



Informatica® Cloud Data Integration  
October 2022

# 基本操作

本ソフトウェアおよびマニュアルは、使用および開示の制限を定めた個別の使用許諾契約のもとでのみ提供されています。本マニュアルのいかなる部分も、いかなる手段（電子的複製、写真複製、録音など）によっても、Informatica LLC の事前の承諾なしに複製または転載することは禁じられています。

米政府の権利プログラム、ソフトウェア、データベース、および関連文書や技術データは、米国政府の顧客に配信され、「商用コンピュータソフトウェア」または「商業技術データ」は、該当する連邦政府の取得規制と代理店固有の補足規定に基づきます。このように、使用、複製、開示、変更、および適応は、適用される政府の契約に規定されている制限およびライセンス条項に従うものとし、政府契約の条項によって適当な範囲において、FAR 52.227-19、商用コンピュータソフトウェアライセンスの追加権利を規定します。

Informatica、Informatica Cloud、Informatica Intelligent Cloud Services、PowerCenter、PowerExchange、および Informatica ロゴは、米国およびその他の国における Informatica LLC の商標または登録商標です。Informatica の商標の最新リストは、Web (<https://www.informatica.com/trademarks.html>) にあります。その他の企業名および製品名は、それぞれの企業の商標または登録商標です。

本ソフトウェアまたはドキュメンテーション（あるいはその両方）の一部は、第三者が保有する著作権の対象となります。必要な第三者の通知は、製品に含まれています。

本マニュアルの情報は、予告なしに変更されることがあります。このドキュメントで問題が見つかった場合は、[infa\\_documentation@informatica.com](mailto:infa_documentation@informatica.com) までご報告ください。

Informatica 製品は、それらが提供される契約の条件に従って保証されます。Informatica は、商品性、特定目的への適合性、非侵害性の保証等を含めて、明示的または黙示的ないかなる種類の保証をせず、本マニュアルの情報を「現状のまま」提供するものとします。

# 目次

<b>序文</b> .....	5
Informatica のリソース.....	5
Informatica マニュアル.....	5
Informatica Intelligent Cloud Services Web サイト.....	5
Informatica Intelligent Cloud Services コミュニティ.....	5
Informatica Intelligent Cloud Services マーケットプレイス.....	6
データ統合コネクタのドキュメント.....	6
Informatica ナレッジベース.....	6
Informatica Intelligent Cloud Services Trust Center.....	6
Informatica グローバルカスタマサポート.....	6
 <b>第 1 章 : Informatica Cloud データ統合の基本操作</b> .....	7
 <b>第 2 章 : システム要件</b> .....	9
Internet Explorer 11 での CORS の有効化.....	9
 <b>第 3 章 : Secure Agent のインストール</b> .....	14
Windows での Secure Agent のインストール.....	14
Windows での Secure Agent の要件.....	14
Windows での Secure Agent のダウンロードおよびインストール.....	15
Windows でのプロキシ設定.....	17
Windows Secure Agent サービスへのログインの設定.....	17
Linux での Secure Agent のインストール.....	18
Linux での Secure Agent の要件.....	18
Linux での Secure Agent のダウンロードおよびインストール.....	19
Linux でのプロキシ設定.....	20
 <b>第 4 章 : 接続設定</b> .....	22
接続の設定.....	22
オブジェクト検索と選択.....	23
 <b>第 5 章 : プロジェクトの設定</b> .....	25
プロジェクトとプロジェクトフォルダの作成.....	25
アセットの作成.....	26
 <b>第 6 章 : ソース管理の有効化</b> .....	27
リポジトリアクセスの設定.....	27
 <b>第 7 章 : ユーザープロファイルの編集</b> .....	28

第 8 章 : 別の組織への切り替え.....	29
索引.....	30

# 序文

Informatica Cloud® Data Integration の使用を開始する方法については、「基本操作」を参照してください。「基本操作」では、ランタイム環境を構成し、Data Integration をシステムに接続してプロジェクトを開始する方法を説明します。

## Informatica のリソース

Informatica は、Informatica Network やその他のオンラインポータルを通じてさまざまな製品リソースを提供しています。リソースを使用して Informatica 製品とソリューションを最大限に活用し、その他の Informatica ユーザーや各分野の専門家から知見を得ることができます。

### Informatica マニュアル

Informatica マニュアルポータルでは、最新および最近の製品リリースに関するドキュメントの膨大なライブラリを参照できます。マニュアルポータルを利用するには、<https://docs.informatica.com> にアクセスしてください。

製品マニュアルに関する質問、コメント、ご意見については、Informatica マニュアルチーム ([infa\\_documentation@informatica.com](mailto:infa_documentation@informatica.com)) までご連絡ください。

### Informatica Intelligent Cloud Services Web サイト

Informatica Intelligent Cloud Services Web サイト (<http://www.informatica.com/cloud>) にアクセスできます。このサイトには、Informatica Cloud 統合サービスに関する情報が含まれます。

### Informatica Intelligent Cloud Services コミュニティ

Informatica Intelligent Cloud Services コミュニティを使用して、技術的な問題について議論し、解決します。また、技術的なヒント、マニュアルの更新情報、FAQ（よくある質問）への答えを得ることもできます。

次の Informatica Intelligent Cloud Services コミュニティにアクセスします。

<https://network.informatica.com/community/informatica-network/products/cloud-integration>

開発者は、次の Cloud 開発者コミュニティで詳細情報を確認したり、ヒントを共有したりできます。

<https://network.informatica.com/community/informatica-network/products/cloud-integration/cloud-developers>

## Informatica Intelligent Cloud Services マーケットプレイス

Informatica マーケットプレイスにアクセスすると、データ統合コネクタ、テンプレート、およびマップレットを試用したり購入したりできます。

<https://marketplace.informatica.com/>

## データ統合コネクタのドキュメント

データ統合コネクタのドキュメントには、マニュアルポータルからアクセスできます。マニュアルポータルを利用するには、<https://docs.informatica.com> にアクセスしてください。

## Informatica ナレッジベース

Informatica ナレッジベースを使用して、ハウツー記事、ベストプラクティス、よくある質問に対する回答など、製品リソースを見つけることができます。

ナレッジベースを検索するには、<https://search.informatica.com> にアクセスしてください。ナレッジベースに関する質問、コメント、ご意見の連絡先は、Informatica ナレッジベースチーム ([KB\\_Feedback@informatica.com](mailto:KB_Feedback@informatica.com)) です。

## Informatica Intelligent Cloud Services Trust Center

Informatica Intelligent Cloud Services Trust Center は、Informatica のセキュリティポリシーおよびリアルタイムでのシステムの可用性について情報を提供します。

Trust Center (<https://www.informatica.com/trust-center.html>) にアクセスします。

Informatica Intelligent Cloud Services Trust Center にサブスクライブして、アップグレード、メンテナンス、およびインシデントの通知を受信します。[Informatica Intelligent Cloud Services Status](#) ページには、すべての Informatica Cloud 製品の実稼働ステータスが表示されます。メンテナンスの更新はすべてこのページに送信され、停止中は最新の情報が表示されます。更新と停止の通知がされるようにするには、Informatica Intelligent Cloud Services の 1 つのコンポーネントまたはすべてのコンポーネントについて更新の受信をサブスクライブします。すべてのコンポーネントにサブスクライブするのが、更新を逃さないようにするための最良の方法です。

登録するには、<https://status.informatica.com/> に移動し、**[更新を購読登録]** をクリックします。その後、電子メール、SMS テキストメッセージ、Webhook、RSS フィードとして、またはこの 4 つを任意に組み合わせて送信された通知を受信することを選択ができます。

## Informatica グローバルカスタマサポート

電話またはオンラインでカスタマサポートセンターに連絡できます。

オンラインサポートについては、Informatica Intelligent Cloud Services の **[サポート要求の送信]** をクリックしてください。またオンラインサポートを使用して問題を記録することもできます。オンラインサポートを利用するには、ログインが必要です。<https://network.informatica.com/welcome> でログイン要求できます。

Informatica グローバルカスタマサポートの電話番号は、Informatica の Web サイト <https://www.informatica.com/services-and-training/support-services/contact-us.html> に掲載されています。

