



Informatica®

Informatica® Intelligent Cloud Services  
October 2022

# 組織管理

© 著作権 Informatica LLC 2021, 2022

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（電子的複写、写真複写、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」提供するものとしします。

発行日: 2022-12-01

# 目次

<b>序文</b> .....	6
Informatica のリソース.....	6
Informatica マニュアル.....	6
Informatica Intelligent Cloud Services Web サイト.....	6
Informatica Intelligent Cloud Services コミュニティ.....	6
Informatica Intelligent Cloud Services マーケットプレース.....	7
データ統合コネクタのドキュメント.....	7
Informatica ナレッジベース.....	7
Informatica Intelligent Cloud Services Trust Center.....	7
Informatica グローバルカスタマサポート.....	7
<b>第 1 章 : 管理者について</b> .....	8
<b>第 2 章 : 組織</b> .....	11
組織の設定.....	11
組織のプロパティ.....	12
組織の全般プロパティ.....	13
認証プロパティ.....	14
接続プロパティの保存場所.....	15
データ統合サービスのプロパティ.....	15
CLAIRE の推奨設定.....	16
Enterprise Data Catalog 統合プロパティ.....	16
サブ組織.....	17
サブ組織の追加.....	18
サブ組織の削除.....	19
サブ組織の無効化または有効化.....	20
別の組織への切り替え.....	21
サブ組織への親組織のアクセスを拒否.....	21
サブ組織のアドオンコネクタ.....	21
サブ組織でのアセットのエクスポートとインポート.....	22
追加プロダクション組織とサンドボックス組織.....	22
追加の組織の作成.....	23
<b>第 3 章 : ライセンス</b> .....	25
ライセンスのカテゴリ.....	25
ライセンスのタイプ.....	26
サブ組織のライセンス.....	26
サブ組織のライセンスの編集.....	27
親組織とのライセンスの同期.....	27
組織タイプの設定.....	27

ライセンスの有効期限. . . . .	28
<b>第 4 章: メータリング. . . . .</b>	<b>29</b>
機能ベースのライセンスメーター. . . . .	29
ライセンスメトリックの表示. . . . .	30
メータリングの使用状況レポート. . . . .	34
使用状況の詳細の表示. . . . .	35
Informatica のプロセッシングユニットのメトリック. . . . .	36
IPU メトリックの表示. . . . .	37
IPU スカラ. . . . .	37
IPU メーター. . . . .	38
IPU メトリックレポート. . . . .	39
<b>第 5 章: ソース管理、サービスアップグレード、およびブランディング設定. . . . .</b>	<b>41</b>
ソース管理設定. . . . .	41
サブ組織のソース管理設定. . . . .	43
OAuth を使用したリポジトリアクセス. . . . .	43
オンプレミスリポジトリの操作. . . . .	43
組織のソース管理の有効化. . . . .	44
ソース管理リポジトリ URL の変更. . . . .	45
組織のソース管理の無効化. . . . .	46
リポジトリアクセスの設定. . . . .	47
ソース管理のベストプラクティス. . . . .	47
別のユーザーのチェックアウトの取り消し. . . . .	48
Secure Agent サービスのローリングアップグレード. . . . .	49
ローリングアップグレードエラーの処理. . . . .	50
Secure Agent サービスの再開スケジュールの設定. . . . .	50
カスタムブランディングの設定. . . . .	51
ロゴおよびファビコンのガイドライン. . . . .	51
組織のカスタムブランディングの設定. . . . .	51
<b>第 6 章: 権限. . . . .</b>	<b>52</b>
権限のルールおよびガイドライン. . . . .	53
権限の設定. . . . .	54
<b>第 7 章: スケジュール. . . . .</b>	<b>56</b>
ブラックアウト期間の設定. . . . .	57
繰り返し頻度. . . . .	57
タイムゾーンとスケジュール. . . . .	58
夏時間への移行とスケジュール. . . . .	58
スケジュールの設定. . . . .	59
スケジュールのエクスポート. . . . .	60

スケジュール済みタスクのトラブルシューティング.....	60
<b>第 8 章: バンドル管理.....</b>	<b>62</b>
バンドルのインストール.....	62
バンドルのコピー.....	63
バンドルのアップグレード.....	64
バンドルのアンインストール.....	64
<b>第 9 章: イベント監視.....</b>	<b>65</b>
<b>第 10 章: セキュリティのトラブルシューティング.....</b>	<b>67</b>
<b>索引.....</b>	<b>68</b>

# 序文

「組織管理」を参考にして、Informatica Intelligent Cloud Services<sup>SM</sup>の組織およびサブ組織を設定および保守する方法を学びます。ライセンスの管理とライセンスの使用状況の監視、ソース管理の設定、オブジェクトの権限の設定、スケジュールの作成、バンドルの管理、イベントの監視、およびセキュリティ問題のトラブルシューティングの方法を確認します。

## 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> に掲載されていません。

# 第 1 章

## 管理者について

管理者は、Informatica Intelligent Cloud Services にわたる組織管理機能を提供します。

管理者を使用して、組織の以下の側面を管理します。

### 組織とサブ組織

パスワードの要件、信頼される IP アドレス、接続プロパティの保存、データ統合タスクのタイムゾーンおよび電子メール通知の設定、CLAIRE™推奨の設定、Enterprise Data Catalog の設定など、組織およびサブ組織の設定を行います。サブ組織を作成し、管理します。

組織およびサブ組織の詳細については、[第 2 章、「組織」 \(ページ 11\)](#)を参照してください。

### ライセンス

組織のライセンスを表示し、下位組織のライセンスを管理します。

ライセンスについては、[第 3 章、「ライセンス」 \(ページ 25\)](#)を参照してください。

### メータリング

ジョブ制限、使用状況、Informatica プロセッシングユニット (IPU) のバランスなどのメータリング情報を表示します。

メータリングについては、[第 4 章、「メータリング」 \(ページ 29\)](#)を参照してください。

### エコシステムと SAML のシングルサインオン

Microsoft Azure のシングルサインオン設定を行います。SAML のサードパーティ ID プロバイダのシングルサインオン機能を有効にします。

Microsoft Azure シングルサインオン設定の詳細、および SAML シングルサインオンの有効化と設定に関する詳細については、「[ユーザー管理](#)」を参照してください。

### ソース管理および Secure Agent サービスのアップグレード設定

プロジェクト、フォルダ、およびアセットのバージョン管理を有効にするためのソース管理を設定します。一部の Secure Agent サービス用にアップグレードエラー処理とアップグレード再起動スケジュールを設定します。

ソース管理と Secure Agent サービスのアップグレード設定の詳細については、[第 5 章、「ソース管理、サービスアップグレード、およびブランディング設定」 \(ページ 41\)](#)を参照してください。

### ユーザー、ユーザーグループ、およびユーザーロール

ユーザーアカウントを個別に作成および設定して、組織にアクセスできるようにします。同じタスクを実行できるユーザーグループを作成します。ロールを作成および設定して、ユーザーとユーザーグループの特権を定義します。

ユーザー、ユーザーグループ、およびユーザーロールの詳細については、「[ユーザー管理](#)」を参照してください。

## 許可

ユーザーとユーザーグループが Secure Agent、Secure Agent グループ、接続、およびスケジュールなどのオブジェクトに対して持つ事のできるアクセス権限を設定します。

権限および権限の設定に関する詳細については、[第 6 章、「権限」 \(ページ 52\)](#)を参照してください。

## ランタイム環境

Secure Agent をダウンロードし、インストールします。Secure Agent グループを作成し、設定します。

Secure Agent、Secure Agent グループ、および Secure Agent のダウンロードとインストールの詳細については、「ランタイム環境」を参照してください。

## サーバーレスランタイム環境

メンテナンスのオーバーヘッドを削減するために、データ統合によって管理されるランタイム環境を使用します。

**注:** サーバーレスランタイム環境を使用するには、AWS クラウドプラットフォームでプライベートクラウドを使用する必要があります。

サーバーレスランタイム環境の詳細については、「ランタイム環境」を参照してください。

## Secure Agent サービス

エラスティックサーバー、CIH プロセッサ、データ統合サーバー、EDC 検索エージェント、プロセスサーバーなど、Secure Agent がデータ処理に使用するマイクロサービスを設定します。

Secure Agent サービスとその設定の詳細については、「*Secure Agent* サービス」を参照してください。

## 詳細クラスタ

組織がデータ統合ジョブを処理するために使用できる一時クラスタを管理します。

詳細クラスタの詳細については、[詳細クラスタに関する説明](#)を参照してください。

## スケジュール

タスクまたはタスクフローを、指定した時間または一定の間隔で実行するようにスケジュールを作成します。組織でスケジュールされたタスクやジョブが実行出来なくなるブラックアウト期間を定義します。

スケジュールおよび組織のブラックアウト期間に関する詳細については、[第 7 章、「スケジュール」 \(ページ 56\)](#)を参照してください。

## アドオンバンドル

データ統合ユーザーがデータ統合プロジェクトで使用できる関連マッピング、マッピングタスク、マップレット、および Visio テンプレートのセットをインストール、コピー、アップグレード、およびアンインストールします。

アドオンバンドルの管理に関する詳細については、[第 8 章、「バンドル管理」 \(ページ 62\)](#)を参照してください。

## イベント監視

アセットおよびセキュリティログを使用して、組織内のアセット、ライセンス、ユーザー、および Secure Agent のイベントを監視します。

アセットおよびセキュリティログの詳細については、[第 9 章、「イベント監視」 \(ページ 65\)](#)を参照してください。

## ファイル転送

組織のファイルサーバーを設定して、ビジネスパートナーのリモートサーバーからファイルを安全に送受信します。接続を設定してから Informatica Intelligent Cloud Services の REST API を使用してパートナーにファイルを送信します。

ファイルサーバーとファイル転送の詳細については、「[ファイル転送](#)」を参照してください。

## 第 2 章

# 組織

組織は、ライセンス、ユーザーアカウント、マッピングやタスクなどのデータ統合アセット、およびジョブとセキュリティに関する情報を格納する Informatica Intelligent Cloud Services リポジトリ内の安全な領域です。1 つ以上の組織にアクセスできる場合があります。

デフォルトでは、無料トライアルを開始するときに作成する組織はプロダクション組織です。

ライセンスに基づき、次の組織にもアクセスできる場合があります。

### サブ組織

適切なライセンスがある場合、プロダクション組織の管理者は 1 つ以上のサブ組織を作成できます。サブ組織は、プロダクション組織の子組織です。これらは親組織に自動的にリンクされます。

各サブ組織には、独自のアセット、接続、ランタイム環境、およびユーザーのセットがあります。ただし、親組織は、ランタイム環境とアドオンコネクタをサブ組織と共有できます。親組織の管理者は、サブ組織がこれを禁止していない限り、サブ組織に切り替えることができます。

サブ組織から他の組織を作成することはできません。

### 追加プロダクション組織とサンドボックス組織

適切なライセンスがある場合、プロダクション組織の管理者は追加プロダクション組織とサンドボックス組織を作成できます。

これらの組織は、IPU を使用するためプロダクション組織に自動的にリンクされますが、それ以外は完全に独立した組織です。これらは、アセット、接続、ランタイム環境、またはユーザーをプロダクション組織と共有しません。プロダクション組織の管理者は、追加プロダクション組織またはサンドボックス組織に切り替えることはできません。

プロダクション組織が、サブ組織を作成するライセンスを持っている場合、追加プロダクション組織とサンドボックス組織の管理者は、組織のサブ組織を作成できます。

組織の管理者は、組織とそのサブ組織を保持します。Informatica Intelligent Cloud Services に管理者としてログインし、組織の設定、スケジュールの作成と管理、およびアセットとセキュリティに関連するアクティビティの監視を行います。

## 組織の設定

組織を構成するときは、組織のプロパティ、サブ組織、追加プロダクション組織、ライセンス、ランタイム環境、およびユーザーアカウントを設定します。

会社の組織を設定するには、次の手順を実行します。

1. 組織名や住所、認証情報、通知を受ける電子メールアドレスなどの組織のプロパティを構成します。

2. 組織に適切なライセンスがあることを確認します。
3. 必要に応じて、1つ以上のサブ組織を作成し、サブ組織のライセンスを設定します。
4. 必要に応じて、追加プロダクション組織とサンドボックス組織を作成します。
5. ランタイム環境と Secure Agents を設定します。
6. ユーザー、ユーザーグループ、およびロールを設定します。

また、組織用に非ネイティブコネクタをダウンロードしてインストールする必要がある場合もあります。例えば、組織内のユーザーが Teradata テーブルからデータを読み取るタスクを作成する場合は、Teradata のアドオンコネクタをダウンロードしてインストールする必要があります。アドオンコネクタのダウンロードとインストールの詳細については、「[接続](#)」を参照してください。

## 組織のプロパティ

**【組織】** ページで、組織またはサブ組織のプロパティを設定します。**【組織】** ページにアクセスするには、管理者で **【組織】** を選択します。

次の図は、**【組織】** ページを示しています。

The screenshot displays the Informatica Administrator interface for the 'InfoProd' organization. The left sidebar contains navigation options such as Licenses, SAHL Setup, Metering, Settings, Users, User Groups, User Roles, Runtime Environments, Serverless Environments, Connections, Add-On Connectors, Schedules, Add-On Bundles, Swagger Files, Logs, Elastic Clusters, and File Servers. The main content area is titled 'InfoProd' and includes a 'Save' button. It is divided into four sections: Overview, Address, History, and Authentication. The Overview section contains fields for Name (InfoProd), ID (1sig81FMVghyRkQsfz3w), Environment Type (Production), Description, and Number of Employees (1001 - 5000 employees). The Address section contains fields for Address 1 (2100 Seaport Blvd.), Address 2, Address 3, City (Redwood City), State (CA), Zip Code (94063), and Country (United States). The History section shows Created By (System builtin user), Created On (Mar 10, 2018, 1:56 PM), Updated By (System builtin user), and Updated On (Mar 10, 2018, 1:58 PM). The Authentication section includes fields for Minimum Password Length (9), Minimum Character Mix (3), Password Reuse (After 90 Days), and Password Expires (After 180 Days), along with a checkbox for Use Trusted IP Ranges.

