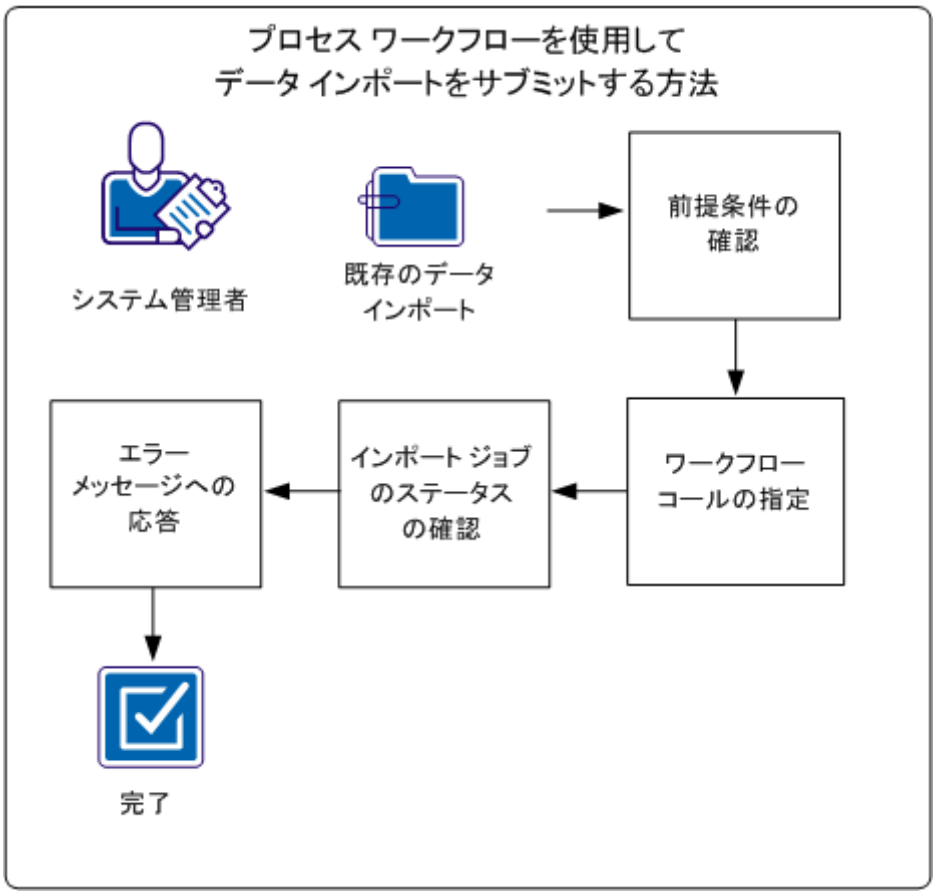
このセクションには、以下のトピックが含まれています。

プロセス ワークフローを使用してデータ インポートをサブミットする方法

CA APM ユーザ インターフェースを使用する代わりに、プロセス ワークフロー（たとえば CA Process Automation）を使用して処理用に Data Importer データ インポートをサブミットできます。

注: 会社から提供されたサンプル XML ファイルを使用し、CA Process Automation と統合して、データ インポート プロセス ワークフローを作成できます。 この統合の詳細については、「*実装ガイド*」を参照してください。

以下の図は、システム管理者がプロセス ワークフローを使用してデータ インポートをサブミットする方法を示しています。



プロセス ワークフローを使用して、データ インポートをサブミットするには、以下の手順に従います。

1. 前提条件を確認します (P. 249)。
2. ワークフロー呼び出しを指定します (P. 249)。
3. インポート ジョブのステータスを確認します (P. 252)。
4. （オプション）エラー メッセージに応答します (P. 253)。

例: プロセス ワークフローによる新しいハードウェア デバイスのインポート

Document Management Company の CA APM システム管理者であるサムは、ビジネス プロセス ワークフローを定義しました。 ワークフローによって、新しいハードウェア デバイスを検出し、社内データ リポジトリに新しいデバイスを追加し、新しいデバイスに関するレポートを実行します。サムは、データ リポジトリに新しいハードウェア デバイスを追加するデータ インポートを CA APM にすでに作成しています。サムはワークフロー全体の特定のポイントでそのデータ インポートを実行したいと考えています。 また、データ インポートをビジネス プロセス ワークフロー全体に統合したいと思っています。 ユーザが製品ユーザ インターフェースにログインすることなく、ワークフローで指定された時間にデータ インポートを実行することを望んでいます。 サムは、Data Importer の CA APM Web サービス操作に呼び出しを含めるためにビジネス プロセス ワークフローを更新します。