# 第 1 章

## Informatica Cloud データ統合の基本操作

データ統合プロジェクトは、わずかな手順で作成できます。

### 手順 1. システム要件の確認

Informatica Intelligent Cloud Services プロジェクトの設計時に互換性のあるブラウザを使用していることを確認し、データ統合がサポートするオペレーティングシステム、データベース、およびその他のシステムについて、Informatica Intelligent Cloud Services の製品可用性マトリックスを確認してください。

### 手順 2. ランタイム環境の設定

ランタイム環境は、タスクを実行するための実行プラットフォームです。ランタイム環境は、1 つ以上の Secure Agent で構成されます。Secure Agent は、タスクを実行し、組織と Informatica Intelligent Cloud Services 間でのファイアウォールを越えた安全な通信を可能にする軽量プログラムです。組織内のユーザーがタスクを実行できるように、各組織に少なくとも 1 つのランタイム環境が必要です。

以下のタイプのランタイム環境を作成できます。

#### Informatica Cloud Hosted Agent

SaaS 環境でデータにアクセスする場合は、Informatica Cloud Hosted Agent を使用できます。Hosted Agent は、Informatica Intelligent Cloud Services ホスティング機能内で実行されるため、インストールするものではありません。

Hosted Agent は、特定のコネクタを使用する同期タスク、マッピングタスク、およびレプリケーションタスクを実行できます。使用するコネクタが Hosted Agent をサポートしているかどうかを確認するには、関連するコネクタのヘルプを参照してください。

#### Secure Agent グループ

オンプレミスのデータにアクセスする必要がある場合や、Hosted Agent を使用せずに SaaS データにアクセスする場合は、Secure Agent グループを使用します。Secure Agent グループには、1 つ以上の Secure Agent が含まれます。グループ内のエージェントは、ネットワーク内、または Amazon Web サービスや Microsoft Azure などのクラウドコンピューティングサービス環境で実行します。

Secure Agent グループを作成するには、Secure Agent をダウンロードしてインストールします。1 つの Secure Agent を各物理マシンまたは仮想マシンにインストールできます。インストールする各エージェントは、デフォルトで独自のグループに追加されます。複数のエージェントをグループに追加してワークロードのバランスを調整し、スケーラビリティを向上させることができます。

Secure Agent を詳細クラスタに関連付けることができます。詳細クラスタとは、クラウド上で分散処理環境を提供する Kubernetes クラスタです。フルマネージド型のセルフサービスクラスタはスケーラブルなアーキテクチャを使用してデータロジックを実行できます。一方、ローカルクラスタは単一ノードを使用して、高度なユースケースのプロジェクトをすばやくオンボードします。

## サーバーレスランタイム環境

サーバーレスランタイム環境は、Secure Agent や Secure Agent グループのダウンロード、インストール、設定、管理が必要ない高度なサーバーレスデプロイメントソリューションです。

Hosted Agent のマルチテナントモデルと比較して、サーバーレスランタイム環境は、タスクを実行するための仮想マシンリソースを専用サーバーに提供する分離されたシングルテナントモデルを使用します。サーバーレスランタイム環境は、負荷の規模に合わせて自動スケールしますが、データはクラウド環境内に残ります。

### 手順 3。接続の作成

データ統合を使用してデータ統合タスクを実行する前に、接続を作成する必要があります。接続を設定するときは、データ統合とソースオブジェクトとターゲットオブジェクトとの間でのデータ交換を可能にするコネクタを指定します。例えば、Salesforce データを使用するタスクを作成する場合は、Salesforce 接続を作成します。Salesforce 接続は Salesforce コネクタを使用して、Salesforce とデータ統合との間のデータ交換を可能にします。

### 手順 4。プロジェクトの作成

マッピング、タスク、タスクフローなどのアセットを含むフォルダ内のデータ統合プロジェクトを整理します。プロジェクトフォルダと、プロジェクトに必要なアセットを含むフォルダを作成します。

フォルダを設定したら、プロジェクトアセットを作成します。アセットには次のオブジェクトが含まれます。

- マッピング
- タスク
- タスクフロー
- ビジネスサービス、マップレット、および階層スキーマなどのコンポーネント

### 手順 5。ソース管理リポジトリへのプロジェクトの追加（オプション）

所属する組織がソース管理に対応しており、ソース管理リポジトリへの読み書きアクセス権を組織が持っている場合は、プロジェクトをリポジトリに追加できます。

プロジェクトを追加する前に、組織の管理者は、組織とソース管理リポジトリとの間のリンクを設定する必要があります。また、Informatica Intelligent Cloud Services でソース管理のユーザー資格情報を指定する必要があります。



## 第 2 章

# システム要件

システム要件の詳細については、Informatica Intelligent Cloud Services の製品可用性マトリックス (PAM) を参照してください。

PAM には、製品リリースでサポートされるブラウザ、オペレーティングシステム、データベースのバージョン、およびその他のデータソースやターゲットが記載されています。PAM は、Informatica Network (<https://network.informatica.com/community/informatica-network/product-availability-matrices/>) でご確認ください。

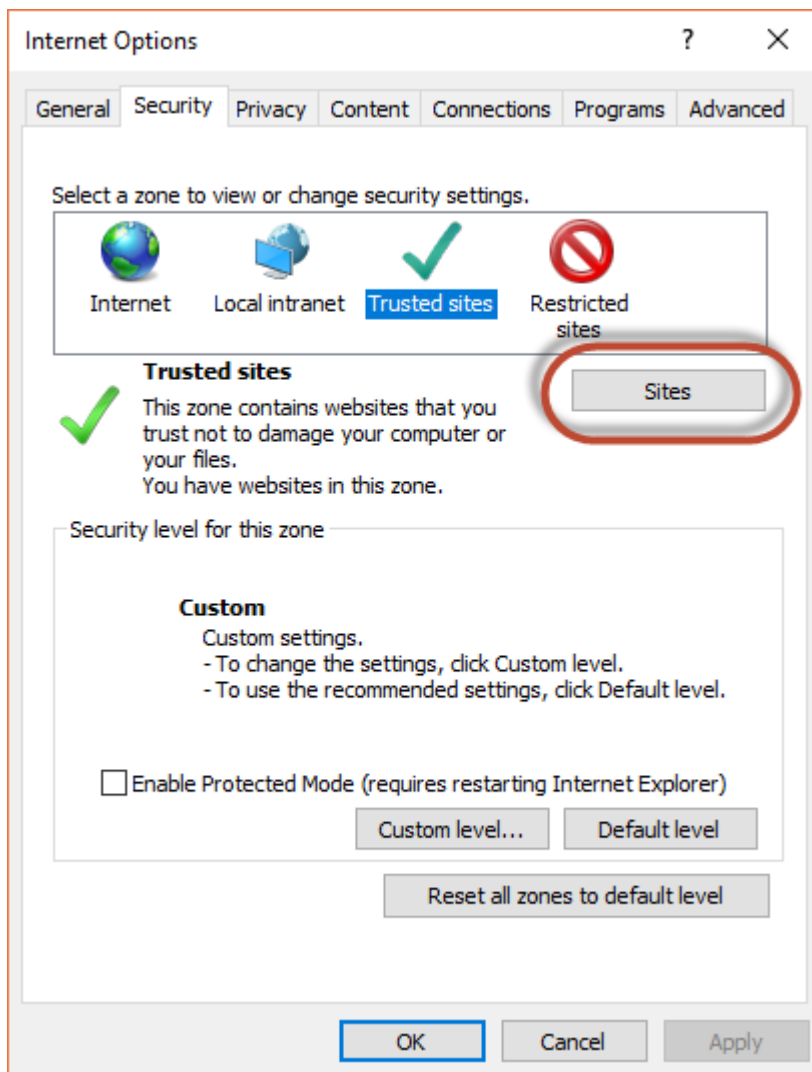
## Internet Explorer 11 での CORS の有効化

Informatica Intelligent Cloud Services では、Internet Explorer 11 でクロスオリジンサポート (CORS) を有効にする必要があります。Internet Explorer 11 のデフォルトでは、CORS は有効になっていません。