次のプロパティを設定することができます。

- 組織名、説明、従業員数、住所情報などの全般的なプロパティ。
- 認証情報と接続プロパティの保存場所。
- 電子メール通知に使用するタイムゾーンや電子メールアドレスなどのデータ統合サービスのプロパティ。
- CLAIRE™の推奨設定。有効にすると、収集されたメタデータに基づいて CLAIRE で推奨する設計時間が指定されます。
- Enterprise Data Catalog サービスの URL、Enterprise Data Catalog からデータを読み取るランタイム環境、Enterprise Data Catalog のユーザー名とパスワードなどの Enterprise Data Catalog 統合プロパティ。

## 組織の全般プロパティ

組織およびサブ組織の全般的なプロパティを構成できます。全般プロパティには、組織名、ID、説明、住所、従業員の数などの情報が含まれます。組織の履歴情報も全般プロパティに表示されます。

全般プロパティには次のような情報があります。

### 概要情報

以下の表で、概要プロパティについて説明します。

プロパティ	説明
名前	組織の名前。 組織名を変更した場合、ログアウトしてログインし直すと【組織】メニューに新しい名前が表示されます。
ID	組織の作成時に組織に割り当てられた ID。組織 ID を変更することはできません。
親組織 ID	サブ組織を表示すると、このプロパティには、親組織に割り当てられた ID が表示されます。組織 ID を変更することはできません。
組織のステータス	サブ組織を表示した場合、このプロパティにはサブ組織が有効であるか無効であるかが表示されます。
環境タイプ	組織の環境タイプ（本番(商用)環境、QA、開発環境、またはサンドボックス）。 Informatica Intelligent Cloud Services は、組織の作成方法に基づいて、次の方法で環境タイプを設定します。 - 無料トライアルを使用して組織を作成する場合、環境タイプは [本番(商用)環境] です。 - 追加プロダクション組織を作成する場合、環境タイプは [本番(商用)環境] です。 - サンドボックス組織を作成する場合、環境タイプは [サンドボックス] です。 環境タイプ間で機能の違いはありません。
説明	組織の説明（省略可能）。
従業員数	組織内の従業員数。
このサブ組織への親組織のアクセスを拒否	このオプションをオンにすると、親組織のユーザーは、親組織からサブ組織に切り替えられません。適切な権限を所有する親組織のユーザーは、サブ組織に次の変更のみを加えることができます。 - サブ組織の有効化および無効化 - サブ組織のライセンスの更新 - 組織の説明や CLAIR の推奨設定などのサブ組織のプロパティの編集 このオプションはサブ組織の【組織】ページに表示されます。このオプションは、サブ組織の管理者がサブ組織にログインすると変更できます。このオプションは、親組織の管理者がサブ組織の組織のプロパティを表示するときは読み取り専用です。 このオプションはデフォルトでオフになっています。

### 住所情報

住所プロパティを使用して、組織の住所、郵便番号、都道府県、および国を指定します。

### 履歴情報

組織の履歴情報には、組織が作成された日時、組織を作成したユーザー、組織が最後に更新された日時、および組織を最後に更新したユーザーが表示されます。組織に変更を加えると、Informatica Intelligent Cloud Services で履歴情報が更新されます。

## 認証プロパティ

組織およびサブ組織の認証プロパティを構成できます。認証プロパティは、パスワード制限および IP アドレスフィルタリングを制御します。

ユーザーが匿名ユーザーのパスワードを作成または変更する場合は、パスワード制限が適用されます。パスワードの有効期限日を [Never (なし)] からある日数に変更すると、その日数より古いパスワードを持つユーザーは、次回 Informatica Intelligent Cloud Services にログインするときにパスワードを変更する必要があります。

次の表に、認証プロパティを示します。

プロパティ	説明
パスワードの最小文字数	有効なパスワードに必要なパスワードの最小文字数。4 から 12 文字の範囲でなければなりません。
最小混合文字数	有効なパスワードに必要な文字タイプの最小数。 パスワードには、次の文字セットを混在させることができます。 <ul style="list-style-type: none"><li>- 小文字の英字</li><li>- 大文字の英字</li><li>- 数字</li><li>- 特殊文字</li></ul> 例えば、 <b>[最小混合文字数]</b> オプションを 1 に設定した場合、パスワードには 1 つ以上の文字セットが含まれている必要があります。 <b>[最小混合文字数]</b> を 2 に設定した場合は、パスワードに 2 つ以上の文字セットが含まれている必要があります。
パスワードの再利用	ユーザーがパスワードを再利用できるかどうかを制御します。
パスワードの有効期限が切れる	ユーザーがパスワードをリセットしなければならない頻度を設定します。
セッションのアイドルタイムアウト	非アクティブによりユーザーのセッションがタイムアウトするまでの時間。Informatica Intelligent Cloud Services は、ユーザーがログアウトする 60 秒前に警告メッセージを表示します。 デフォルトは 30 分です。
信頼済み IP 範囲を使用	IP アドレスフィルタリングを有効にします。 IP アドレスフィルタリングは、信頼済み IP アドレス範囲とアカウントパスワードを使用し、未認証のユーザーが組織にアクセスできないようにします。IP アドレスフィルタリングを有効にすると、有効なログインのあるユーザーに、信頼済み IP アドレス範囲内の IP アドレスも必要になります。そうでない場合、そのユーザーは組織にログインできなくなります。 このオプションを有効にした場合は、1 つ以上の信頼済み IP アドレス範囲も入力する必要があります。
許可された信頼済み IP 範囲	組織にアクセスするためのログインに使用可能な信頼済み IP アドレス範囲。Informatica Intelligent Cloud Services では、IP version 4 (IPv4) と IP version 6 (IPv6) での IP アドレス形式がサポートされています。 IP アドレスフィルタリングを有効にすると、信頼済み IP アドレス範囲のフィールドが表示されます。追加のアドレス範囲を入力するには、 <b>[+]</b> をクリックします。 <b>注:</b> 無効な IP アドレス範囲を入力した場合、ユーザーは組織にアクセスできません。有効な IP アドレス範囲については、ネットワーク管理者にお問い合わせください。

## 接続プロパティの保存場所

組織およびサブ組織の接続プロパティを保存する場所を設定できます。接続プロパティの保存場所を指定するには、**【組織】** ページで **【接続の資格情報】** を設定します。

接続プロパティは、次のいずれかの場所に保存できます。

### Informatica Cloud

Informatica Intelligent Cloud Services を使用して接続プロパティを保存した場合は、接続プロパティをいつでも利用できます。Informatica Intelligent Cloud Services では、標準のバックアップ手順の一環として、接続プロパティを定期的にバックアップします。

### ローカルの Secure Agent

ファイアウォール内に存在する接続プロパティが必要な場合は、ローカルな Secure Agent を使用して接続プロパティを格納できます。ローカルの Secure Agent との接続プロパティを保存するには、組織に接続の外部化ライセンスが必要です。このオプションを有効にすると、**【接続】** ページにリストされているすべての接続のプロパティがローカルのエージェントに保存されます。

1つの Secure Agent で複数の接続プロパティを保存できます。接続プロパティは次のディレクトリに格納されます。

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

ローカルな Secure Agent を使用してプロパティを格納する場合は、タスクを実行し、ユーザーが接続を操作できるように、Secure Agent を実行する必要があります。データの損失を回避するために、接続プロパティを定期的にバックアップします。ベストプラクティスとして、接続プロパティの場所または暗号化キーを変更した後に接続プロパティをバックアップすることをお勧めします。

Informatica Intelligent Cloud Services は、CBS (Cipher Blocker Chaining) モードの 128 AES 暗号化を使用して接続を保存します。

Informatica Intelligent Cloud Services では、暗号化キーを生成して、Secure Agent を使用して格納された接続プロパティの安全性を確保します。ランダムに生成されたパスワードを使用することも、暗号化キーの基盤としてカスタムパスワードを入力することもできます。

暗号化キーを定期的に更新する場合は、カスタムパスワードを使用します。暗号化キーを更新するときに、カスタムパスワードを変更できます。

接続プロパティを格納する場所を変更できます。これにより、Informatica Intelligent Cloud Services は、接続プロパティを適切な場所に移動します。例えば、ライセンスの有効期限が切れるため、クラウドに接続を格納するように組織を設定するとします。Informatica Intelligent Cloud Services は、ローカルな Secure Agent から Informatica Intelligent Cloud Services へ接続プロパティを移動します。

**注:** FedRAMP の対象となる組織の場合、接続プロパティをローカルの Secure Agent に保存することはできません。

## データ統合サービスのプロパティ

データ統合サービスプロパティはデータ統合で使用されます。次のプロパティを設定して、ジョブの通知に使用するタイムゾーンと電子メールアドレスを設定します。

以下のデータ統合サービスのプロパティを設定できます。

## ジョブのプロパティ

次の表に、ジョブのプロパティを示します。

プロパティ	説明
スケジュールオフセット	標準の予定開始時刻でのサーバーのオーバーロードを防ぐために、予定開始時刻に追加されるわずかな時間。組織には、すべてのスケジュールに適用される単一のスケジュールオフセットがあります。スケジュールオフセットは、手動で開始されたタスクまたはタスクフローの開始時刻には影響しません。スケジュールオフセットは変更できません。スケジュールの詳細には表示されませんが、組織のスケジュールオフセットはすべてのスケジュールに設定した時間範囲に追加されます。これにより、スケジュール済みのタスクが想定どおりの頻度で実行されるようになります。例えば、8:00 a.m.から 12:00 p.m.まで毎時間タスクを実行するようにスケジュールを設定し、組織のスケジュールオフセットを 15 秒とすると、そのスケジュールで、8:00:15、9:00:15、10:00:15、11:00:15、および 12:00:15 にタスクが実行されます。
時間帯	電子メール通知でのジョブ実行タイムスタンプの表示に使用するタイムゾーン。

### デフォルトの電子メール通知プロパティ

ジョブの失敗、警告、および成功メッセージに使用するデフォルトの電子メールアドレスを設定するための電子メール通知プロパティを構成します。有効な電子メールアドレスを1つ以上入力します。カンマ (,) またはセミコロン (;) を使用して電子メールアドレスを区切ります。

また、タスクレベルで電子メール通知のプロパティを設定することもできます。タスクまたはタスクフローで電子メール通知を設定すると、Informatica Intelligent Cloud Services は、組織に対して設定されたアドレスではなく、タスクまたはタスクフローのアドレスに電子メールを送信します。

## CLAIRE の推奨設定

CLAIRE の推奨を有効にすると、ご自身の会社のアセットまたはその他の Informatica Intelligent Cloud Services 組織のアセットのメタデータの分析に基づいたマッピングデザインに対する製品内の推奨事項が許可されます。CLAIRE エンジンによって収集され処理されたメタデータは匿名です。

CLAIRE の推奨はデフォルトで「有効」に設定されています。CLAIRE の推奨を無効にすると、会社内のすべてのユーザーに対して推奨が無効になります。会社では推奨をいつでも有効または無効にする事ができます。

下位組織の CLAIRE の推奨は、下位組織内から有効および無効にします。

CLAIRE の推奨を有効にすると、データ統合ユーザーは個々のマッピングの推奨をマッピングデザイナーで無効にできます。

詳細モードのマッピングに基づくマッピングタスクを作成する場合は、CLAIRE の推奨を有効にして CLAIRE チューニングを使用できます。

## Enterprise Data Catalog 統合プロパティ

Azure のデータアクセラレータを使用している場合、またはデータ統合でデータカタログ検出を使用している場合、組織およびサブ組織に Enterprise Data Catalog 統合プロパティを設定できます。ユーザーがマッピング、同期タスク、ファイル取り込みタスク、および Azure のデータ同期タスクでカタログアセットを使用できるように、Enterprise Data Catalog 統合プロパティを設定します。