前提条件の確認

プロセス ワークフローを使用して正常にデータ インポートをサブミットできることを確認するには、以下の前提条件を満たしていることを確認します。

1. CA APM ユーザ インターフェースですべてのマッピングおよび設定を含むデータ インポートを定義します。
2. データ ファイル パス（パスを指定している場合）がインポート サービスが実行されているサーバからアクセス可能であることを確認します。 また、ネットワーク サービス（アプリケーション プール アイデンティティ）ユーザは、このパスへのアクセスが必要です。
3. ワークフロー プロバイダ（CA Process Automation など）を使用してプロセス ワークフローを定義します。

ワークフロー呼び出しの指定

Data Importer を起動し、プロセス ワークフローからデータ インポートを実行するには、CA APM Web サービス操作に特定のワークフロー呼び出しを指定します。これらの操作では以下の機能を実行します。

- ログイン操作 - CA APM へのログイン。

- 以下のいずれかのデータ ファイル提供方法を使用したデータ インポートのサブミット。
  - SubmitImportwithfilepath 操作 - データ ファイルは指定されたファイル パスにあります。 このファイル パスは、インポート サービスが実行されているサーバからアクセス可能である必要があります。 Web サービス操作によってファイルがアップロードされます。
  - SubmitImport 操作 - データ ファイル コンテンツはバイナリのバイト配列形式に変換されています。 Web サービス操作は、アプリケーションからバイト配列コンテンツを受信し、Data Importer にコンテンツをサブミットします。

    注: このデータ ファイル提供方法を使用するには、アプリケーションを作成し（利用できるアプリケーションがない場合）、データ ファイル コンテンツをバイト配列形式に変換します。 その後、アプリケーションはコンテンツを Web サービス操作に送信します。

ビジネス プロセス ワークフローにこれらの操作の呼び出しを組み込みます。

注: プロセス ワークフローの作成については、ワークフロー プロバイダの製品ドキュメントを参照してください。

ログイン操作

この操作では、指定された CA APM ユーザ ID およびパスワードを使用して CA APM にログインします。 この操作の出力はログイン トークンです。 ログイン トークンは、その他のデータ インポート ワークフロー操作への入力として使用されます。

入力パラメータ

ItamUserName – CA APM ユーザ ID

ItamUserPassword – CA APM ユーザ パスワード

出力パラメータ

loginToken – CA APM ログインの後に返されるトークン

SubmitImport 操作

この操作は、バイト配列形式に変換されたデータ ファイル コンテンツを受信し、データ インポートを持つコンテンツを Data Importer にサブミットします。 この操作を使用するには、アプリケーションを作成し（利用できるアプリケーションがない場合）、データ ファイル コンテンツをバイト配列フォーマットに変換します。 その後、アプリケーションはコンテンツをこの Web サービス操作に送信します。

この操作はデータ インポート ジョブ ID を返します。これはインポート ジョブのステータスを確認するために使用されます。

入力パラメータ

loginToken – CA APM ログインの後に返されるトークン。

ImportName – データ インポートの名前。

Datafilename – データ インポートに関連付けられているデータ ファイルの名前。

Datafilestream – バイト配列形式のデータ ファイル コンテンツ。

Caprovided – （オプション）製品提供のデータ インポートを指定するインジケータ。 製品提供のインポートを指定するには、このパラメータを 1 に設定します。

Tenant – （マルチテナントのみ）インポートが適用されるテナントの名前。

出力パラメータ

Job ID – データ インポートが正常にサブミットされた後に返される ID。GetJobStatus 操作は、この ID を使用してインポート ジョブのステータスを確認します。

SubmitImportwithfilepath 操作

この操作は指定されたファイル パスからデータ ファイルをアップロードし、データ インポートを持つデータ ファイルを Data Importer にサブミットします。 このファイル パスは、インポート サービスが実行されているサーバからアクセス可能である必要があります。

この操作はデータ インポート ジョブ ID を返します。これはインポート ジョブのステータスを確認するために使用されます。

入力パラメータ

loginToken – CA APM ログインの後に返されるトークン。

ImportName – データ インポートの名前。

Datafilepath – データ インポートに関連付けられたデータ ファイルの完全パスおよび名前。このパスは、インポート サービスが実行されているサーバからアクセス可能である必要があります。 また、ネットワーク サービス（アプリケーション プール アイデンティティ）ユーザは、このパスへのアクセスが必要です。