**注:** 一部の会社のセキュリティポリシーでは、Web ブラウザーで CORS を有効にすることが制限されています。これらの設定を更新する前に、会社または IT 部門に CORS 設定を変更してもよいか確認してください。

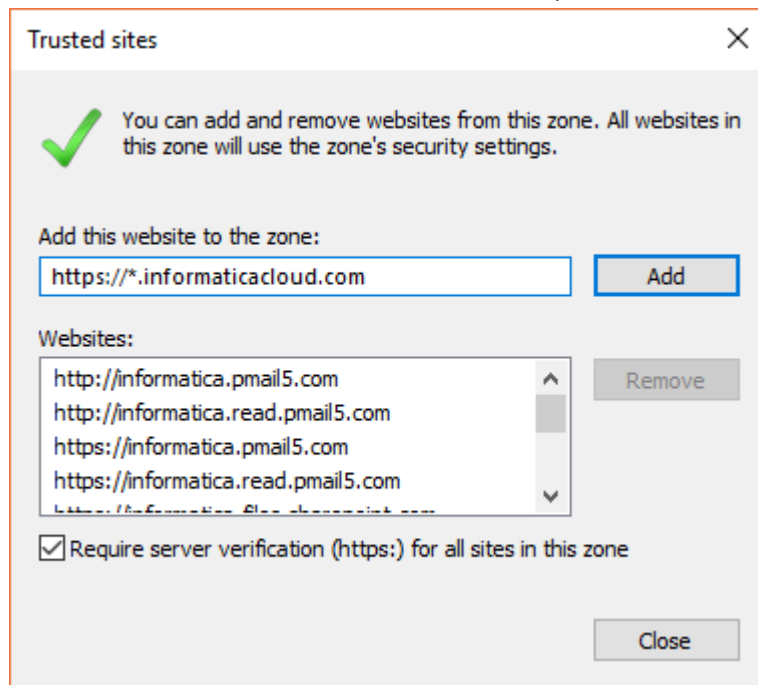
1. Internet Explorer 11 を開きます。
2. [ツール] メニューで、[インターネットオプション] を選択します。

3. 次の図に示すように、[セキュリティ] タブで [信頼済みサイト] をクリックし、[サイト] をクリックします。



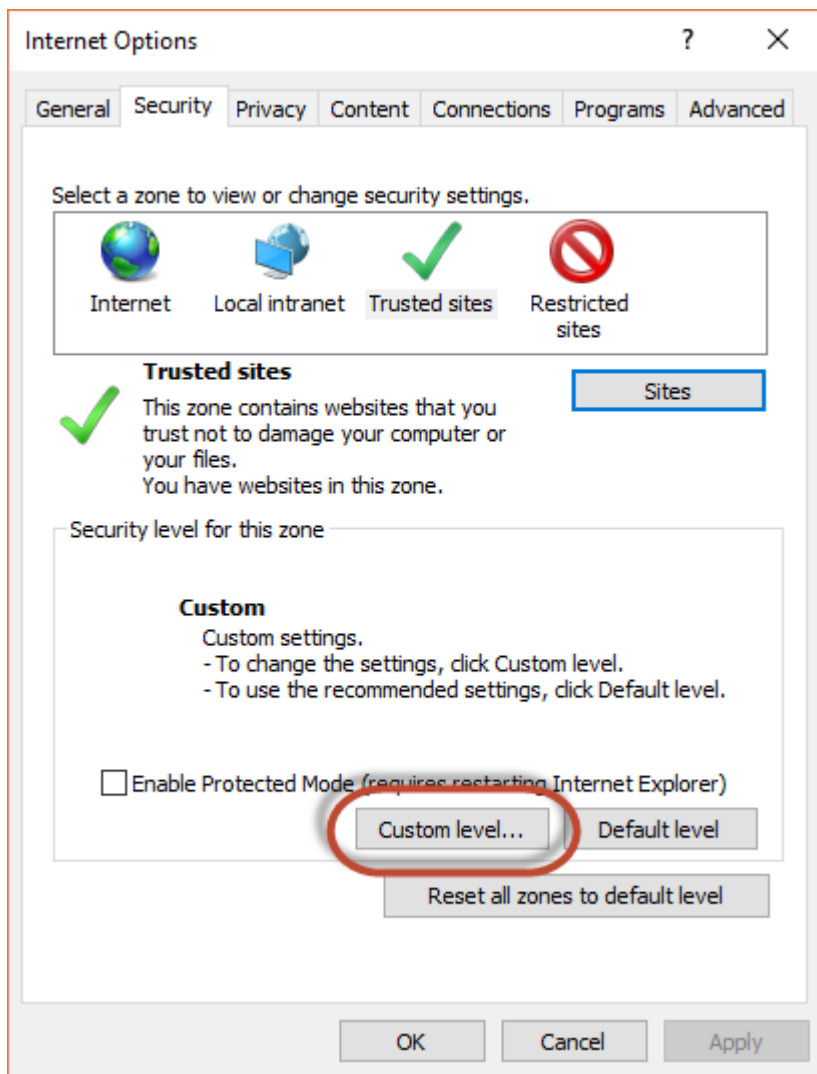
4. [信頼済みサイト] ダイアログボックスで、Informatica Intelligent Cloud Services ドメインをゾーンに追加し、[追加] をクリックします。

例えば、次の図は、ゾーンに追加されたドメイン `https://*.informaticacloud.com` を示しています。

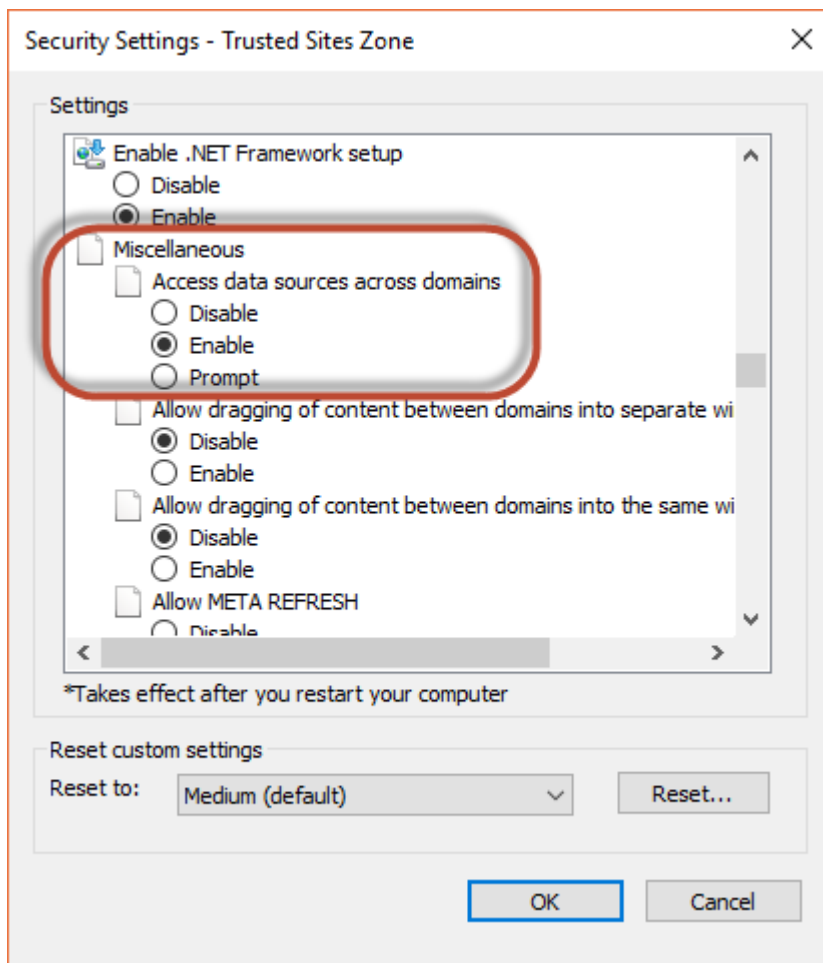


5. 【閉じる】をクリックします。

6. 次の図に示すように、[セキュリティ] タブの [このゾーンのセキュリティのレベル] 領域で、[レベルのカスタマイズ] をクリックします。



7. 次の図に示すように、[セキュリティ設定 - 信頼されたゾーン] ダイアログボックスで、[その他] の見出しが表示されるまで下にスクロールし、[ドメイン間でのデータソースのアクセス] を有効にします。