組織に設定する Enterprise Data Catalog 統合プロパティは、組織の全ユーザーが実行するデータカタログ検索に適用されます。組織にサブ組織が含まれる場合は、親組織と各サブ組織に異なる Enterprise Data Catalog 統合プロパティを設定できます。

以下の表に、Enterprise Data Catalog 統合プロパティを示します。

プロパティ	説明
カタログ URL	Enterprise Data Catalog サービスの URL。次の形式を使用します。 http://<完全修飾ホスト名>:<ポート> URL の最後に「/ldmcatalog」を追加しないでください。
ランタイム環境	Enterprise Data Catalog からのデータの読み取りに使用する Secure Agent グループの名前。 選択したグループのエージェントは、Enterprise Data Catalog と通信できる必要があります。このため、Enterprise Data Catalog ホストがエージェントマシンと同じネットワーク内に存在するか、通信用の適切なポートが開かれている必要があります。
ユーザー名	Secure Agent が Enterprise Data Catalog にアクセスするために使用する Enterprise Data Catalog ユーザーアカウント。 このユーザーアカウントは、Enterprise Data Catalog 内のオブジェクトを表示および検索し、Enterprise Data Catalog REST API を使用して機能を実行する権限を持っている必要があります。
パスワード	Enterprise Data Catalog ユーザーアカウントのパスワード。
データカタログを表示	<b>データ統合</b> のデータ統合ページを表示および非表示にします。

## サブ組織

組織に適切なライセンスがある場合は、組織内に 1 つ以上のサブ組織を作成できます。企業内のさまざまなビジネス環境を表すサブ組織を作成します。例えば、開発、テスト、およびプロダクション環境を表す個別のサブ組織を作成することができます。

プロダクション組織、追加プロダクション組織、またはサンドボックス組織からサブ組織を作成できます。

サブ組織を作成すると、サブ組織を作成するために使用する組織が親組織になります。各サブ組織の親組織は 1 つのみで、別のサブ組織を含めることはできません。

組織のライセンスは、作成できるサブ組織の数を制御します。この数を増やすには、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。

サブ組織の作成には、次の利点があります。

**サブ組織のライセンスは、個別に管理するか、親組織のライセンスと自動的に同期できます。**

各サブ組織は、サブ組織を作成するためのライセンスとバンドルライセンスを除く、親組織からのすべての機能、コネクタ、およびカスタムライセンスを継承します。

ライセンスを個別に管理すると、親組織の管理者は、サブ組織が継承するライセンスの有効期限の無効化、有効化、および変更を行うことができます。各サブ組織のライセンスを個別に設定します。したがって、あるサブ組織でライセンスを無効にしても、他のサブ組織のライセンスは無効になりません。

または、適切なライセンスを所有している場合、サブ組織のライセンスを親組織と自動的に同期できます。このライセンスを有効にすると、ライセンスが親組織で変更されるたびに、すべてのサブ組織はライセンスの変更を継承します。

### ユーザーとアセットを個別に管理できます。

各サブ組織には、ユーザーとアセットの独自のセットがあります。

サブ組織で作成するユーザーは、サブ組織に固有のもので、親組織や他のサブ組織にはログインできません。親組織の管理者と、サブ組織のアクセス特権を持つ親組織のユーザーのみが、親組織およびすべてのサブ組織にアクセスできます。

マッピングやタスクなどのアセットも組織内で固有のもので、アセットは、サブ組織間、または親組織と任意のサブ組織間では共有されません。組織間でアセットを移行する場合は、片方の組織からアセットをエクスポートし、別の組織にインポートします。

### ランタイム環境を共有できます。

親組織の管理者は、Secure Agent グループをサブ組織と共有できます。Secure Agent グループを共有すると、サブ組織のユーザーは、グループ内の Secure Agent でタスクを実行できます。

アプリケーションの統合、一括取り込みアプリケーション、および一括取り込みデータベースは、サブ組織間で Secure Agent の共有をサポートしません。親組織またはサブ組織のユーザーは、その組織またはサブ組織に属する Secure Agent のみを使用できます。サブ組織のユーザーは、親組織に属する Secure Agent を使用することはできません。

### ログインせずに組織間を切り替えることができます。

サブ組織を表示する特権を持つ親組織のユーザーは、ログアウトせずに組織間を切り替えたり、Informatica Intelligent Cloud Services にログインし直したりすることができます。

### サブ組織の例

同期タスクの開発、テスト、およびプロダクションのための個別の環境が必要であり、タスクはプロダクション環境で実行される前に必ずテストを行います。

管理者として親組織にログインし、タスク開発用のサブ組織、テスト用のサブ組織、およびプロダクション用のサブ組織を作成します。サブ組織にユーザーを追加し、組織ごとにデータ同期ライセンスが有効になっていることを確認します。

タスクの開発が完了したら、開発サブ組織からタスクをエクスポートし、テスト用のサブ組織にログインしてタスクをインポートします。テストが完了したら、テスト用のサブ組織からタスクをエクスポートし、プロダクション用のサブ組織にログインしてタスクをインポートします。

## サブ組織の追加

サブ組織を追加するには、新しいサブ組織を作成するか、既存の組織をリンクします。

次のいずれかの方法でサブ組織を追加できます。

#### サブ組織の作成。

親組織にする組織にログインし、サブ組織を作成します。新しいサブ組織は、親組織に自動的にリンクされます。

#### 既存の組織のリンク。

リンク元の組織が親組織になり、リンク先の組織がサブ組織になります。

### サブ組織の作成

親組織の管理者はサブ組織を作成できます。

1. 親組織にする組織にログインします。
2. 管理者を開いて **[組織]** を選択します。

3. **【サブ組織】** タブを開き、**【新しいサブ組織】** をクリックします。
4. サブ組織のプロパティを入力し、**【保存】** をクリックします。

サブ組織を作成したら、ライセンスを確認し、他の人が使用できるようにランタイム環境、ユーザーアカウント、および接続を構成します。

## 組織のリンク

既存の組織をリンクすることで、サブ組織を作成できます。リンク元の組織が親組織になり、リンク先の組織がサブ組織になります。

組織をリンクするには、リンクする組織の組織 ID が必要になります。この情報は、**【組織】** ページで確認できます。

**注:** 親組織が持っていないライセンスを持つサブ組織をリンクすると、サブ組織はそのライセンスを失います。

次のすべての条件が該当する場合に、組織をリンクできます。

- ユーザーアカウントと組織があること。
- 組織は別の組織の親でもサブ組織でもありません。
- 親組織の管理者であること、およびサブ組織を作成するためのライセンスが親組織にあること。
- サブ組織としてリンクする組織に、サブ組織を作成するためのライセンスがないこと。

後から組織をリンク解除できます。

組織をリンクするには:

1. 親組織にする組織にログインします。
2. 管理者を開いて **【組織】** を選択します。
3. **【サブ組織】** タブを開き、**【サブ組織をリンク】** をクリックします。
4. **【サブ組織をリンク】** ダイアログボックスで、次の情報を入力します。
  - リンクする組織の組織 ID。
  - サブ組織として設定する組織の管理者のユーザー名とパスワード。
5. 組織をリンクするには、**【サブ組織をリンク】** をクリックします。  
組織が **【サブ組織】** ページに表示されます。

## サブ組織の削除

サブ組織を削除するには、組織のリンクを解除するか、サブ組織を削除します。

次のいずれかの方法でサブ組織を削除できます。

### 親組織からの既存サブ組織のリンク解除。

リンクされていないサブ組織は、スタンドアロン組織になります。スタンドアロン組織は、別の親組織にリンクすることや元の親組織に再リンクすることができます。リンクされていない組織について、サブ組織を作成するためのライセンスを取得すると、それを別のサブ組織の親組織にすることができます。

### サブ組織の削除。

組織を削除すると、その組織に関連付けられたすべてのアセットとデータが削除されます。

## サブ組織のリンク解除

親組織からサブ組織のリンクを解除することができます。組織のリンクを解除した後は、別の親組織にリンクする予定がある場合を除いて、リンク解除した組織を必要なライセンスで更新します。

次のすべての条件に当てはまる場合は、サブ組織のリンクを解除できます。

- リンク解除するサブ組織に対する管理者アカウントを持っていること。
- 親組織の管理者であること、およびサブ組織を作成するためのライセンスが親組織にあること。
- リンクを解除するサブ組織内のアセットは、Secure Agent グループの共有をランタイム環境として使用しません。サブ組織内の任意のアセットが Secure Agent グループの共有をランタイム環境として使用している場合は、サブ組織のリンクを解除する前に、別のランタイム環境を使用するようにアセットを更新します。

**注:** この条件は一括取り込みアプリケーションと一括取り込みデータベースには適用されません。これは、一括取り込みアプリケーションと一括取り込みデータベースは共有ランタイム環境をサポートしていないためです。

サブ組織のリンクを解除するには:

1. 親組織にログインします。
2. 管理者を開いて **[組織]** を選択します。
3. **[サブ組織]** タブを開きます。
4. リンクを解除するサブ組織の **[アクション]** メニューを展開し、**[リンク解除]** を選択します。
5. **[リンク解除]** ダイアログボックスで、管理者ロールを持つサブ組織内のユーザーのユーザー名とパスワードを入力します。
6. **[リンク解除]** をクリックします。  
サブ組織が、親組織からリンク解除されます。

## サブ組織の削除

サブ組織を削除できます。サブ組織を削除すると、関連付けられたすべてのデータが削除されます。使用量ベースのライセンスをお持ちの場合、サブ組織のメタリング情報は親組織に保持されます。

親組織の管理者であれば、サブ組織を削除できます。

1. 親組織にログインします。
2. 管理者を開いて **[組織]** を選択します。
3. **[サブ組織]** タブを開きます。
4. リンクを解除するサブ組織の **[アクション]** メニューを展開し、**[削除]** を選択します。

## サブ組織の無効化または有効化

親組織の管理者である場合は、サブ組織を無効または有効にできます。

サブ組織の作成時に、デフォルトでサブ組織は有効化されます。サブ組織と別個の使用許諾契約がある場合や、使用許諾契約の有効期限が切れた場合、サブ組織を無効にすることがあります。サブ組織は、無効化後に再度有効にできます。

サブ組織は、サブ組織の管理者がサブ組織への親組織のアクセスをブロックしている場合も、無効または有効にできます。

次のアクションを実行できます。

### サブ組織の無効化

サブ組織を無効にすると、その組織は残りますが、サブ組織のユーザーはサブ組織にログインできない、または REST API を介してサブ組織にアクセスします。サブ組織内のスケジュールされたジョブは実行されません。

### サブ組織の有効化

サブ組織を有効にすると、サブ組織のユーザーはサブ組織にログインでき、自分のユーザーロールに基づいてアセットにアクセスし、タスクを実行できます。適切な権限を持つユーザーは、REST API を介してサブ組織にアクセスできます。スケジュールされたジョブは、スケジュールに従って再開されます。

サブ組織を [組織] ページの [サブ組織] タブで無効または有効にします。サブ組織の [アクション] メニューで、[無効] または [有効] を選択します。

## 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。

## サブ組織への親組織のアクセスを拒否

サブ組織の管理者である場合は、サブ組織への親組織のアクセスを拒否できます。

サブ組織へのアクセスを拒否すると、親組織のユーザーは、親組織からサブ組織に切り替えられません。適切な権限を所有する親組織のユーザーは、サブ組織に次の変更のみを加えることができます。

- サブ組織の有効化および無効化
- サブ組織のライセンスの更新
- 組織の説明や CLAIRE の推奨設定などのサブ組織のプロパティの編集

親組織のサブ組織へのアクセスを拒否するには、管理者としてサブ組織にログインします。[組織] ページで、[このサブ組織への親組織のアクセスを拒否] オプションを有効にします。

## サブ組織のアドオンコネクタ

サブ組織でアドオンコネクタを使用するには、親組織にコネクタをインストールする必要があります。サブ組織にアドオンコネクタをインストールすることはできません。

サブ組織は、親組織からすべてのコネクタライセンスを継承します。サブ組織で特定のコネクタを使用しない場合は、サブ組織のコネクタライセンスを無効にします。サブ組織のライセンスの編集と無効化に関する詳細については、[「サブ組織のライセンスの編集」](#) (ページ 27) を参照してください。

## サブ組織でのアセットのエクスポートとインポート

サブ組織では、次の方法でアセットをエクスポートおよびインポートします。

- サブ組織にログインして、サブ組織からアセットをエクスポートおよびインポートします。
- 親組織の管理者は親組織にログインし、サブ組織に切り替えて、データ統合アセットをインポートまたはエクスポートできます。