注: データ ファイル ロケーションが共有パスである場合、CA APM サーバと共有コンピュータは同じドメインにある必要があります。

Caprovided – （オプション）製品提供のデータ インポートを指定するインジケータ。 製品提供のインポートを指定するには、このパラメータを 1 に設定します。

Tenant – （マルチテナントのみ）インポートが適用されるテナントの名前。

出力パラメータ

Job ID – データ インポートが正常にサブミットされた後に返される ID。GetJobStatus 操作は、この ID を使用してインポート ジョブのステータスを確認します。

インポート ジョブのステータスの確認

Data Importer は、サブミットされた各データ インポート ジョブのステータス サマリを提供します。 プロセス ワークフローには、サブミットされたデータ インポート ジョブのステータスを取得する CA APM Web サービス操作の呼び出しを含めることができます。プロセス ワークフローにこの操作の呼び出しを組み込みます。

GetJobStatus 操作

この操作はデータ インポート ジョブ ID を使用してインポート ジョブのステータスを確認します。

入力パラメータ

loginToken – CA APM ログインの後に返されるトークン。

Job ID – データ インポートが正常にサブミットされた後に返される ID。

出力パラメータ

Job Status – インポート ジョブのステータス

エラー メッセージへの応答

エラーがデータ インポート ワークフロー プロセス中に発生した場合、エラー メッセージを受信できます。 以下のメッセージについて説明します。

20002 - ユーザ権限のためにデータ インポートにアクセスできません。管理者に問い合わせてください。

ユーザ役割には、データ インポートをサブミットするための Data Importer 管理者アクセスまたは Data Importer ユーザ アクセスが必要です。

20005 - インポート サービスに接続できません。管理者に問い合わせてください。

ImportProcessor.config ファイル内のインポート サービス URL を確認するか、管理者に問い合わせてください。

21002 - データ インポート名が無効です。

データ インポートが存在しないか、ユーザがデータ インポートにアクセスできません。データ インポートが製品提供されている場合は、CA から提供されたパラメータの値に 1 を指定します。

21004 - データ ファイルのアップロードに失敗しました。

このメッセージは、設定エラーによって発生する場合があります。 ストレージ マネージャ サービスのログ ファイルを確認します。

21005 - データ インポートのマッピングが定義されていません。

マッピングを定義し、データ インポートを再サブミットします。

22001 - データ インポート ジョブ ID が無効です。ジョブ ID を確認し、再度インポートを実行します。

CA APM にログインしてデータ インポート ジョブを見つけることにより、ジョブ ID を確認します。 有効なジョブ ID を持ったデータ インポートを再サブミットします。

用語集

アイテム

「*モデル*」を参照してください。

アセット

アセットは、所有しているか、取得を予定している IT 製品です。アセットは、シリアル番号、構成、連絡先などの一意の識別子を持つ物理的な製品を表します。個別に追跡する必要がある各アセットに対して、アセット レコードを定義します。

アセット グループ

アセット グループは、情報を共有するアセットを関連付けるためのセットです。グループの個々のメンバではなく、グループの情報が追跡されます。

アセット構成

アセット構成は、ユーザの環境内に現在存在するハードウェア アセットの構成を説明するレコードです。アセット構成は時間が経つにつれて変更されるため、モデル構成とは異なります。

アセット ファミリ

*アセット ファミリ*は、ユーザの組織で使用される製品、サービス、または装置に特化した情報を追跡するために、アセットを整理および分類する方法です。 アセット ファミリによって、アセットを定義するときにページに表示される情報が決まります。 アセット ファミリは、以前はアセット タイプという名前でした。

一致する値

一致する値は、一意にデータベース内のエンティティを識別するキー フィールドです。 ハードウェア アセットの場合、一致する値はドメイン ID、ユニット ID、およびタイプの組み合わせになります。これにより、ユニット テーブル内の行を一意に識別します。

イベント サーバ

イベント サーバは、イベントを処理する製品コンポーネントです。サーバは定期的にリポジトリ内のイベント テーブルをスキャンし、イベントが発生したときにイベントを始動します。イベントを始動した後、ワークフロー プロバイダはユーザに通知を送信し、確認応答を管理します。ワークフロー プロセスの完了、進行中、失敗、中断を管理者が判断できるように、サーバはリポジトリの情報を更新します。