8. [OK] をクリックします。
9. メッセージが表示された場合は、ゾーンの設定を変更することを確認します。
10. [OK] をクリックします。
11. Internet Explorer を再起動し、Informatica Intelligent Cloud Services を開き直します。

## 第 3 章

# Secure Agent のインストール

Secure Agent は Windows または Linux にインストールできます。

## Windows での Secure Agent のインストール

Windows 上では、Secure Agent が Windows サービスとして実行されます。Secure Agent をインストールする際には、Informatica Cloud Secure Agent Manager もインストールします。

Secure Agent Manager または Windows サービスを使用して Secure Agent を停止および再起動できます。インストールプログラムの実行に使用するボリュームとは異なるボリュームに Secure Agent をインストールする場合は、Windows サービスから Secure Agent を起動および停止する必要があります。

また、Secure Agent Manager を使用して、Secure Agent のステータスをチェックし、プロキシ情報を設定することもできます。

Secure Agent Manager は、[スタート] メニューまたはデスクトップアイコンから起動できます。Secure Agent Manager を閉じると、最小化されて Windows タスクバーの通知領域に表示され、すぐにアクセスできるようにされます。

Secure Agent をインストールする際には、次のタスクを実行します。

1. Secure Agent をインストールするマシンが最小要件を満たしていることを確認します。
2. Secure Agent インストーラのファイルをダウンロードします。
3. Secure Agent をインストールして登録します。

## Windows での Secure Agent の要件

Secure Agent は、インターネット接続が可能であり、Informatica Intelligent Cloud Services にアクセス可能な任意のマシンにインストールすることができます。

Windows で Secure Agent をインストールする前に、次の要件を確認してください。

- Secure Agent をインストールするコンピュータがサポート対象のオペレーティングシステムを使用していることを確認します。Secure Agent でサポートされているオペレーティングシステムのリストについては、ナレッジベースの [Product Availability Matrix \(PAM\) for Informatica Intelligent Cloud Services](#) を参照してください。
- Secure Agent をインストールするマシンに 5 GB 以上の空きディスク容量があることを確認します。
- Secure Agent のインストールに使用するアカウントに、フラットのソースまたはターゲットファイルが格納されているすべてのリモートディレクトリに対するアクセス権が付与されていることを確認します。
- マシンに他の Secure Agent がインストールされていないことを確認します。マシンに別の Secure Agent がインストールされている場合は、まずそのエージェントをアンインストールする必要があります。

Secure Agent の要件の詳細については、Informatica グローバルカスタマサポートにお問い合わせください。

## ファイアウォールの設定

組織で保護ファイアウォールを使用している場合は、Informatica Intelligent Cloud Services のドメイン名または IP アドレス範囲を承認済みのドメイン名または IP アドレスの一覧に含めます。Secure Agent がファイアウォールを介して必要なすべてのタスクを実行できるようにするには、Secure Agent が使用するポートを有効にします。

Secure Agent はインターネットに接続するためにポート 443 (HTTPS) を使用します。トラフィックがポート 443 を通過することを許可するようにファイアウォールを設定してください。

ドメインと IP アドレスの許可リストはデータセンターに応じて異なり、これは POD (Point of Deployment) とも呼ばれます。POD は、Informatica Intelligent Cloud Services で任意のサービスを開いたときに表示される URL から特定できます。URL 文字列の最初の数文字が POD を表します。例えば、URL が `usw3.dm-us.informaticacloud.com` で始まる場合、POD は USW3 です。

Informatica Network の Informatica Intelligent Cloud Services Administrator [this Knowledge Base article](#) の **【ランタイム環境】** ページの上部にあるリンクをクリックすると、さまざまな POD の管理者ドメインと IP アドレスの許可リストを確認することができます。

## Windows での Secure Agent の権限

Secure Agent には、ソースとターゲットの間でデータを転送するために特定の権限が必要です。

Windows に Secure Agent をインストールする場合、その Secure Agent はローカル管理者グループの一部になっている必要があります。

## Windows の設定の実行

Windows で Secure Agent を使用する前に、プロキシ設定と Windows Secure Agent サービスログインを設定します。

プロキシ設定は、Secure Agent Manager で設定できます。Windows で Windows Secure Agent サービスのログインを設定します。

**注:** Informatica Cloud Data ウィザードで Secure Agent を使用する場合、Secure Agent に対してプロキシ設定または Windows サービスログインを設定する必要はありません。

## Windows での Secure Agent のダウンロードおよびインストール

Windows マシンに Secure Agent をインストールするには、Secure Agent インストールプログラムをダウンロードして実行してから、エージェントを登録する必要があります。

Secure Agent の登録にはインストールトークンが必要です。インストールトークンを取得するには、エージェントのダウンロード時にトークンをコピーするか、または管理者で **【インストールトークンの生成】** オプションを使用します。トークンは 24 時間後に有効期限が切れます。

Secure Agent をダウンロードしてインストールする前に、そのマシンに他の Secure Agent がインストールされていないことを確認します。他のエージェントが存在する場合は、アンインストールする必要があります。

**ヒント:** Secure Agent インストールプログラムのチェックサムを確認するには、エージェントの REST API バージョン 2 リソースを使用します。エージェントリソースの詳細は、『*REST API リファレンス*』を参照してください。

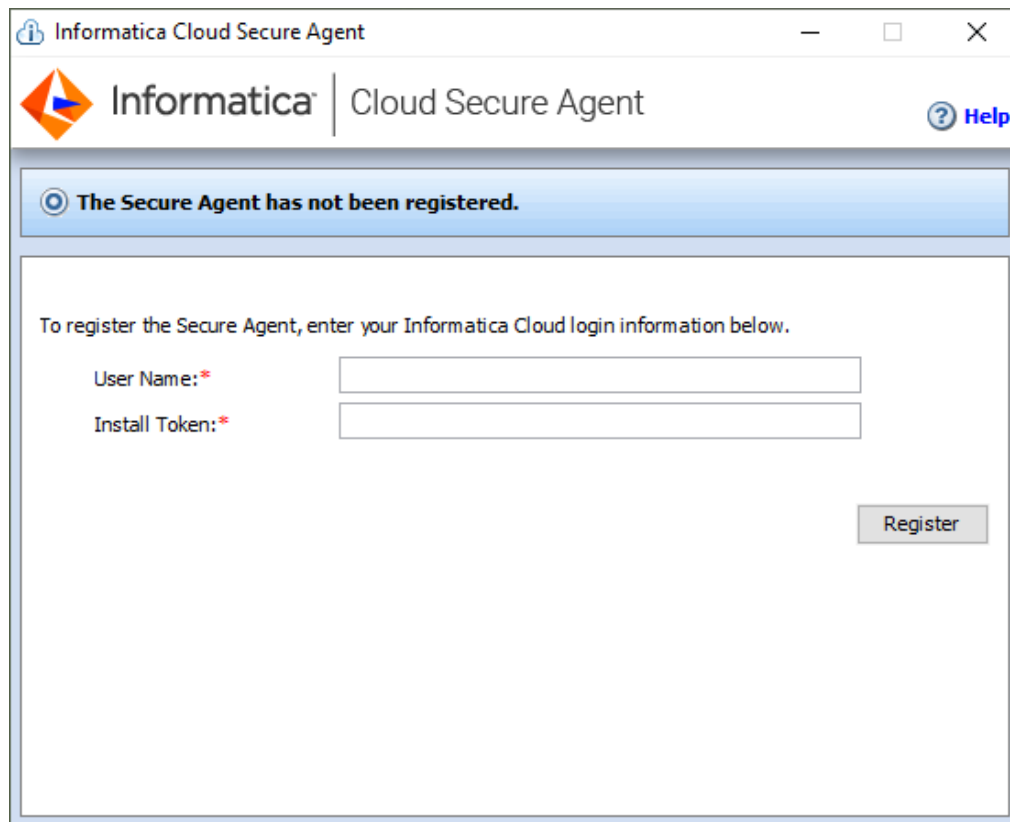
1. 管理者を開いて **【ランタイム環境】** を選択します。
2. **【ランタイム環境】** ページで、**【Secure Agent のダウンロード】** をクリックします。