**注:** この条件は、タスクフローとアプリケーション統合アセットには適用されません。

## 追加プロダクション組織とサンドボックス組織

組織に適切なライセンスがある場合は、プロダクション組織から追加プロダクション組織とサンドボックス組織を作成できます。これらの組織は、アセットやユーザーごとに別の組織を用意しつつ、すべてのIPUの使用状況をプロダクション組織から管理する場合に作成します。追加プロダクション組織とサンドボックス組織は、プロダクション組織に自動的にリンクされます。

以下のタイプの組織を作成できます。

### 追加プロダクション組織

これは別個のプロダクション組織です。これは、プロダクション組織と同じように機能します。ただし、追加プロダクション組織から、さらに追加プロダクション組織やサンドボックス組織を作成することはできません。

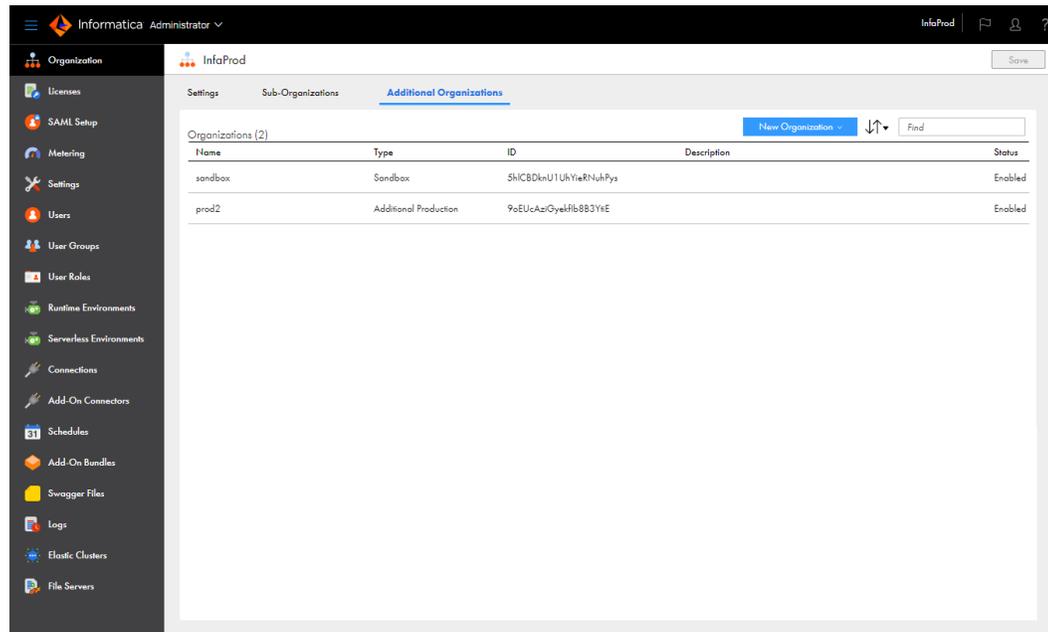
### サンドボックス組織

これは、アセットの開発とテストに通常使用される組織です。サンドボックス組織と追加プロダクション組織との間に、機能上の違いはありません。

追加プロダクション組織とサンドボックス組織は、プロダクション組織からは相互に完全に独立しています。これらが、アセット、接続、ランタイム環境、またはユーザーを共有することはありません。ただし、これらの中でアセットをエクスポートおよびインポートすることはできます。

作成する追加プロダクション組織とサンドボックス組織は、プロダクション組織からすべてのライセンスとエディションを継承します。プロダクション組織が、サブ組織を作成するライセンスを持っている場合、追加プロダクション組織とサンドボックス組織の管理者は、組織のサブ組織を作成できます。

追加プロダクション組織とサンドボックス組織は、プロダクション組織の【組織】 ページにある【追加組織】 タブに表示されます。次の画像は、【追加組織】 タブを示しています。



追加プロダクション組織またはサンドボックス組織を作成するときは、組織名と組織管理者のユーザー名を入力する必要があります。このユーザーアカウントを使用して新しい組織にログインし、他のユーザーやアセットを追加できます。

追加プロダクション組織またはサンドボックス組織を作成した後、これらを無効にしたり削除したりすることはできません。また、プロダクション組織からリンクを解除することもできません。これを行う必要がある場合は、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。

## 追加の組織の作成

【組織】 ページの【追加組織】 タブで、追加プロダクション組織またはサンドボックス組織を作成します。

**注:** 追加プロダクション組織またはサンドボックス組織を作成すると、組織に対して追加の IPU 料金が発生する場合があります。

1. プロダクション組織にログインします。
2. 管理者を開いて【組織】を選択します。
3. 【追加組織】タブを開きます。
4. 【新しい組織】をクリックし、【追加プロダクション組織】または【サンドボックス組織】を選択します。
5. 【新しい組織】 ページで、新しい組織の管理者のユーザー名と組織名を入力します。  
ユーザー名は一意にする必要があります。これは、有効な電子メールアドレスにするか、英数字、ハイフン、アンダースコア、ピリオド、アポストロフィーのみで構成します。
6. 必要に応じて、説明、従業員数、および住所情報を入力します。
7. 【保存】をクリックします。  
【追加組織】タブに新しい組織が表示され、ステータスが【有効】になります。Informatica Intelligent Cloud Services から、新しい組織管理者向けのウェルカムメールが電子メールアドレスに送信されます。
8. プロダクション組織からログアウトします。

9. ウェルカムメールにある [アカウントの確認] リンクをクリックし、プロンプトに従って、新しい組織管理者のアカウントをアクティブ化します。

アカウントのアクティブ化が完了したら、Informatica Intelligent Cloud Services により、新しい組織へのログインが実行されます。

新しい組織にログインした後は、他のユーザーを追加して、ランタイム環境、接続、およびアセットを作成できます。

## 第 3 章

# ライセンス

ライセンスによって組織の Informatica Intelligent Cloud Services サブスクリプションレベルが決まり、Informatica Intelligent Cloud Services の機能、コネクタ、およびバンドルへアクセスできるようになります。

管理者は、組織に設定されたライセンスの確認、ライセンスの有効期限の確認、および下位組織のライセンスの管理ができます。

ライセンスされたジョブの制限と使用量のメトリックを確認することもできます。メトリックの確認については、[第 4 章、「メータリング」 \(ページ 29\)](#)を参照してください。

## ライセンスのカテゴリ

ライセンスは、エディションライセンス、コネクタライセンス、およびカスタムライセンスに分類されます。次のライセンスカテゴリを利用できます。

### エディションライセンス

エディションライセンスは、機能ベースまたは使用量ベースとなります。機能ベースのエディションライセンスは、データ統合マッピングタスク、ビジネスサービスコンポーネント、きめ細かいセキュリティなどの Informatica Intelligent Cloud Services 機能へのアクセスを提供します。インテリジェントクラウドデータ管理機能のライセンスなどの使用量ベースのエディションライセンスは、前払い式の消費モデルを使用して Informatica Intelligent Cloud Services へのアクセスを提供します。

### コネクタライセンス

コネクタライセンスは、Amazon Redshift、Microsoft SQL Server、Oracle などのエンティティへの接続を提供します。

### カスタムライセンス

カスタムライセンスは、エディションに含まれていないライセンスです。機能、パッケージ、またはバンドルへのアクセスを提供します。エディションライセンスにも含まれている機能へのアクセスを提供するカスタムライセンスを組織で使用している場合、カスタムライセンスの使用条件は、エディションライセンスの条件を上書きします。

# ライセンスのタイプ

組織を作成すると、Informatica Intelligent Cloud Services でライセンスされている各エディションのライセンスタイプを組織に割り当てます。

Informatica Intelligent Cloud Services では、以下のタイプのライセンスを使用します。

## トライアル

30 日間無料でエディションを使用できます。トライアル期間の終了時に、エディションをサブスクライブできます。トライアルサブスクリプションでは、ライセンスに関連付けられている機能、コネクタ、およびパッケージへのアクセスが制限される場合があります。

## サブスクリプション

契約期間中は、ライセンスされているエディションを使用することができます。契約期間の終わりに近づくと、Informatica Intelligent Cloud Services から契約が間もなく終了することが通知されます。エディションの使用を続けるには、契約を更新します。

## 無料サブスクリプション

同期タスクは、無料で使用できます。無料サブスクリプションでは、同期タスクの機能へのアクセスが制限される場合があります。

# サブ組織のライセンス

サブ組織には、親組織によって保持されるライセンスがあります。親組織に属していないライセンスをサブ組織が必要とする場合は、Informatica グローバルカスタマサポートに連絡して、親組織のライセンスを取得します。

サブ組織を作成すると、各サブ組織は親組織からカスタムライセンスとしてライセンスを継承します。サブ組織は、次のライセンスを除くすべてのライセンスを継承します。

- サブ組織を作成するためのライセンス
- バンドルライセンスサブ組織でバンドルを使用するには、サブ組織のユーザーがバンドルをインストールする必要があります。

組織がインテリジェントクラウドデータ管理ライセンスを持っている場合、サブ組織でもこのライセンスを利用できます。親組織とサブ組織は、Informatica プロセッシングユニット (IPU) のバランスを共有します。

サブ組織のライセンスは、次の方法で管理できます。

## ライセンスの個別管理

ライセンスを個別に管理すると、親組織の管理者は、継承されたライセンスの有効期限の無効化、有効化、および短縮を行うことができます。各サブ組織のライセンスを個別に管理します。サブ組織の管理者はライセンスを表示できますが、変更はできません。

これがデフォルトのオプションです。

## サブ組織のライセンスの親組織との自動同期

適切なライセンスを所有している場合、サブ組織のライセンスを親組織と自動的に同期できます。このライセンスを有効にすると、ライセンスが親組織で変更されるたびに、すべてのサブ組織はライセンスの変更を継承します。

ライセンスの同期は、組織に多数のサブ組織があり、サブ組織が同じライセンスを所有しているときに有効にすることがあります。

ライセンスの同期が組織に対して有効でない場合、サブ組織のライセンスを個別に管理する必要があります。

**注:** 親組織が持っていないライセンスを持つサブ組織をリンクすると、サブ組織はそのライセンスを失います。

## サブ組織のライセンスの編集

親組織の管理者であり、親組織とサブ組織との間のライセンス同期が有効でない場合、サブ組織のライセンスを編集できます。サブ組織のライセンスは、親組織内またはサブ組織内から編集できます。

1. 親組織にログインします。
2. 親組織内からライセンスを編集するには:
  - a. 管理者を開いて **【組織】** を選択します。
  - b. **【サブ組織】** をクリックします。
  - c. ライセンスを編集するサブ組織を選択します。
  - d. **【ライセンス】** をクリックします。
3. サブ組織内からライセンスを編集するには:
  - a. 右上隅の **【組織】** メニューから、ライセンスを編集するサブ組織を選択します。
  - b. 管理者を開いて **【ライセンス】** を選択します。
4. 機能を有効にするにはライセンスを選択し、機能を無効にするにはライセンスの選択を解除します。
5. 必要に応じて、有効期限を変更します。

すべてのライセンスには有効期限が必要です。元の有効期限を過ぎたライセンスを延長することはできません。
6. **【保存】** をクリックします。

## 親組織とのライセンスの同期

サブ組織のライセンスを親組織と自動的に同期できます。ライセンスが親組織で変更されるたびに、すべてのサブ組織はライセンスの変更を継承します。

ライセンスの同期を有効にするには、Informatica グローバルカスタマサポートに問い合わせ、この機能のライセンスを要求してください。ライセンスが親組織に対して有効になると、ライセンスのサブ組織との同期が自動的に発生します。親組織の管理者は、ライセンスを同期させるために、何か操作をする必要はありません。

**注:** この機能のライセンスが有効になると、サブ組織のライセンスを個別に編集することはできません。

この機能のライセンスが有効になり、サブ組織を無効にすると、サブ組織はライセンス設定を失います。サブ組織を再度有効にした場合、サブ組織はすべてのライセンス設定を親組織から継承します。

親組織とサブ組織との間のライセンス同期は、サブ組織のライセンスメーターカウントには影響しません。

## 組織タイプの設定

**【ライセンス】** ページを表示すると、組織のライセンスに関する詳細や、組織タイプなどのその他の詳細を確認できます。組織タイプは、組織がトライアル組織、プロダクション組織、またはサンドボックス組織のいずれであるかを表します。親組織の管理者である場合は、それぞれのサブ組織の組織タイプを設定する必要があります。