エスカレーション

エスカレーションは、元の受信者が指定された期間内に応答しなかった場合、別の宛先に自動的に通知を転送するプロセスです。

エスカレーションの上限

エスカレーションの上限は、繰り返し発生するコストによって増加する可能性がある金額の上限です。 通常、契約によって制限が指定されます。

エスカレーションの割合

エスカレーションの割合は、繰り返しが続く期間ごとに予想される、アセットまたはリーガル ドキュメントに関連して繰り返し発生するコストの増加割合です。たとえば、3 年間、1 年に 1 回 100 ドルの料金が継続的に発生するとします。 インフレに対応するため、ベンダーは毎年製品コストを 5% 上げると予想されます。製品のコストは、1 年目に 100 ドル、2 年目に 105 ドル（100 ドル + （0.05 x 100 ドル） = 105 ドル）、3 年目に 110.25 ドル（105 ドル + （0.05 x 105 ドル） = 110.25 ドル）になります。

エスカレーションの割合は、繰り返しが続く期間に基づきます。 月払いでも支払い予定額は年単位で上がるため、エスカレーションの割合を考慮した年払いのコストとしてコストを入力できます。 年払いの場合は契約終了日まで、毎年料金を計算する際にエスカレーションの割合に応じて料金が上がります。

オブジェクト

オブジェクトは、リポジトリ内で記録および追跡する対象を表します。CA APM 内の主なオブジェクトは、モデル、アセット、リーガル ドキュメント、連絡先、会社、組織、ロケーション、およびサイトです。

親会社

親会社は別の会社（その子会社）を所有または管理する会社です。

会社

会社は、リポジトリで追跡される製品を製造、販売、または購入する組織か、リポジトリで追跡されるリーガル ドキュメントに関係する組織です。

開始リクエスト フォーム

*開始リクエスト フォーム*は、CA Process Automation オートメーション オブジェクトの 1 つで、ユーザは新規ワークフロー プロセスの開始をリクエストできます。開始リクエスト フォームを使用して、ユーザに構造化された入力とプロセスの起動を提供するインターフェースを作成できます。

拡張フィールド

拡張フィールドは、任意のオブジェクト レコードに追加できるフィールドです。拡張フィールドは、追跡する必要があるがデフォルト フィールドに存在しないオブジェクト情報を保存するために使用できます。

関係

関係は、管理対象オブジェクトと別のオブジェクトとの関連付けです。 関係レコードは、関連付けに関する詳細情報を提供します。

関係テンプレート

関係テンプレートは、特定のカテゴリの関係に属する属性のセットです。 これらの属性により、相互にリンクできるオブジェクトのタイプや、それらのリンクの性質が決まります。

関係レコード

*関係レコード*は、プライマリ オブジェクトが 1 つ以上のセカンダリ オブジェクトにリンクされるときに作成されます。

監査履歴

監査履歴は、一定期間におけるオブジェクト レコードに対する変更の時系列のリストです。

監視イベント

*監視イベント*は、オブジェクトのフィールドの変更をモニタし、ワークフロー プロバイダ（たとえば CA Process Automation）が作成する通知と連携して、タスクを実行する場合の潜在的な障害をユーザに通知します。

関連テナント グループ

*関連テナント グループ*は、*サブテナント グループ*または*スーパーテナント グループ*に属する 1 つまたはすべてのテナントを含むテナント グループです。

規程リーガル ドキュメント

*規程リーガル ドキュメント*は、リーガル ドキュメントが基礎とするドキュメントです。 規程リーガル ドキュメントには、リーガル ドキュメントから作成される主な契約条件のセットが含まれています。

クラス

クラスは、モデルまたはアセットに割り当てられて情報検索を促進する、アセット ファミリの広範な記述カテゴリです。

繰り返し発生するコスト

*繰り返し発生するコスト*とは、特定の期間に繰り返されるコストです。 繰り返しが続く期間は、ユーザの契約条件に基づきます。 繰り返しが続く期間の長さと支払いの頻度を混同しないでください。 たとえば、コストが 3 年間毎年発生する場合、月単位で支払いをする場合でも、繰り返し発生するコストに対して 3 年を指定します。 支払い頻度は後で変更できます。