3. Windows 64 ビットオペレーティングシステムプラットフォームを選択し、インストールトークンをコピーしてから **【ダウンロード】** をクリックします。

インストールプログラムがご使用のマシンにダウンロードされます。このインストールプログラムの名前は agent64\_install\_ng\_ext.<Agent Core バージョン>.exe です。

4. インストールプログラムの実行:
  - a. Secure Agent インストールディレクトリを指定し、**【次へ】** をクリックします。
  - b. **【インストール】** をクリックしてエージェントをインストールします。

Secure Agent Manager が開き、次の図に示すようにエージェントを登録するように求めるプロンプトが表示されます。



5. エージェントのダウンロード時にインストールトークンをコピーしなかった場合は、管理者の **【ランタイム環境】** ページで **【インストールトークンの生成】** をクリックし、トークンをコピーします。
6. Secure Agent Manager で、次の情報を入力し、**【登録】** をクリックします。

オプション	説明
ユーザー名	Informatica Intelligent Cloud Services へのアクセスに使用するユーザー名。
インストールトークン	コピーしたトークン。

Secure Agent Manager が Secure Agent のステータスを表示します。すべてのサービスが起動するまで 1 分かかります。

7. お客様の組織で送信プロキシサーバーを使用してインターネットに接続している場合は、プロキシサーバー情報を入力します。



- Secure Agent Manager を閉じます。

Secure Agent Manager は、最小化されてタスクバーに表示され、停止されるまでサービスとして実行し続けます。

## Windows でのプロキシ設定

組織で送信プロキシサーバーを使用してインターネットに接続する場合、Secure Agent は、そのプロキシサーバー経由で Informatica Intelligent Cloud Services に接続します。Secure Agent のインストーラにより、ブラウザで設定されている設定項目に基づいて Secure Agent のプロキシサーバー設定が設定されます。プロキシサーバーの設定は、Secure Agent Manager から変更できます。

正しいプロキシ設定については、ネットワーク管理者にお問い合わせください。

- Secure Agent Manager で、**【プロキシ】** をクリックします。
- プロキシサーバーの設定値を入力するには、**【プロキシサーバーを使用】** をクリックします。
- 次の情報を入力します。

フィールド	説明
プロキシホスト	必須。Secure Agent が使用する送信プロキシサーバーのホスト名。
プロキシポート	必須。送信プロキシサーバーのポート番号。
ユーザー名	送信プロキシサーバーに接続するユーザー名。
パスワード	送信プロキシサーバーに接続するためのパスワード。

- 【OK】** をクリックします。

Secure Agent Manager によって Secure Agent が再起動され、設定が適用されます。

## Windows Secure Agent サービスへのログインの設定

Windows では、Secure Agent サービスのネットワークログインを設定します。Secure Agent は、ログインに関連付けられている特権と権限によってネットワークにアクセスできます。

Secure Agent がディレクトリにアクセスしてタスクを設定および実行できるように、Secure Agent がインストールされているマシンのログインを設定します。接続を設定する、タスクを設定する、およびフラットファイルまたは FTP/SFTP 接続タイプを使用するタスクを実行する場合、Secure Agent には、関連するディレクトリでの読み取りおよび書き込み権限が必要です。

例えば、ディレクトリを参照してフラットファイルまたは FTP/SFTP 接続を設定するには、Secure Agent のログインでそのディレクトリへのアクセス権限を必要とする場合があります。Secure Agent のログインに適切な権限が付与されていないと、Informatica Intelligent Cloud Services では、**【ディレクトリの参照】** ダイアログボックスにディレクトリを表示できません。

- Windows の **【管理ツール】** から、**【サービス】** ウィンドウに移動します。
- 【サービス】** ウィンドウで、Informatica Cloud Secure Agent サービスを右クリックし、**【プロパティ】** を選択します。
- 【プロパティ】** ダイアログボックスで、**【ログオン】** タブをクリックします。
- ログインを設定するには、**【このアカウント】** を選択します。
- アカウントとパスワードを入力します。

ドメインで定義されているネットワークセキュリティに応じて、必須の特権と権限が付与されているアカウントを使用します。デフォルトのアカウント形式は、<ドメイン名>\<ユーザー名>です。

6. **[OK]** をクリックします。
7. **[サービス]** ウィンドウで、Secure Agent サービスを再起動して変更を有効にします。

## Linux での Secure Agent のインストール

Linux の場合、Secure Agent はプロセスとして実行されます。シェルコマンドラインを使用して、Secure Agent をインストール、登録、起動、停止、およびアンインストールすることができます。

また、シェルコマンドラインを使用して Secure Agent のステータスをチェックすることもできます。

Secure Agent をインストールするときには、次のタスクを実行します。

1. Secure Agent をインストールするマシンが最小要件を満たしていることを確認します。
2. Secure Agent インストーラのファイルをダウンロードします。
3. Secure Agent をインストールして登録します。

## Linux での Secure Agent の要件

Secure Agent は、インターネット接続が可能であり、Informatica Intelligent Cloud Services にアクセス可能な任意のマシンにインストールすることができます。Linux で Secure Agent をインストールする前に、システム要件を確認してください。

Linux で Secure Agent をインストールする前に、次の要件を確認してください。

- Secure Agent をインストールするコンピュータがサポート対象のオペレーティングシステムを使用していることを確認します。Secure Agent でサポートされているオペレーティングシステムのリストについては、ナレッジベースの [Product Availability Matrix \(PAM\) for Informatica Intelligent Cloud Services](#) を参照してください。
- Secure Agent をインストールするマシンに 5 GB 以上の空きディスク容量があることを確認します。
- Secure Agent のインストールに使用するアカウントに、フラットのソースまたはターゲットファイルが格納されているすべてのリモートディレクトリに対するアクセス権が付与されている必要があります。
- PowerCenter を使用する場合は、PowerCenter のインストールに使用したアカウントとは別のユーザーアカウントを使用して、Secure Agent をインストールします。

Informatica Intelligent Cloud Services と PowerCenter は、いくつかの共通の環境変数を使用します。Informatica Intelligent Cloud Services に対して環境変数が正しく設定されていない場合、ジョブは実行時に失敗する可能性があります。

Secure Agent の要件の詳細については、Informatica グローバルカスタマサポートにお問い合わせください。

## ファイアウォールの設定

組織で保護ファイアウォールを使用している場合は、Informatica Intelligent Cloud Services のドメイン名または IP アドレス範囲を承認済みのドメイン名または IP アドレスの一覧に含めます。Secure Agent がファイアウォールを介して必要なすべてのタスクを実行できるようにするには、Secure Agent が使用するポートを有効にします。

Secure Agent はインターネットに接続するためにポート 443 (HTTPS) を使用します。トラフィックがポート 443 を通過することを許可するようにファイアウォールを設定してください。

ドメインと IP アドレスの許可リストはデータセンターに応じて異なり、これは POD (Point of Deployment) とも呼ばれます。POD は、Informatica Intelligent Cloud Services で任意のサービスを開いたときに表示される URL から特定できます。URL 文字列の最初の数文字が POD を表します。例えば、URL が `usw3.dm-us.informaticacloud.com` で始まる場合、POD は USW3 です。

Informatica Network の Informatica Intelligent Cloud Services Administrator [this Knowledge Base article](#) の **【ランタイム環境】** ページの上部にあるリンクをクリックすると、さまざまな POD の管理者ドメインと IP アドレスの許可リストを確認することができます。

## Linux での Secure Agent の権限

Secure Agent には、ソースとターゲットの間でデータを転送するために特定の権限が必要です。

Linux に Secure Agent をインストールする場合、その Secure Agent には、インストールディレクトリに対する読み取り/書き込み/実行権限が必要です。

## Linux での Secure Agent のダウンロードおよびインストール

Linux マシンに Secure Agent をインストールするには、Secure Agent インストールプログラムをダウンロードして実行してから、エージェントを登録する必要があります。