組織タイプは、親組織の管理者がサブ組織の **【ライセンス】** ページを表示することで編集できます。サブ組織のユーザーまたは親組織では編集できません。

親組織の管理者の場合は、親組織内またはサブ組織内からサブ組織の組織タイプを設定できます。組織タイプは設定後に変更できます。

1. 親組織にログインします。
2. 親組織内から組織タイプを編集する手順
  - a. 管理者を開いて **【組織】** を選択します。
  - b. **【サブ組織】** をクリックします。
  - c. タイプを設定するサブ組織を選択します。
  - d. **【ライセンス】** をクリックします。
  - e. [サブ組織の詳細] 領域の **【タイプ】** リストで、組織タイプを選択します。
3. サブ組織内から組織タイプを編集する手順
  - a. 右上隅の **【組織】** メニューから、タイプを設定するサブ組織を選択します。
  - b. 管理者を開いて **【ライセンス】** を選択します。
  - c. [サブ組織の詳細] 領域の **【タイプ】** リストで、組織タイプを選択します。
4. **【保存】** をクリックします。

## ライセンスの有効期限

ライセンスの有効期限が切れると、ライセンスに関連付けられている機能、コネクタ、またはパッケージにアクセスできなくなります。ライセンスに関連付けられているスケジュール済みのジョブも無効になります。組織のすべてのライセンスの有効期限が切れると、Informatica Intelligent Cloud Services にログインできなくなります。

管理者の **【ライセンス】** ページでライセンスの有効期限を確認することができます。ライセンスを延長するには、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。ライセンスを延長すると、関連付けられている機能、コネクタ、およびパッケージにアクセスし、スケジュール済みのジョブの処理を再開できます。

## 第 4 章

# メータリング

組織およびサブ組織のメータリング情報を表示できます。メータリング情報は【メータリング】ページに表示されます。

機能ベースのライセンスを持っている場合、【メータリング】ページには、組織が使用したコンピューティングリソースの量および残りのコンピューティングリソースの量が表示されます。また、ページには、組織のライセンスを通じて設定された使用制限が表示されます。【メータリング】ページには、ライセンスに基づいて、ダッシュボードまたはテーブルとして情報が表示されます。

使用量ベースのライセンスを持っている場合、【メータリング】ページには、現在の請求サイクルに購入、消費した Informatica プロセッシングユニット (IPU) の数と、残りの IPU 数を含むダッシュボードが表示されます。各サービスに対する使用済みの IPU の数を示すメーターを表示することもできます。

## 機能ベースのライセンスメーター

組織に機能ベースのライセンスがある場合、【メータリング】ページには、ライセンスに基づいた情報が表示されます。

【メータリング】ページには、ライセンスされた機能に応じて次のビューが表示されます。

### ダッシュボードビュー

適切なライセンスがある場合、【メータリング】ページのダッシュボードビューに情報が表示されます。

[今月のメトリック概要] 領域には、その月の残りの合計コンピューティングリソースと各メータータイプが表示されます。組織のエディションに応じて、組織に適用されるすべてのメーターの表を表示することもできます。

それぞれのメータータイプの詳細領域には、残りのリソース量、1日あたりの平均リソース使用量、残りの使用日数など、その月のメーター情報が表示されます。メータータイプの詳細を表示するには、組織またはサブ組織、日付範囲、およびプロジェクトまたはランタイム環境ごとのデータ量の使用状況を示す詳しいグラフを表示できます。

### ライセンスメトリックビュー

ダッシュボードビューの表示に必要なライセンスがない場合は、【メータリング】ページにはライセンスメトリックのテーブルが表示されます。この表には、組織に適用されるすべてのメーターの概要メトリックがリストされ、これは組織のエディションに応じて異なります。ダッシュボードビューの概要領域から、すべてのメーターの [ライセンスメトリック] ビューに移動することもできます。

## ライセンスメトリックの表示

組織で使用しているすべてのメーターのテーブルを表示し、メータリング使用状況を示すレポートをダウンロードできます。[メータリング] ページのライセンスメトリックビューからテーブルを表示し、レポートをダウンロードします。

ダッシュボードビューからライセンスメトリックビューを開くには、[メトリックサマリ - 今月] 領域の [すべてのメーター] をクリックします。ダッシュボードビューの表示に必要なライセンスがない場合は、[メータリング] ページを開くとライセンスメトリックビューが表示されます。

ライセンスメトリックビューに表示されるメーターは、組織が使用しているエディションによって決まります。また、組織にはカスタムメーターも割り当てられる場合があります。メータリング情報はすべてのエディションで使用できない場合があります。

組織で複数のエディションを使用している場合、またはカスタムメーターを使用している場合、1つのメーターが異なる制限で複数回表示されることがあります。この場合、最新の制限が適用されます。例えば、あるエディションの同期ジョブが1日500個に制限され、別のエディションの同期ジョブが1日に100個に制限されている場合、1日のジョブは500個に制限されます。[有効] カラムに適用した制限が表示されます。

ライセンスメトリックビューには、メーターごとに以下の情報が表示されます。

プロパティ	説明
エディション	メーターに関連付けられているエディションの名前。
サービス	メーターが適用されるサービス。
メータリング	メーターの名前。例えば、1日あたりの同期ジョブの数、マッピングジョブによって処理された1か月あたりの行数、またはレプリケーションジョブの総数です。一括取り込みの場合、このカラムには次の取り込みタイプが表示されます: 一括取り込みファイル、一括取り込みアプリケーション、一括取り込みデータベース、一括取り込みアプリケーション - 変更データキャプチャ、一括取り込みデータベース - 変更データキャプチャ、および一括取り込みストリーミング。
制限	ジョブまたは処理した行の最大数などの制限数。 この制限は親組織と各サブ組織に適用されます。例えば、1日あたりのジョブが100個に制限された場合、親組織が実行できるジョブは1日100個、各サブ組織が実行できるジョブも1日100個になります。 このフィールドに-1が表示された場合、制限はありません。
使用中	使用された実際のユニット数。組織またはサブ組織でメータリング期間に実行されるジョブ数または使用される計算時間などがあります。
使用済みの割合	組織またはサブ組織でメータリング期間に使用されたユニットの割合。
有効	組織またはサブ組織でメーターが有効かどうかを示します。

## メーター定義

[メータリング] ページの [ライセンスメトリック] ビューに表示されるメーターは、組織が使用しているエディションによって決まります。

次の表に、エディションに基づいて効力がある可能性があるメーターについて説明します。

メーター	定義
エージェントの総数	停止したエージェントを含む、Secure Agents の合計数。 Informatica Cloud Hosted Agent は含みません。
接続の総数	接続の総数。
プロジェクトの総数	プロジェクトの総数。
フォルダの総数	フォルダの総数。
日次/月間受信 API 要求最大	日次または月間の API アクセス要求の数。
日次/月間のマッピングジョブの数	日次または月間のマッピングジョブの数。*
マッピングジョブの総数	マッピングジョブの総数。*
日次/月間のマッピングジョブが処理した行数	日次または月間のマッピングジョブが処理した行数。*
マッピングジョブが処理した行の総数	マッピングジョブが処理した行の総数。*
日次/月間のマスキングジョブの数	日次または月間のマスキングジョブの数。
マスキングジョブの総数	マスキングジョブの総数。
日次/月間のマスキングジョブが処理した行数	日次または月間のマスキングジョブが処理した行数。
マスキングジョブが処理した行の総数	マスキングジョブが処理した行の総数。
日次/月間の PowerCenter ジョブの数	日次または月間の PowerCenter ジョブの数。
PowerCenter ジョブの総数	PowerCenter ジョブの総数。
日次/月間の PowerCenter ジョブが処理した行数	日次または月間の PowerCenter ジョブが処理した行数。
PowerCenter ジョブが処理した行の総数	PowerCenter ジョブが処理した行の総数。
日次/月間のレプリケーションジョブの数	日次または月間のレプリケーションジョブの数。
レプリケーションジョブの総数	レプリケーションジョブの総数。
日次/月間のレプリケーションジョブが処理した行数	日次または月間のレプリケーションジョブが処理した行数。
レプリケーションジョブが処理した行の総数	レプリケーションジョブが処理した行の総数。

メーター	定義
一括取り込みメーター	一括取り込みアプリケーション、一括取り込みデータベース、一括取り込みファイル、および一括取り込みストリーミングの場合は、アプリケーション取り込み、データベース統合、ファイル取り込み、またはストリーミング統合ジョブによって1か月の間に取り込まれたギガバイト (GB) の数。一括取り込みアプリケーション - 変更データキャプチャと一括取り込みデータベース - 変更データキャプチャの場合、取り込まれた行数。
日次/月間の同期ジョブの数	日次または月間の同期ジョブの数。
同期ジョブの総数	同期ジョブの総数。
日次/月間の同期ジョブが処理した行数	日次または月間の同期ジョブが処理した行数。
同期ジョブが処理した行の総数	同期ジョブが処理した行の総数。
サブ組織の数	サブ組織の数。サブ組織を削除した場合、このメーターには削除したサブ組織が含まれます。
日次の状態同期ジョブの数	日次の状態同期ジョブの数。 状態同期ジョブには、REST API を介して実行する fetchState ジョブおよび loadState ジョブが含まれます。
ユーザー管理作成要求数	ユーザー管理作成要求数。 ユーザー管理作成要求には、ユーザー、ユーザーグループ、カスタムロールの作成のための要求が含まれます。
エラスティッククラスタのノードが使用した計算時間の合計	非推奨。このメーターは、CDI-E コンピューティングの時間数メーターに置き換えられました。
CDI-E コンピューティングの時間数	詳細モードのマッピングに関する、時間単位で測定されるコンピューティングユニット。
サーバーレス CDI-E コンピューティングの時間数	詳細モードのマッピングに関する、時間単位で測定されるサーバーレスコンピューティングユニット。
サーバーレス CDI コンピューティングの時間数	詳細モード外のマッピングに関する、時間単位で測定されるサーバーレスコンピューティングユニット。
使用されたサーバーレスユニットの総数	タスクの実行に使用されたサーバーレスコンピューティングユニットの総数。
処理された CDI 行	詳細モード外でマッピングによって処理された行数。
Data Quality	詳細モード外のマッピングの Data Quality アセットに関する、時間単位で測定されるコンピューティングユニット。
Data Quality エラスティック	詳細モードのマッピングの Data Quality アセットに関する、時間単位で測定されるコンピューティングユニット。
高度なサーバーレスとの Data Quality	詳細モード外のマッピングの Data Quality アセットに関する、時間単位で測定されるサーバーレスコンピューティングユニット。

メーター	定義
高度なサーバーレスとの Data Quality エラスティック	詳細モードのマッピングの Data Quality アセットに関する、時間単位で測定されるサーバーレスコンピューティングユニット。
* 組織が Azure のデータアクセラレータを使用する場合、このメーターには Azure のデータ同期ジョブが含まれます。これは、各 Azure のデータ同期ジョブは基盤マッピングを実行するためです。	

## Data Quality アセットとデータプロファイリングアセットのガイドライン

トランスフォーメーションが Data Quality アセットを読み取る、詳細モード外のマッピングを実行すると、マッピングのトランザクションが Data Quality メーターに記録されます。トランスフォーメーションが Data Quality アセットを読み取る、詳細モードのマッピングを実行すると、マッピングのトランザクションが Data Quality エラスティックメーターに記録されます。

データ統合サーバーでプロファイルを実行すると、プロファイルのトランザクションが Data Quality メーターに記録されます。詳細クラスターでプロファイルを実行すると、プロファイルのトランザクションが Data Quality エラスティックメーターに記録されます。

マッピング内のトランスフォーメーションの出力データをプレビューできます。Data Quality アセットを読み取るトランスフォーメーションでデータをプレビューする場合、Informatica は次の方法でコストを計算します。

- トランスフォーメーションを含むマッピングが詳細モード外で実行されると、Data Quality のコンピューティング時間が消費されます。
- トランスフォーメーションを含むマッピングが詳細モードで実行されると、Data Quality エラスティックのコンピューティング時間が消費されます。

## サーバーレスコンピューティングユニットのメータリング

使用されているサーバーレスコンピューティングユニットの合計を表示すると、メーターには、組織がタスクの実行に使用しているサーバーレスコンピューティングユニットの数に基づいた値が表示されます。

サーバーレスランタイム環境がタスクを実行すると、環境では、タスクが要求するコンピューティングユニットの数に基づいて、リソースを使用して仮想マシンが作成されます。

最小タスク時間は 5 分です。タスクが 5 分未満で完了する場合、サーバーレスランタイム環境は 5 分のコンピューティングユニットを使用します。5 分が経過すると、コンピューティングユニットは 1 秒単位で使用されます。

ジョブをキャンセルすると、使用されるコンピューティングユニットの数は、次のうちの大きい方の値になります。

- キャンセルされる前にジョブが実行されていた時間
- 5 分

## 詳細クラスターのガイドライン

詳細モードのマッピングを実行すると、サーバーレスランタイム環境は、タスクが要求するサーバーレスコンピューティングユニットの数に基づいたリソースを持つ 1 つのワーカーノードを含む詳細クラスターを作成します。別のタスクを実行すると、環境では、アイドル状態のワーカーノードが再利用されるか、ワーカーノードをクラスターに追加して追加のリソースが予約されます。