契約条件

契約条件は、リーガル ドキュメントの契約の部分を指します。 リーガル テンプレートを定義する前に、すべての契約条件を含むマスタ リストを 1 つ作成し、リーガル テンプレートに割り当てられるようにします。契約条件は、複数のリーガル テンプレートおよびリーガル ドキュメントに割り当てることができます。

構成

構成には、CA APM 固有の定義が 2 つあります。 1 つは、コンピュータ（PC、ラップトップ、サーバなど）およびコンピュータの個々のコンポーネント（モニタ、モデムなど）を表すものである場合があります。 構成レコードを使用して、コンピュータのコンポーネントを表すモデルおよびアセットを識別します。 もう 1 つは、ユーザが情報を簡単に入力、管理、検索できるように、製品のユーザ インターフェースおよびデフォルトの動作を変更する手段を表す場合もあります。

構成関係

構成関係は、ハードウェア構成の特定のカテゴリに属する属性のセットです。 構成関係は、アセットとモデルに対して指定されます。

子会社

子会社は、別の会社（その親会社）によって所有または管理される会社です。

サービス プロバイダ

*サービス プロバイダ*は、製品インスタンスのマスタ テナント（所有者）です。製品インスタンスは 1 つのサービス プロバイダのみを持つことができます。サービス プロバイダは、1 つ以上のテナント階層に親として参加することもできます。

サブクラス

サブクラスは、クラスで提供される説明をさらに細分化するための、モデルまたはアセットに割り当てられるクラスの記述カテゴリです。

サブテナント

*サブテナント*とは、同じテナント階層で別のテナントよりも（*スーパーテナント*から相対的に）下位にあるテナントです。 サブテナントはそのスーパーテナント内の部門またはサイトになることができます。 サブテナントは独自のビジネス ルールとデータを持つことができます。また、一部のビジネス データを親テナントやさらに上位のスーパーテナントと共有します。

サブテナント グループ

*サブテナント グループ*は、テナントとそのサブテナント、さらにサブテナントのサブテナントなど、階層の一番下までのテナントを含むテナント グループです。テナントが階層に存在する限り、そのサブテナント グループは製品によって保持され、その名前と説明のみを変更できます。

支払いスケジュール

支払いスケジュールは、特定のコスト レコードに対する支払いのリストです。支払いスケジュールの情報には、支払い期限、支払い予定額、支払いが実行または承認されたかどうか、およびその金額などが含まれます。 ［コスト］ページに提供する情報は、支払スケジュールを計算するために使用されます。 繰り返し期間の詳細を定義する場合、システムは定義する繰り返し期間の詳細に基づいてデータベース内に支払いレコードを自動作成します。

親テナント

テナントを階層に配置するには、そのテナントに*親テナント*に割り当てます。親テナントになるのは、階層でそのテナントのすぐ上にあるテナントです。階層からテナントを削除するには、その親テナントの割り当てを削除します。

スーパーテナント

*スーパーテナント*は、同じテナント階層で別のテナントよりも（*サブテナント*から相対的に）上位にあるテナントです。

スーパーテナント グループ

*スーパーテナント グループ*は、テナントとその親テナントなど、階層の一番上までのテナント グループです。テナントが階層に存在する限り、そのスーパーテナント グループは製品によって保持され、その名前と説明のみを変更できます。

正規化

*正規化*は照合処理の一部です。CA APM と検出済みのリポジトリ間のデータを標準化、整理、および統合するためのルールのリストを作成します。

通知

通知はワークフロー プロバイダ（CA Process Automation など）によって作成され、重要なイベントおよびアクティビティについてチーム メンバに情報を伝えます。

テナント

*テナント*とは、1 つの製品インストールにある複数のインスタンスの中の 1 つのインスタンスです。 テナントを使用すると、CA APM は、顧客にサポートをする複数の個別の企業を管理できます。テナントが *サービス プロバイダ*の認証または*テナント階層*を使用してデータを共有する場合を除き、各テナントには一意の設定およびプロパティがあり、製品を自分のアプリケーションとして参照します。

テナント階層

*テナント階層*は、ユーザがテナントを定義する（つまり、組織的な目的またはデータ共有の目的でテナントに親テナントを割り当てる）ときに定義および管理するテナント グループです。 CA APM は、テナント階層を無制限の深さまでサポートしています。ただし、サービス プロバイダで階層のテナントの総数や深さを制限できます。また、サービス プロバイダは、個々のテナントがサブテナントを持たないようにすることもできます。