Secure Agent の登録にはインストールトークンが必要です。インストールトークンを取得するには、エージェントのダウンロード時にトークンをコピーするか、または管理者で **【インストールトークンの生成】** オプションを使用します。トークンは 24 時間後に有効期限が切れます。

エージェントを登録すると、デフォルトで独自の Secure Agent グループに追加されます。エージェントは別の Secure Agent グループに追加することもできます。

Secure Agent をダウンロードしてインストールする前に、同じ Linux ユーザーアカウントを使用してそのマシンに他の Secure Agent がインストールされていないことを確認します。他のエージェントが存在する場合は、アンインストールする必要があります。

**ヒント:** Secure Agent インストールプログラムのチェックサムを確認するには、エージェントの REST API バージョン 2 リソースを使用します。エージェントリソースの詳細は、『*REST API リファレンス*』を参照してください。

1. 管理者を開いて **【ランタイム環境】** を選択します。
2. **【ランタイム環境】** ページで、**【Secure Agent のダウンロード】** をクリックします。
3. Linux 64 ビットオペレーティングシステムプラットフォームを選択し、インストールトークンをコピーしてから **【ダウンロード】** をクリックします。

インストールプログラムがご使用のマシンにダウンロードされます。このインストールプログラムの名前は `agent64_install_ng_ext.<Agent Core バージョン>.bin` です。

4. Secure Agent を実行するマシン上のディレクトリにインストールプログラムを保存します。

**注:** ファイルパスにスペースが含まれていると、インストールに失敗します。

5. シェルコマンドラインから、インストールプログラムをダウンロードしたディレクトリに移動し、次のコマンドを入力します。

```
。/agent64_install_ng_ext.bin -i console
```

6. インストーラが終了したら、次のディレクトリに移動します。

```
<Secure Agent のインストールディレクトリ>/apps/agentcore
```

7. Secure Agent を起動するには、次のコマンドを入力します。

```
。/infaagent startup
```

Secure Agent Manager が起動します。Informatica Intelligent Cloud Services へのアクセスに使用するユーザー名を使用してエージェントを登録する必要があります。また、インストールトークンを指定する必要もあります。

8. エージェントのダウンロード時にインストールトークンをコピーしなかった場合は、管理者の **【ランタイム環境】** ページで **【インストールトークンの生成】** をクリックし、トークンをコピーします。
9. エージェントを登録するには、<Secure Agent のインストールディレクトリ>/apps/agentcore ディレクトリで、Informatica Intelligent Cloud Services のユーザー名とコピーしたトークンを使用して、次のいずれかのコマンドを入力します。

- エージェントを独自の Secure Agent グループに追加するには、次のコマンドを使用します。  
`./consoleAgentManager.sh configureToken <user name> <install token>`
- エージェントを既存の Secure Agent グループに追加するには、次のコマンドを使用します。  
`./consoleAgentManager.sh configureTokenWithRuntime <user name> <install token> <Secure Agent group name>`

**注:** 存在しない Secure Agent グループ名がコマンドに含まれている場合、Secure Agent はグループに割り当てられません。有効な Secure Agent グループ名を使用するようにしてください。

以下の表にコマンドのオプションの一覧を示します。

オプション	説明
ユーザー名	必須。Secure Agent をインストールするユーザーの Informatica Intelligent Cloud Services ユーザー名。
インストールトークン	必須。コピーしたインストールトークン。
Secure Agent グループ名	オプション。既存の Secure Agent グループにエージェントを追加する場合、代わりに含めます。このオプションがコマンドに含まれていない場合、エージェントは独自の Secure Agent グループに追加されます。

Secure Agent の登録ステータスは、次のコマンドを使用して確認できます。

。 `./consoleAgentManager.sh isConfigured`

## Linux でのプロキシ設定

組織で送信プロキシサーバーを使用してインターネットに接続する場合、Secure Agent は、そのプロキシサーバー経由で Informatica Intelligent Cloud Services に接続します。Secure Agent のインストーラにより、ブラウザで設定されている設定項目に基づいて Secure Agent のプロキシサーバー設定が設定されます。プロキシサーバーの設定の更新は、コマンドラインおよび管理者サービスから行います。

1. コマンド プロンプトを開き、次のディレクトリに移動します。  
<Secure Agent installation directory>/apps/agentcore
2. proxy.ini ファイルを更新するシェルコマンドを使用します。ネットワーク管理者に問い合わせ、プロキシの設定項目を決めてください。

次のコマンドを使用して、proxy.ini ファイルを更新します。

`./consoleAgentManager.sh configureProxy <proxy host> <proxy port> <proxy user name> <proxy password>`

3. Informatica Intelligent Cloud Services にログインします。
4. [管理者] サービスを開いて **【ランタイム環境】** を選択します。
5. プロキシサーバーを設定する Secure Agent を選択します。

6. ページの右上隅にある【編集】をクリックします。
7. 【システム構成の詳細】セクションで、【サービス】のプロパティを【データ統合サーバー】に設定し、【タイプ】のプロパティを【DTM】に設定します。
8. 使用可能な【JVMOption】フィールドに必要なパラメータを追加し、各パラメータに適切な値を指定します。

以下の表に、追加可能なパラメータを示します。

パラメータ	説明
-Dhttp.proxyHost=	送信 HTTP プロキシサーバーのホスト名。
-Dhttp.proxyPort=	送信 HTTP プロキシサーバーのポート番号。
-Dhttp.proxyUser=	HTTP プロキシサーバの認証ユーザ名。このオプションは、プロキシサーバーが認証を要求した場合に必要です。
-Dhttp.proxyPassword=	認証されたユーザのパスワード。本オプションは、プロキシサーバが認証を要求した場合に必要となります。
-Dhttps.proxyHost=	送信 HTTPS プロキシサーバーのホスト名。
-Dhttps.proxyPort=	送信 HTTPS プロキシサーバーのポート番号。
-Dhttps.proxyUser=	HTTPS プロキシサーバーの認証ユーザー名。このオプションは、プロキシサーバーが認証を要求した場合に必要です。
-Dhttps.proxyPassword=	認証されたユーザのパスワード。本オプションは、プロキシサーバが認証を要求した場合に必要となります。

HTTP の例。

```
JVMOption1=-Dhttp.proxyHost=<proxy_server_hostname>
JVMOption2=-Dhttp.proxyPort=8081
JVMOption3=-Dhttp.proxyUser=<proxy_user_name>
JVMOption4=-Dhttp.proxyPassword=<proxy_password>
```

HTTPS の例。

```
JVMOption1=-Dhttps.proxyHost=<proxy_server_hostname>
JVMOption2=-Dhttps.proxyPort=8081
JVMOption3=-Dhttps.proxyUser=<proxy_user_name>
JVMOption4=-Dhttps.proxyPassword=<proxy_password>
```

9. 【保存】をクリックします。  
Secure Agent が再起動して設定が適用されます。

## 第 4 章

# 接続設定

接続を作成すると、データ統合組織で使用できるようになります。

ほとんどの接続タイプで、接続を設定する際には、接続のランタイム環境を指定します。ランタイム環境には、接続の設定時に稼働中のエージェントが含まれている必要があります。その他の接続タイプの場合は、タスクの設定時にランタイム環境を指定します。

ここでは、接続の設定に関する一般的な情報について説明します。接続およびフラットファイルと FTP 接続の設定に関する詳細については、「[接続](#)」を参照してください。その他の接続の種類の詳細については、ヘルプの「[コネクタ](#)」セクションのデータ統合コネクタのトピックを参照してください。

## 接続の設定

接続を構成するには、**[接続]** ページ、タスクまたはタスクフローを構成するときにウィザードで、またはマッピングを構成するときにマッピングデザイナを実行します。

**[接続]** ページにアクセスするには、管理者で **[接続]** を選択します。

1. 次の接続の詳細を設定します。

接続の詳細	説明
接続名	接続の名前。 各接続名は組織内で一意である必要があります。接続名には、英数字、スペース、および次の特殊文字を含めることができます。_ . + - 最大長は 100 文字です。接続名では大文字と小文字は区別されません。
説明	接続の説明。 最大長は 255 文字です。
タイプ	Salesforce や Oracle などの接続のタイプ。

2. 接続固有のプロパティを設定します。例えば、フラットファイル接続タイプの場合は、接続で使用するランタイム環境、フラットファイルの保存先ディレクトリ、フラットファイルの日付フィールドの形式、フ

ラットファイルをホストするシステムのコードページを入力します。次の画像は、フラットファイル接続のプロパティフィールドを示しています。

The screenshot shows the 'New Connection' dialog box. At the top, there is a title bar with a plug icon, the text 'New Connection', and two buttons: 'Save' and 'Test Connection'. Below the title bar is a section titled 'Connection Details' with the following fields: 'Connection Name' (SalesAccounts-FlatFile), 'Description' (empty), and 'Type' (Flat File). Below this is a section titled 'Flat File Connection Properties' with the following fields: 'Runtime Environment' (CAB123456), 'Directory' (C:\OurCompany\Sales), 'Date Format' (MM/dd/yyyy HH:mm:ss), and 'Code Page' (UTF-8). There is a 'Browse...' button next to the 'Directory' field.