タスクの実行を開始するとメータリングが開始され、タスクが完了すると終了します。メータリングには、ジョブをコンパイルする時間やクラスターを開始する時間は含まれません。

ジョブのコンパイルに失敗した場合、クラスターの開始に失敗した場合、またはクラスターの開始前にジョブをキャンセルした場合など、クラスターが作成される前にジョブが失敗した場合、メータリングは有効になりません。

## メータリングの使用状況レポート

組織でアプリケーション統合、一括取り込みサービス、詳細クラスタ、またはサーバーレスランタイム環境を使用する場合、メータリングの使用状況レポートをダウンロードできます。

メータリングの使用状況レポートには、次の情報が含まれます。

- アプリケーション統合の場合、レポートには、プロセス、アプリケーション接続、および OData API の実行の詳細が含まれます。アプリケーション統合の高度なサーバーレスランタイム環境の場合、レポートにはプロセスとガイドの実行の詳細が含まれます。
- 一括取り込みアプリケーションと一括取り込みデータベースの場合、レポートのコンテンツは、取り込みジョブのロードタイプによって異なります。初期ロードを実行するジョブの場合、レポートには、取り込まれたデータ量が GB 単位で含まれます。増分ロードを実行するジョブの場合、レポートには、処理されたレコード数または行数が含まれます。初期ロードと増分ロードを組み合わせて実行するジョブの場合は、両方のレポートが含まれます。
- 一括取り込みファイルの場合、レポートには、ファイル取り込みタスクによって取り込まれたデータの量に関する詳細が含まれます。
- 一括取り込みストリーミングの場合、レポートには、ストリーミング統合ジョブによって取り込まれたデータの量に関する詳細が含まれます。
- 詳細クラスタの場合、レポートには、クラスタノードのコンピューティング時間に関する詳細が含まれません。
- サーバーレスランタイム環境の場合、レポートには、タスクを実行するために要求および使用されたサーバーレスコンピューティングユニットの数に関する詳細が含まれます。

組織で一括取り込みアプリケーション、一括取り込みデータベース、一括取り込みファイル、一括取り込みストリーミング、詳細クラスタ、またはサーバーレスランタイム環境を使用していない場合、メータリングの使用状況レポートは使用できません。

### [メトリック概要] からのメータリングの使用状況レポートのダウンロード

[メータリング] ページの [メトリック概要] ビューからメータリングの使用状況レポートをダウンロードします。

1. 管理者で [メータリング] を選択します。
2. ダッシュボードビューが表示された場合は、[メトリックサマリ - 今月] 領域で [すべてのメーター] をクリックして、[ライセンスメトリック] ビューを開きます。
3. [ファイルへエクスポート] をクリックして、[メータリングの使用状況の詳細] を選択します。  
注: リストされているすべてのサービスが消費に基づいてメータリングを使用している場合は、警告メッセージが表示され、[ライセンスメトリック] ビューからメータリングの使用状況レポートをダウンロードすることはできません。
4. サービス機能または製品機能と、表示する日付範囲を選択して、[エクスポート] をクリックします。

### [詳しいグラフ] からのメータリングの使用状況レポートのダウンロード

[メータリング] ページの [詳しいグラフ] ビューからメータリングの使用状況レポートをダウンロードします。

1. 管理者で [メータリング] を選択します。
2. ダウンロードするメータリングの使用状況レポートの [詳しいグラフ] をクリックします。
3. 表示する組織と日付範囲を選択します。  
選択した内容に応じてレポートデータが調整されます。

4. ダウンロードアイコンをクリックします。
5. **【エクスポート】** をクリックします。

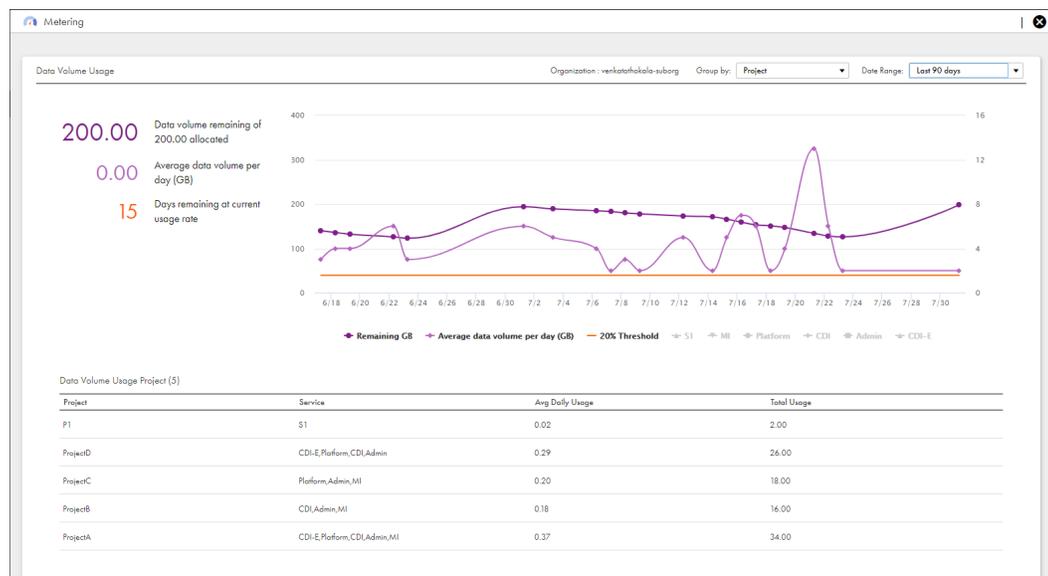
## 使用状況の詳細の表示

詳細なメータリング統計を表示できます。詳細な統計を表示するには、**【メータリング】** ページのダッシュボードビューで、関連するグラフの**【詳しいグラフ】** をクリックするか、**【今月のメトリック概要】** 領域の**【すべてのメーター】** をクリックします。

次のメータータイプでは、詳細なメータリング統計を利用できます。

- アプリケーションの統合
- 高度なサーバーレスとのアプリケーション統合
- CDI-E コンピューティングの時間数
- Data Quality
- Data Quality エラスティック
- 高度なサーバーレスとの Data Quality
- 高度なサーバーレスとの Data Quality エラスティック
- サーバーレス CDI-E コンピューティングの時間数
- サーバーレス CDI コンピューティングの時間数
- 一括取り込みアプリケーション、一括取り込みデータベース、一括取り込みファイル、および一括取り込みストリーミングの場合は、その月に割り当てられた量のうちの残りのデータ量、1日あたりの平均データ量、および現在の使用量での残り日数。一括取り込みアプリケーション-変更データキャプチャおよび一括取り込みデータベース-変更データキャプチャの場合は、割り当てられた合計のうちの残りの行数、1日あたりに処理された平均行数、および現在の使用量での残り日数。

次の図は、過去 90 日間のデータボリューム使用状況の詳細ページの例を示しています。



レポートは、次の方法でカスタマイズできます。

- 組織にサブ組織がある場合は、親組織またはサブ組織の使用状況の詳細を表示できます。削除したサブ組織の使用状況の詳細を表示することはできません。

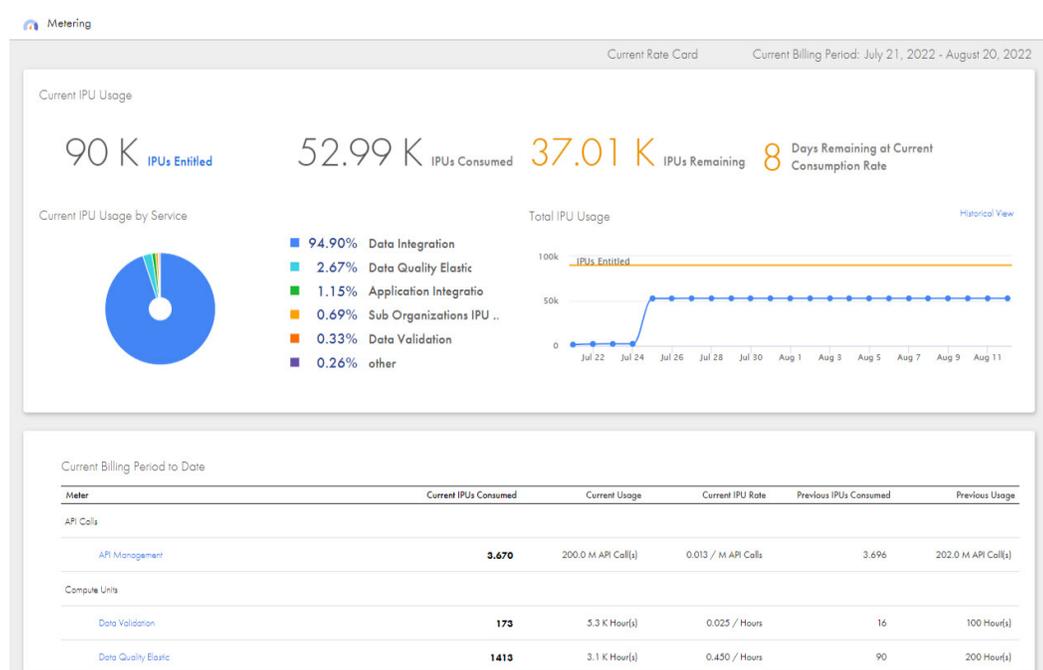
- グループ化は変更できます。例えば、一部のサービスでは、プロジェクト、ランタイム環境、プロジェクトとランタイム環境、またはランタイム環境と日付ごとに、使用状況の詳細を表示できます。一括取り込みの場合、ランタイム環境または IPU（テーブル全体）でグループ化できます。IPU オプションを選択すると、データはランタイム環境と日付および UTC 時間で表示されます。
- 現在の月、先月、過去 90 日間、過去 6 か月または 13 か月など、使用状況の詳細を報告する期間を定義するための日付範囲を変更できます。

**注:** 一括取り込みストリーミングで、実行状態のストリーミング統合ジョブのランタイム環境名またはプロジェクトを変更すると、メタリング情報に古いランタイム環境名が表示されることや、ジョブの古いプロジェクトにメタリング情報が表示されることがあります。ストリーミング統合ジョブを再デプロイすると、それぞれのメタリング情報に新しいランタイム環境名またはプロジェクトが表示されます。一括取り込みアプリケーションおよび一括取り込みデータベースでは、実行中の取り込みジョブのランタイム環境を変更することはできません。

## Informatica のプロセッシングユニットのメトリック

組織でインテリジェントクラウドデータ管理機能を利用している場合、ライセンスは Informatica Intelligent Cloud Services の使用量に基づきます。

Informatica プロセッシングユニット (IPU) は、Informatica Intelligent Cloud Services のスカラ (コンピューティングユニットや処理済みのイベント数など) の使用に対する前払いに使用されるクレジットの単位です。[メタリング] ページで IPU のバランスと使用状況を監視できます。



## IPU メトリックの表示

[**メータリング**] ページで IPU メトリックを表示します。[**メータリング**] ページには、ダッシュボードビューに IPU 情報が表示されます。

ダッシュボードには、プロダクション組織およびサンドボックス組織などのリンクされた組織の IPU 使用量が表示されます。

ダッシュボードには次のパネルが表示されます。

### 現在の IPU 使用量

[現在の IPU 使用量] パネルには、次の情報が表示されます。

- すべての組織およびサブ組織に関する、現在の請求期間に割り当てられた IPU、消費された IPU、および残りの IPU の総数。
- 現在の使用量に基づく、IPU バランスがなくなるまでの残りの推定日数。
- 各サービスまたは主要機能に対する IPU 使用量。

以前の請求サイクルの IPU 使用量について履歴情報を表示するには、[履歴ビュー] をクリックします。

### 現在の請求期間

[現在の請求期間] パネルには、次の情報が表示されます。

- 各メーターの IPU レート。
- 組織数などのスカラタイプに基づく、現在の期間と以前の請求期間の使用量。
- 現在の請求期間と以前の請求期間に消費された IPU。

各メーターの詳細を表示するには、メーター名をクリックします。詳細ページには、IPU およびスカラごとの現在の使用量、選択した日付範囲の IPU 使用量を示す使用履歴グラフ、および日付ごとの詳しい使用状況情報が表示されます。

## IPU スカラ

IPU はスカラ値に基づいています。各サービスには適切なスカラが使用されます。

例えば、データ統合の使用量はコンピューティングユニットで測定され、Cloud 統合ハブの使用量は、処理済みのイベント数によって測定されます。

次の表に、プライマリスカラとその測定単位を示します。

スカラ値	測定単位	説明
API 呼び出し	100 万件の API 呼び出し	カスタム API 呼び出しの数。
コンピューティングユニット	時間	使用または消費された処理容量。
データボリューム	ギガバイト	転送または変換されたデータの量、あるいは組み込まれたデータの量。
処理済みのイベント数	イベント	中間ストレージレイヤにアクセスするデータのインバウンドインスタンスとアウトバウンドインスタンス。
処理済みの行数	100 万行	基になるデータベースログから処理された行数。