添付ファイル

添付ファイルは、オブジェクトの解説ドキュメントが含まれる電子ファイルまたは URL ページです。たとえば契約内容を表すため、スキャンした契約書とリーガル ドキュメントを添付できます。

テンプレート

*テンプレート*は、特定のオブジェクト タイプに関連付けられた、事前定義済みのフィールド グループを提供します。 たとえば、リーガル テンプレートは、特定のタイプのリーガル ドキュメントに属するフィールドを提供します。

特記事項

特記事項は、より多くの詳細情報を追加するためにオブジェクト レコードに追加されるテキストです。

トリミング

*トリミング*とは、ハードウェア照合を実行するときに、アセットで無視する先頭または末尾の文字の定数を指定する方法です。 たとえば、あるサイトで検出されたコンピュータ名には、プレフィックスとして 3 文字のロケーション コードがあるとします。 この場合、検出されたコンピュータ名の左から 3 文字をトリミングするトリミング レコードをアセット一致基準に対して作成します。

配置

*配置*は、組織が特定のソフトウェア製品の使用を内部的に承認する方法を表し、ソフトウェア ライセンスに指定されます。 配置の例として、エンタープライズ、単一ユーザ、単一サーバなどがあります。

配置関係

*配置関係*は、ソフトウェアの内部配置の属性を提供するレコードです。 各配置関係は、特定の配置タイプに適用される属性および関係を提供します。

日付イベント

日付イベントは、オブジェクトの日付フィールドの変更をモニタし、ワークフロー プロバイダ（CA Process Automation など）によって作成される通知と連携して、重要な日付が近いまたは経過したことを管理者に通知します。

変更イベント

変更イベントは、オブジェクトのフィールド変更をモニタし、ワークフロー プロバイダ（CA Process Automation など）によって作成される通知と連携して、管理者にフィールド値の変更を通知します。

マスキング

マスキングは、文字列の一部の代わりに 1 文字を使用して検索条件を指定する方法です。マスキング文字は、*ワイルドカード文字*とも呼ばれます。 検索で返されるレコード数を制限する場合や、正確なスペルが不明な検索対象の文字の代わりとして、マスキングを使用します。

マルチテナント

*マルチテナント*では、複数の独立したテナント（およびそのユーザ）が 1 つの製品インスタンス（たとえば CA APM）の実装を共有できます。 マルチテナントでは、テナントがハードウェアとアプリケーションのサポート リソースを共有し、独立した実装の利点の大部分を活かしながらコストを下げることができます。テナントは、定義済みの方法だけで互いに対話することができます。それ以外では、各テナントは自分が使用するためだけにアプリケーション インスタンスを表示します。

モデル

モデルは、過去に購入した製品または今後購入する可能性がある製品を説明するレコードです。 モデルは、以前はアイテムという名前でした。

モデル構成

モデル構成は、購入した特定のハードウェア モデルの標準構成を説明するレコードです。

役割

セキュリティに使用される役割は、同じタスクを実行し、同じレベルのデータまたは機能へのアクセス権を必要とするユーザのグループです。

優先ベンダー/優先販売会社

優先ベンダー/優先販売会社は、将来の製品の取得で優先される販売会社です。

リーガル テンプレート

リーガル テンプレートは、特定のカテゴリのリーガル ドキュメントに属する属性のセットです（たとえば、すべてのリースには開始日、終了日、賃貸人、および賃借人が含まれます）。 これらの属性には一般に、そのカテゴリとユーザ フィールドに適用される契約条件が含まれます。

リーガル ドキュメント

リーガル ドキュメントは、複数の当事者間の法的関係または契約について説明するドキュメントです。 たとえば、契約書、通知書、基本契約書、リース、大量購入契約書、同意書などはすべてリーガル ドキュメントと見なされます。 ソフトウェア ライセンスはリーガル ドキュメントですが、これは別途追跡されます。

リマインダ

*リマインダ*は、重要なイベントまたはアクティビティについてユーザに警告するイベントによってトリガされる通知です。

連絡先

連絡先は、リポジトリ内のオブジェクトの取得、使用、または管理に関係する人物または部門です。

ロケーション

ロケーションは、アセット、会社、または連絡先が存在する物理的な場所です。

ワークフロー プロバイダ

*ワークフロー プロバイダ*は、イベントの通知および承認を管理します。