3. 接続をテストするには、**【テスト】** をクリックします。次の画像に示すとおり、テスト結果がページに表示されます。

The screenshot shows the 'SalesAccounts-FlatFile' dialog box. At the top, there is a title bar with a plug icon, the text 'SalesAccounts-FlatFile', and two buttons: 'Save' and 'Test Connection'. Below the title bar is a green checkmark icon and the text 'The test for this connection was successful.' Below this is a section titled 'Connection Details' with the following fields: 'Connection Name' (SalesAccounts-FlatFile), 'Description' (empty), and 'Type' (Flat File). Below this is a section titled 'Flat File Connection Properties' with the following fields: 'Runtime Environment' (CAB123456), 'Directory' (C:\OurCompany\Sales), 'Date Format' (MM/dd/yyyy HH:mm:ss), and 'Code Page' (UTF-8). There is a 'Browse...' button next to the 'Directory' field.

データベース接続に失敗する場合は、データベース管理者にお問い合わせください。

4. **【保存】** をクリックして接続を保存します。

## オブジェクト検索と選択

データ統合のマッピングまたはタスクで接続を選択すると、使用する 1 つのオブジェクトまたは複数のオブジェクトを検索できます。オブジェクトはマッピングとタスクウィザードで検索できます。

オブジェクトを検索するとき、**【オブジェクトを選択】** ダイアログボックスに、接続に使用できるオブジェクトが表示されます。いずれかのオブジェクトを選択するか、検索文字列を入力できます。検索を開始するには、**【検索】** をクリックするか、**Enter** を押します。

**注:** 一部の接続タイプでは、オブジェクトを表示して選択する前に、**[パッケージ]** ペインでオブジェクトに関連付けられたスキーマを選択する必要があります。使用するスキーマを検索できます。

同期とマッピングタスクの場合、接続の応答が遅いときにオブジェクト検索を使用します。

検索文字列を入力するときは、以下のガイドラインに従ってください。

- ワイルドカード文字にはアスタリスク (\*) を使用します。
- 完全一致検索を実行するには引用符 (") を使用します。完全一致検索では大文字と小文字が区別されます。
- 接続タイプに基づいて次の検索パラメータを使用できます。

接続タイプ	検索パラメータ
データベース	名前
CDC	名前
フラットファイル	名前



## 第 5 章

# プロジェクトの設定

**【エクスプローラ】** ページでプロジェクトとプロジェクトフォルダを作成し、アセットを整理します。プロジェクトに必要なランタイム環境と接続を設定したら、プロジェクトのアセットを作成できます。

次の文字は使用できません。

# ? ' | { } " ^ & [ ] / \

これらの文字を、プロジェクト、アセット、タグ名に使用しないでください。

## プロジェクトとプロジェクトフォルダの作成

プロジェクトで使用されるアセットを整理するために使用できる複数のフォルダを含めることができます。**【エクスプローラ】** ページを使用してプロジェクトを作成します。

プロジェクトを作成するには、**【エクスプローラ】** ページに移動し、プロジェクト別およびフォルダ別のエクスプローラを選択して、**【新規プロジェクト】** をクリックします。



プロジェクトフォルダを作成するには、**【エクスプローラ】** ページに移動してプロジェクトを開き、**【新規フォルダ】** をクリックします。



プロジェクトには、1つのレベルのフォルダを作成できます。フォルダ内にフォルダを作成することはできません。

プロジェクトの操作の詳細については、「**アセットの管理**」を参照してください。

# アセットの作成

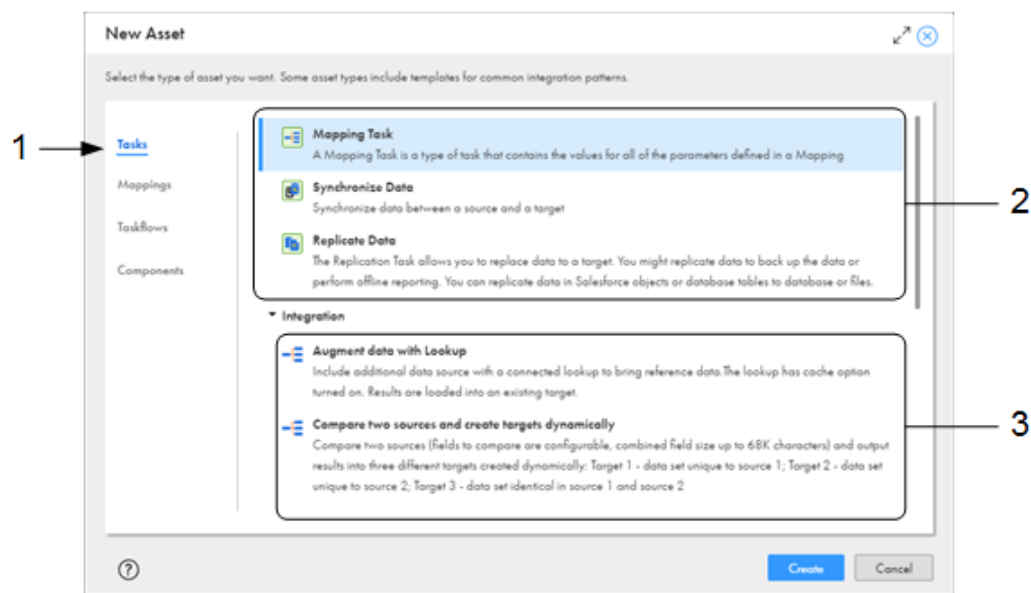
統合アセットを作成し、プロジェクトに割り当てます。

カスタムアセットを作成したり、テンプレートからアセットを作成したりできます。

カスタムアセットを作成するには、**【新規】** をクリックし、アセットタイプを選択します。特定のタイプのアセットを作成する具体的な方法については、マッピングまたはタスクの適切なアセットタイプを参照してください。

テンプレートからアセットを作成するには、**【新規】** をクリックし、アセットタイプを選択して、適切なテンプレートを選択します。マッピングタスクテンプレートとマッピングテンプレートは、マッピングタイプに対応する見出しの下に一覧表示されます。

次の図は、アセットを作成するときに表示されるダイアログボックスを示しています。



1. 作成するアセットのタイプを選択します。このイメージでは、[Tasks] が選択されています。
2. これらのオプションのいずれかを選択して、カスタムアセットを作成します。左側で [Tasks] が選択されているため、この領域には作成できるタスクが一覧表示されます。
3. 見出しの下いずれかのオプションを選択して、テンプレートからタスクを作成します。このイメージでは、[Integration] の見出しが展開されているので、一覧表示されているテンプレートはデータ統合マッピングに基づいています。

**ヒント:** 組織で理解できるような標準的な命名規則を使用する事をお勧めします。以下はその例です。

- すべてのアセット名の先頭にアセットタイプの略語を付けます。例えば、マッピング名の場合は m\_、マッピングタスクの場合は mt\_ を先頭に付けます。
- マッピング内では、すべてのソーストランスフォーメーション名が src\_ で始まり、すべてのパラメータ名が p\_ で始まるようにするなどができます。
- フィルタ名を flt\_ から始めるなど、オブジェクトの目的を説明する名前も使用できます。