スカラ値	測定単位	説明
組織	Number	追加プロダクション組織、サブ組織、およびサンドボックス組織の数。 サブ組織を削除した場合、次の請求期間が始まるまで、この数には削除したサブ組織が含まれます。
保存されているレコード数	レコード	保存されたレコード数。

## IPU メーター

IPU メーターは、インテリジェントクラウドデータ管理に含まれるサービスと機能です。

次の表に、IPU メーターと適用可能なスカラを示します。

メーター	スカラ値
高度なプッシュダウンの最適化	処理済みの行数
API 管理	API 呼び出し
アプリケーションの統合	コンピューティングユニット
高度なサーバーレスとのアプリケーション統合	コンピューティングユニット
B2B Gateway	コンピューティングユニット
データガバナンスとデータカタログ	コンピューティングユニット
データガバナンスとデータカタログ - ガバナンスレコードのスカラ単位あたり 10,000 件のレコード - カタログレコードのスカラ単位あたり 100,000 件のレコード	保存されているレコード数
データ統合	コンピューティングユニット
高度なサーバーレスとのデータ統合	コンピューティングユニット
データ統合エラスティック	コンピューティングユニット
高度なサーバーレスとのデータ統合エラスティック	コンピューティングユニット
データマーケットプレイス: スカラユニットあたり 10,000 件のレコード	保存されているレコード数
データマスキング	コンピューティングユニット
Data Quality	コンピューティングユニット
高度なサーバーレスとの Data Quality	コンピューティングユニット
Data Quality エラスティック	コンピューティングユニット
高度なサーバーレスとの Data Quality エラスティック	コンピューティングユニット

メーター	スカラ値
Integration Hub	処理済みのイベント数
一括取り込みアプリケーション	データボリューム
一括取り込みアプリケーション - 変更データキャプチャ	処理済みの行数
一括取り込みデータベース	データボリューム
一括取り込みデータベース - 変更データキャプチャ	処理済みの行数
一括取り込みファイル	データボリューム
一括取り込みストリーミング	データボリューム
追加のプロダクション組織	組織
サンドボックス	組織
サブ組織の IPU 使用率	組織

## IPU メトリックレポート

IPU メトリックレポートは **[メータリング]** ページからダウンロードできます。

次のタイプのレポートをダウンロードできます。

### IPU 使用率サマリレポート

IPU 使用率のサマリレポートには、組織、サンドボックス、およびサブ組織の IPU 使用率のサマリが含まれています。レポートには、現在の請求期間、または最大で過去 13 回の請求期間のデータが含まれます。レポートには、次のデータが含まれています。

- 請求期間
- メーター
- 使用率
- 使用された IPU

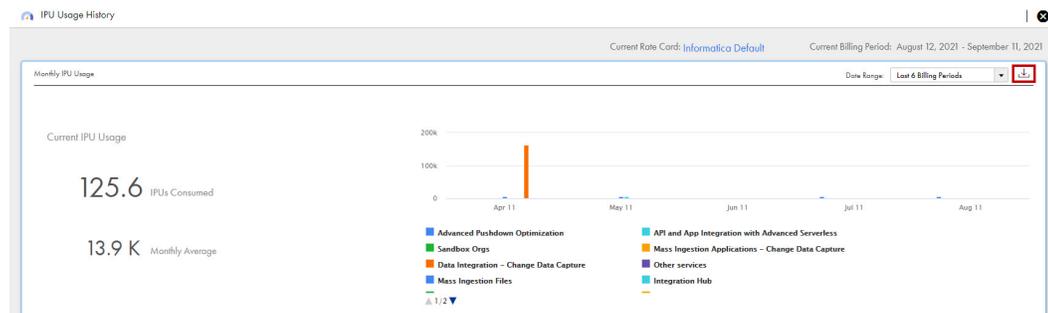
### テーブルビューレポート

テーブルビューレポートには、IPU メーターの詳細ページのテーブルに現在表示されている情報が含まれます。

### 詳細なサービスレポート

一部のメーターでは、特定の日付範囲のサービスの詳細を含む IPU メーターのレポートをダウンロードできます。

レポートをダウンロードするには、**[ダウンロード]** アイコンをクリックします。次の図は、**[IPU 使用率の履歴]** ページの **[ダウンロード]** アイコンを示しています。



## IPU 使用率サマリレポートのダウンロード

**[IPU 使用率の履歴]** ページからサマリレポートをダウンロードします。

1. **[メータリング]** ページで **[履歴ビュー]** をクリックします。
2. レポートに含める請求期間を選択します。最大で過去 13 回の請求期間を選択できます。
3. **[ダウンロード]** アイコンをクリックします。
4. **[エクスポート]** をクリックします。

## IPU メーターレポートのダウンロード

メーターの詳細ページで特定のメーターのレポートをダウンロードします。現在のテーブルビューに基づくレポートをダウンロードできます。一部のメーターについては、詳細なサービスレポートをダウンロードすることもできます。

1. **[メータリング]** ページの **[現在の請求期間]** 領域で、メーター名をクリックして詳細ページを開きます。
2. レポートに含める請求期間を選択します。
3. **[ダウンロード]** アイコンをクリックします。
4. 詳細なサービスレポートをダウンロードするオプションが利用可能な場合、**[ダウンロード]** アイコンをクリックすると **[メータリングの使用状況レポート]** ダイアログボックスが表示されます。次のいずれかの手順に従います。
  - テーブルビューレポートを選択し、**[エクスポート]** をクリックします。
  - 詳細なサービスレポートを選択し、レポートの日付範囲を選択して、**[エクスポート]** をクリックします。

## 第 5 章

# ソース管理、サービスアップグレード、およびブランディング設定

Secure Agent サービスのソース管理設定とアップグレード設定、およびカスタムブランディングは、**【設定】** ページで設定できます。

以下の設定項目を設定することができます。

### ソース管理設定

組織に適切なライセンスがある場合は、組織のソース管理を設定できます。プロジェクト、フォルダ、およびアセットのバージョン管理を有効にするためのソース管理を設定します。ソース管理を設定するには、**【ソース管理の有効化】** オプションを有効にし、リポジトリアクセスのタイプを設定してから、ソース管理リポジトリへの接続を設定します。

ソース管理リポジトリへの読み取り/書き込み、または読み取り専用アクセスを設定できます。読み取り/書き込みアクセスを設定するには、**【Git リポジトリへのプッシュを許可】** オプションを有効にします。読み取り専用アクセスを設定するには、**【Git リポジトリへのプッシュを許可】** オプションを無効にします。

### Secure Agent サービスのアップグレード設定

ローリングアップグレードをサポートするサービスのアップグレード中にエラーが発生した場合、そのサービスのアップグレードを続行するか停止するかを指定できます。

マイナーアップグレード後に再起動する必要があるサービスの再起動スケジュールを設定できます。再起動スケジュールの再開を設定するには、アップグレードを実行する曜日と時刻を選択します。

### カスタムブランディング

組織に適切なライセンスがある場合は、親組織のカスタムブランド設定を構成し、それらをサブ組織に適用できます。各サブ組織のカスタムブランディング設定を、要件に応じて設定することもできます。カスタムブランディング設定には、ロゴ、カラーテーマ、ファビコンが含まれます。

カスタムブランディング設定を構成すると、Reference 360 サービスには、指定したロゴとファビコンが表示されます。

## ソース管理設定

プロジェクト、フォルダ、およびアセットのバージョン管理を有効にするために、組織のソース管理を設定できます。ソース管理を設定すると、クラウドでホストされた Git リポジトリ、またはオンプレミスの Git リポジトリにオブジェクトのバージョンを保存できます。ソース管理は **【設定】** ページで設定します。

Informatica Intelligent Cloud Services でソース管理を使用するには、適切なライセンスが必要です。

次の表に、サポートされているソース管理リポジトリを示します。

リポジトリ	セルフホスト	クラウドホスト
Atlassian Bitbucket	サポート	-
GitHub	サポート	サポート
GitLab	サポート	-
Microsoft Azure DevOps	-	サポート

組織のソース管理を設定すると、ユーザーはソース管理をオブジェクトに適用できます。オブジェクトは自動的にチェックインされません。ユーザーは、ソース管理を個別のアセットまたはプロジェクトまたはフォルダ内のすべてのアセットに適用できます。ソース管理のプロジェクト、フォルダ、およびアセットへの適用の詳細については、該当する Informatica Intelligent Cloud Services サービスのヘルプシステムを参照してください。

組織のソース管理は、次の方法で設定できます。

#### ソース管理リポジトリへの読み取り/書き込みアクセスを設定します。

読み取り/書き込みアクセスを設定すると、組織内のユーザーは、オブジェクトのチェックインおよびチェックアウト、オブジェクトのバージョンのプル、オブジェクトを前のバージョンに戻すことができます。ユーザーは、ソース管理オブジェクトを変更するには、それらをチェックアウトする必要があります。ユーザーはオブジェクトを排他的にチェックアウトするため、ユーザーは別のユーザーによってチェックアウトされているオブジェクトを変更することはできません。ユーザーは、ソース管理されていないオブジェクトはチェックアウトせずに変更できます。

読み取り/書き込みアクセスは、プロジェクトおよびアセットを開発する組織用に設定することがあります。

#### ソース管理リポジトリへの読み取り専用アクセスを設定します。

読み取り専用アクセスを設定すると、組織内のユーザーは、ソース管理オブジェクトのバージョンをリポジトリからプルできます。しかし、ユーザーはオブジェクトのチェックアウトまたはチェックインをすることはできません。ユーザーは、組織内のプロジェクト、フォルダ、およびアセットをチェックアウトせずに、それらに変更を加えることができます。

読み取り専用アクセスは、テストまたは本番組織に設定し、ユーザーがアセットの最新バージョンをテストまたは実行できるようにすることがあります。

**警告:** 読み取り専用アクセスを設定すると、ユーザーは、ソース管理オブジェクトを上書きできます。例えば、ユーザー John が最新バージョンのソース管理マッピングをプルし、変更するとします。別のユーザーが後でこのマッピングの任意のバージョンをプルした場合、John の変更は失われます。オブジェクトの権限およびユーザー権限は、ユーザーが誤って組織内のソース管理アセットを上書きするのを防止するように、注意深く設定します。

リポジトリアクセスタイプを変更できます。しかし、読み取り/書き込みから読み取り専用に変更するには、まずオブジェクトがチェックアウトされていないことを確認する必要があります。Informatica Intelligent Cloud Services は、チェックアウトされているオブジェクトがある場合、リポジトリアクセスタイプの読み取り/書き込みから読み取り専用への変更を許可しません。

リポジトリ URL も変更できます。これを実行するには、まずすべてのソース管理アセットのリンクを解除します。Informatica Intelligent Cloud Services は、ソース管理アセットがある場合、リポジトリ URL の変更を許可しません。

設定した後でソース管理を無効にする場合、ソース管理からすべてのオブジェクトのリンクを解除してから、組織のソース管理を無効にします。

管理者ロールまたは [チェックアウトの取り消しを強制] 特権を持つユーザーロールを持っている場合は、別のユーザーによってチェックアウトされたオブジェクトのリンクを解除できます。

## サブ組織のソース管理設定

サブ組織のソース管理は、サブ組織の [設定] ページで設定します。ベストプラクティスとして、各サブ組織は、その組織用のソース管理リポジトリを使用する必要があります。さらに、サブ組織用のソース管理リポジトリは、その親組織のソース管理リポジトリと別である必要があります。

個別のソース管理リポジトリを管理することで、1つの組織内のユーザーが、別の組織のアセットを誤って上書きしたり変更したりすること起きないようにします。

親組織の管理者がサブ組織のソース管理操作を実行できるようにする場合、親組織の管理者の Git ユーザーアカウントが、サブ組織のソース管理リポジトリへのアクセス権を持つように設定します。

## OAuth を使用したリポジトリアクセス

ソース管理リポジトリがクラウドでホストされている場合は、個人アクセストークンの代わりに OAuth 認証を使用してリポジトリへのアクセスを提供するように組織を設定できます。OAuth 認証は [設定] ページで設定します。

GitHub リポジトリを使用する場合は、Informatica Intelligent Cloud Services が組織の GitHub リポジトリに対してソース管理操作を実行できるようにする GitHub アクセサアプリケーションがリポジトリにインストールされている必要があります。このアプリケーションがリポジトリにインストールされていない場合は、[設定] ページからインストールできます。

## オンプレミスリポジトリの操作

ソース管理リポジトリがオンプレミスの場合、Secure Agent は Secure Agent マシンにリポジトリのローカルコピーを作成します。Secure Agent は、ローカルリポジトリでソース管理操作を実行してから、それらをリモートリポジトリにプッシュします。