標準的な命名規則は、大規模で複雑なマッピングを使用する場合に特に役立ちます。これにより、各オブジェクトのタイプおよび目的を簡単に識別できます。

アセットの操作の詳細については、「アセットの管理」を参照してください。

## 第 6 章

# ソース管理の有効化

Informatica Intelligent Cloud Services 組織に、ソース管理を使用するライセンスがある場合は、Informatica Intelligent Cloud Services でソース管理リポジトリのユーザー資格情報を指定します。

組織でソース管理を使用するには、組織の管理者が、Informatica Intelligent Cloud Services 組織と GitHub または Azure DevOps Git ソース管理リポジトリとの間のリンクを事前に設定する必要があります。

ソース管理リポジトリに対する読み取り/書き込みアクセス権が組織にある場合は、プロジェクトやアセットをリポジトリに追加できます。オブジェクトをチェックアウトまたは変更してリポジトリにチェックインするたびに、ソース管理システムによってオブジェクトの新しいバージョンが作成されます。

ソース管理リポジトリに対する組織のアクセス権が読み取り専用アクセス権の場合、プロジェクトやアセットのバージョンを取り出すことはできますが、新しいオブジェクトや更新したオブジェクトをリポジトリに追加することはできません。

ソース管理に関する詳細については、「[アセットの管理](#)」を参照してください。

## リポジトリアクセスの設定

ソース制御オブジェクトを操作するには、Informatica Intelligent Cloud Services で GitHub または Azure DevOps Git リポジトリの認証情報を指定します。

資格情報には、ユーザー名とパーソナルアクセストークンを含めることができます。

管理者が組織のリポジトリを OAuth アクセス用に設定している場合は、パーソナルアクセストークンを提供する代わりに OAuth アクセスを有効化することができます。

パーソナルアクセストークンは、プライベートリポジトリを完全に制御できるように設定する必要があります。パーソナルアクセストークンの生成については、GitHub または Azure DevOps Git のヘルプを参照してください。

Informatica Intelligent Cloud Services で次のステップを実行して、リポジトリへのアクセスを設定します。

1. Informatica Intelligent Cloud Services ウィンドウ右上隅にある **【ユーザー】** アイコンをクリックして、**【設定】** を選択します。
2. 次のいずれかの手順に従います。
  - リポジトリの資格情報を入力します。GitHub の場合は、ユーザー名とパーソナルアクセストークンを入力します。Azure DevOps Git の場合は、パーソナルアクセストークンを入力します。
  - リポジトリへの OAuth アクセスを有効にします。アクセスを許可していない場合は、Git アクセスアプリが表示されます。Informatica Intelligent Cloud Services へのアクセスを承認する場合に選択します。
3. **【保存】** をクリックします。

## 第 7 章

# ユーザープロファイルの編集

ユーザープロファイルには Informatica Intelligent Cloud Services のユーザーアカウントの詳細が含まれます。

プロファイル内の次の情報を更新できます。

- 姓名
- 役職
- 電子メールアドレス
- 電話番号
- タイムゾーン（[すべてのジョブ]、[実行中のジョブ]、[マイジョブ]、[インポート/エクスポートログ]、[マイインポート/エクスポートログ] ページのジョブ実行のタイムスタンプで使用）
- パスワード
- セキュリティの質問および回答

**注:** SAML を使用して Informatica Intelligent Cloud Services にサインオンし、組織の管理者が管理者の **[SAML セットアップ]** ページで SAML グループとロールのマッピングを有効にしている場合、更新できるのはタイムゾーンのみです。その他の属性は、Informatica Intelligent Cloud Services にログインするたびにエンタープライズディレクトリから直接更新されます。

1. Informatica Intelligent Cloud Services ウィンドウ右上隅にある **[ユーザー]** アイコンをクリックして、**[プロファイル]** を選択します。
2. **[プロファイル]** ページで、氏名、役職、電話番号、タイムゾーンなどの個人情報を追加または編集します。
3. 電子メールアドレスを更新するには、**[電子メールを更新]** をクリックします。  
Informatica Intelligent Cloud Services から新しい電子メールアドレス宛てに確認メールが送信されます。電子メールには、24 時間有効なリンクが含まれています。電子メール内のリンクをクリックすると、新しいアドレスが確認され、プロファイルに表示されます。リンクの有効期限が切れた場合は、確認メールを再送信できます。
4. 必要に応じて、パスワードまたはセキュリティの質問を変更します。
5. **[保存]** をクリックします。

## 第 8 章

# 別の組織への切り替え

親組織の管理者またはサブ組織の表示権限を持つ親組織のユーザーの場合は、これらの組織間で切り替えることができます。Informatica Intelligent Cloud Services をログアウトして、もう一度ログインする必要はありません。

**注:** 親組織から下位組織に切り替えると、下位組織で次の操作を実行できなくなります。

- データ転送タスクの作成またはインポート
- 動的マッピングタスクの作成またはインポート
- タスクフローの検証または実行

別の組織に切り替えるには:

- ▶ 右上隅の【組織】メニューから、表示する組織を選択します。

# 索引

## A

Azure DevOps ユーザー資格情報 [27](#)

## C

Cloud Application Integration コミュニティ  
URL [5](#)  
Cloud 開発者コミュニティ  
URL [5](#)

## G

GitHub ユーザー資格情報 [27](#)

## H

Hosted Agent  
定義 [7](#)

## I

Informatica Intelligent Cloud Services  
Web サイト [5](#)  
Informatica グローバルカスタマサポート  
連絡先情報 [6](#)  
Internet Explorer 11  
要求条件 [9](#)

## L

Linux  
プロキシの設定 [20](#)

## P

POD  
特定方法 [15](#), [18](#)

## S

Secure Agent  
IP アドレス許可リスト [15](#), [18](#)  
Linux での権限 [19](#)  
Linux での登録 [19](#)  
Linux での要件 [18](#)  
Linux へのインストール [19](#)  
Windows サービスログインの設定 [17](#)  
Windows での起動 [14](#)

Secure Agent (続く)  
Windows での権限 [15](#)  
Windows での登録 [15](#)  
Windows での要件 [14](#)  
Windows へのインストール [15](#)  
ドメイン許可リスト [15](#), [18](#)  
通信ポート [15](#), [18](#)  
定義 [7](#)  
Secure Agent Manager  
起動 [14](#)  
Secure Agent グループ  
定義 [7](#)

## W

Web サイト [5](#)  
Windows  
プロキシの設定 [17](#)  
Windows サービス  
Secure Agent ログインの設定 [17](#)

## あ

アセット  
ソース管理 [27](#)  
作成 [26](#)  
アップグレード通知 [6](#)

## お

オブジェクト検索  
タスクウィザード [23](#)

## さ

サブ組織  
別の組織への切り替え [29](#)

## し

システムステータス [6](#)  
システム要件 [9](#)

## す

ステータス  
Informatica Intelligent Cloud Services [6](#)

## せ

セキュリティの質問  
編集 [28](#)

## そ

ソース  
タスクウィザードでの検索 [23](#)  
ソース管理  
リポジトリへのアクセスの設定 [27](#)

## た

ターゲット  
タスクウィザードでの検索 [23](#)  
タイムゾーン  
ユーザープロファイルの変更 [28](#)

## て

ディレクトリ  
アクセスする Secure Agent ログインの設定 [17](#)

## は

バージョン管理 [27](#)  
パスワード  
変更 [28](#)

## ふ

ファイアウォール  
設定 [15](#), [18](#)

フォルダ  
作成 [25](#)  
プロキシ設定  
Linux での設定 [20](#)  
Windows 上での設定 [17](#)  
プロジェクト  
ソース管理 [27](#)  
フォルダの作成 [25](#)  
作成 [25](#)  
プロファイル  
編集 [28](#)

## め

メンテナンスの停止 [6](#)

## ゆ

ユーザープロファイル  
編集 [28](#)

## ら

ランタイム環境  
設定 [7](#)

## る

ルックアップ  
タスクウィザードでの検索 [23](#)