オンプレミスリポジトリを使用する場合は、Secure Agent マシンにリポジトリのローカルコピーとその後のすべてのバージョン管理操作のための十分なスペースがあることを確認してください。

Secure Agent は、ユーザーがアセットのチェックインなどのソース管理操作を初めて実行するときに、ローカルリポジトリを作成します。ローカルリポジトリの作成する時に、Informatica Intelligent Cloud Services アセットを格納するブランチをコピーします。他のブランチはコピーされません。ユーザーがソース管理操作を実行するたびに、エージェントは、操作をサポートするために変更に関する情報をリモートリポジトリから取得します。

デフォルトでは、Secure Agent は、Secure Agent マシンの次のディレクトリにローカルリポジトリを作成します。

```
<Secure Agent インストールディレクトリ>/apps/GitRepoConnectApp/data/git_repository/<クライアント URL>/<組織 ID>/<ブランチ>/<リモートリポジトリ名>
```

Secure Agent の詳細ページで GitRepoConnectApp サービスの **git\_local\_repository\_path** プロパティを編集することで、ローカルリポジトリディレクトリを変更できます。このプロパティの値の変更に関する詳細については、「*Secure Agent サービス*」を参照してください。

## 組織のソース管理の有効化

組織のソース管理を有効にする場合、**【設定】** ページでソース管理リポジトリへのアクセスタイプと接続を設定します。構成する設定は、リポジトリのタイプに応じて異なります。

1. 管理者の **【設定】** ページで、[ソース管理] 領域の **【編集】** をクリックします。
2. **【ソース管理の有効化】** オプションを有効にします。
3. ソース管理リポジトリへのアクセスタイプを設定します。
  - 読み取り/書き込みアクセスを設定するには、**【Git リポジトリへのプッシュを許可】** オプションを有効にします。
  - 読み取り専用アクセスを設定するには、**【Git リポジトリへのプッシュを許可】** オプションを無効にします。
4. クラウドでホストされているリポジトリへのアクセスを設定するには、次の情報を入力します。

オプション	説明
プラットフォーム	プラットフォームタイプ。 <b>【クラウド】</b> を選択します。
Git リポジトリの URL	リポジトリ URL。以下に例を示します。 <code>https://github.com/MyGitUser/MyRepositoryName.git</code> リポジトリ URL は HTTPS プロトコルを使用する必要があります。 <b>ヒント:</b> リポジトリのクローンオプションを選択することで、リポジトリの URL を見つけることができます。
Git ブランチ名	Informatica Intelligent Cloud Services オブジェクトを格納するブランチの名前。指定するブランチは、リポジトリにすでに存在している必要があります。 ブランチ名を入力しない場合は、Informatica Intelligent Cloud Services では、リモートリポジトリのデフォルトのブランチの名前に基づいて、ブランチ名が「master」または「main」に設定されます。
Git への OAuth アクセスを許可	OAuth を使用してリポジトリにアクセスするには、このオプションを有効にします。 GitHub リポジトリを使用する場合は、Informatica Intelligent Cloud Services のアクセスを許可する Git アクセスアプリケーションをリポジトリにインストールする必要があります。このアプリケーションをインストールするには、 <b>【Github に Git アクセスアプリをインストール】</b> をクリックします。

5. オンプレミスリポジトリへのアクセスを設定するには、次の情報を入力します。

オプション	説明
プラットフォーム	プラットフォームタイプ。 <b>【オンプレミス】</b> を選択します。
Git リポジトリの URL	リポジトリ URL。以下に例を示します。 <code>https://gitlab.example.com/MyGitUser/MyRepositoryName.git</code> リポジトリ URL は HTTPS プロトコルを使用する必要があります。 <b>ヒント:</b> リポジトリのクローンオプションを選択することで、リポジトリの URL を見つけることができます。

オプション	説明
Git ブランチ名	Informatica Intelligent Cloud Services オブジェクトを格納するブランチの名前。指定するブランチは、リポジトリにすでに存在する必要があります。 ブランチ名を入力しない場合は、Informatica Intelligent Cloud Services では、リモートリポジトリのデフォルトのブランチの名前に基づいて、ブランチ名が「master」または「main」に設定されます。
ランタイム環境	Git リポジトリへの接続に使用されるランタイム環境。 このリポジトリは、選択したランタイム環境のすべてのエージェントがアクセスできる必要があります。

オンプレミスリポジトリへの OAuth アクセスを設定することはできません。

6. **【保存】** をクリックします。

Informatica Intelligent Cloud Services は、リポジトリ接続を確認するためのソース管理資格情報の入力を求めるプロンプトを表示します。Informatica Intelligent Cloud Services はこの情報を保存しません。

接続が有効であり、リポジトリへの読み取り/書き込みアクセスを設定した場合、Informatica Intelligent Cloud Services はこのリポジトリに小さな readme ファイルを書き込み、これがリポジトリにオブジェクトをプッシュできることを確認します。

ソース管理の有効化後、ソース管理を使用するすべてのユーザーは、ユーザー設定で自分のソース管理資格情報を入力する必要があります。ユーザーは、自分の資格情報を入力するまでは、**【参照】** ページのソース管理カラムを表示できず、ソース管理アクションを実行できません。ソース管理資格情報を入力するには、**【ユーザー】** アイコンを Informatica Intelligent Cloud Services ウィンドウの右上隅でクリックし、**【設定】** を選択します。

## ソース管理リポジトリ URL の変更

ソース管理リポジトリ URL を変更するには、まず組織内のすべてのオブジェクトをリンク解除し、新規リポジトリ URL を管理者の **【設定】** ページで入力します。URL の変更後、ソース管理を使用するすべてのユーザーは、ユーザー設定で自分のソース管理資格情報を更新する必要があります。

- そのリポジトリを使用する各 Informatica Intelligent Cloud Services サービスで、すべてのオブジェクトをソース管理からリンク解除します。
- 管理者で、**【設定】** ページを開き、[ソース管理] 領域の **【編集】** をクリックします。
- 【ソース管理の有効化】** オプションが有効になっていることを確認します。
- ソース管理リポジトリへのアクセスタイプを設定します。
  - 読み取り/書き込みアクセスを設定するには、**【Git リポジトリへのプッシュを許可】** オプションを有効にします。
  - 読み取り専用アクセスを設定するには、**【Git リポジトリへのプッシュを許可】** オプションを無効にします。
- プラットフォームと、Informatica Intelligent Cloud Services オブジェクトを格納するブランチの名前を確認します。クラウドでホストされているリポジトリの場合は、OAuth アクセス設定も確認します。
- 新規リポジトリ URL を次のように入力します。

`https://github.com/MyGitUser/MyRepositoryName.git`

**ヒント:** リポジトリの URL は、リポジトリのタイプに基づいて次の方法で見つけることができます。

リポジトリ	URL を見つける方法
Atlassian Bitbucket (セルフホスト)	リポジトリを開き、 <b>【クローン】</b> を選択します。
GitHub (クラウドホスト)	リポジトリを開き、 <b>【クローンまたはダウンロード】</b> > <b>【HTTPS でクローン】</b> を選択します。
GitHub Enterprise (セルフホステッド)	リポジトリを開き、 <b>【コード】</b> > <b>【HTTPS でクローン】</b> を選択します。
GitLab セルフマネージド	リポジトリを開き、 <b>【クローン】</b> > <b>【HTTPS でクローン】</b> を選択します。
Microsoft Azure DevOps (クラウドホスト)	リポジトリを開き、 <b>【クローン】</b> を選択します。

リポジトリ URL は HTTPS プロトコルを使用する必要があります。

7. **【保存】** をクリックします。

Informatica Intelligent Cloud Services は、リポジトリ接続を確認するためのソース管理資格情報の入力を求めるプロンプトを表示します。Informatica Intelligent Cloud Services はこの情報を保存しません。

接続が有効であり、リポジトリへの読み取り/書き込みアクセスを設定した場合、Informatica Intelligent Cloud Services はこのリポジトリに小さな readme ファイルを書き込み、これがリポジトリにオブジェクトをプッシュできることを確認します。

ソース管理リポジトリ URL の変更後、ソース管理を使用するすべてのユーザーは、ユーザー設定で自分のソース管理資格情報を更新する必要があります。ソース管理資格情報を更新するには、**【ユーザー】** アイコンを Informatica Intelligent Cloud Services ウィンドウの右上隅でクリックし、**【設定】** を選択します。

## 組織のソース管理の無効化

組織のソース管理を無効にできます。ソース管理を無効にすると、組織とソース管理リポジトリの間のリンクが解除されます。ソース管理リポジトリ内のオブジェクトは削除されません。

読み取り書き込みに関する組織のソース管理を無効にする前に、すべてのアセットをリンク解除する必要があります。

1. そのリポジトリを使用する各 Informatica Intelligent Cloud Services サービスで、すべてのオブジェクトをソース管理からリンク解除します。
2. 管理者で、ソース管理を無効にします。
  - a. 管理者で、**【設定】** ページを開きます。
  - b. **【ソース管理】** 領域の **【編集】** をクリックします。
  - c. **【ソース管理の有効化】** オプションを無効にします。
  - d. **【保存】** をクリックします。
3. オプションとして、組織内のユーザーがユーザー設定で自分のソース管理資格情報を削除できるようにします。
  - a. Informatica Intelligent Cloud Services ウィンドウの右上隅で、**【ユーザー】** アイコンをクリックし、**【設定】** を選択します。
  - b. ソース管理資格情報をクリアします。

- c. **【保存】** をクリックします。

## 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 アクセサ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。

## ソース管理のベストプラクティス

組織がソース管理を効果的に設定して使用できるようにするには、次のガイドラインをベストプラクティスとして使用します。

### 設定のガイドライン

組織のソース管理を設定するときは、次のガイドラインに従います。

- 開発、テスト、ステージング、本番には別々の組織を使用します。

異なる組織を管理するときは、環境間を独立させ、1つの環境に対する変更が、他の環境に影響しないようにします。例えば、テスト環境内のアセットへの変更が、誤って本番環境にデプロイされることがないようにします。
- ソース管理リポジトリへの読み取り/書き込みアクセスを持つ開発組織を設定し、ソース管理リポジトリへの読み取り専用アクセスを持つ非開発組織を設定します。

そうすることで、開発組織内のユーザーのみが、アセットに変更を加えられます。また、非開発環境内のユーザーが、誤って変更をソース管理リポジトリにプッシュすることを防止できます。
- 特定のソース管理リポジトリにプッシュする開発組織は1つのみにしてください。

開発組織用の独立したリポジトリを管理することで、ある組織内のユーザーが別の組織のアセットを誤って変更したり上書きしたりする事故が起きないようにします。独立したリポジトリを管理すると、別の組織からのアセット ID 参照の競合も回避できます。

- 組織のソース管理を有効にするときは、空のリポジトリを選択します。  
Informatica Intelligent Cloud Services はアセットを Git リポジトリ内の Explore フォルダに保存するため、リポジトリに Explore という名前のフォルダが含まれないようにします。
- ソース管理の資格情報を、複数の Informatica Intelligent Cloud Services ユーザー間で共有しないようにします。  
個別の資格情報によってセキュリティが維持され、特定の変更を加えたユーザーが誰かを追跡するのが簡単になります。さらに、各ユーザーは、GitHub 内に自分の制限を持ちます。

## 開発ガイドライン

アセットを開発し操作するときは、次のガイドラインに従います。

### 依存関係の管理に関するガイドライン

依存関係を持つアセットを管理するには、次のガイドラインに従います。

- アセットをリポジトリからプルする前に、接続およびランタイム環境を作成します。  
必要な接続およびランタイム環境がターゲット組織内にあるときは、タスクをリポジトリからプルした直後に実行できます。
- マッピングやコンポーネントなどの再利用可能なアセットが、使用前にリポジトリ内にあることを確認します。  
Informatica Intelligent Cloud Services は、マッピングタスクなどのアセットが依存するマッピングが組織内がない場合、アセットの保存を許可しません。

### アセットのチェックインおよびチェックアウトに関するガイドライン

アセットをチェックインおよびチェックアウトするときは、次のガイドラインに従います。

- アセットの名前を変更または移動する場合は、アセットの第 1 レベルの依存アセットをチェックアウトし、それらを同じチェックインに含めます。  
例えば、マッピングタスクが使用するマッピングの名前を変更する必要がある場合、そのマッピングタスクがタスクフローで使用されている場合は、マッピングとマッピングタスクをチェックアウトします。タスクフローをチェックアウトする必要はありません。マッピングの名前を変更した後に、マッピングとマッピングタスクを 1 回のチェックインアクションでチェックインします。
- アセットのチェックイン時にコメントを入力します。  
アセットのチェックイン時に、リリースタグ名を **【サマリ】** フィールドに入力し、より説明的なコメントを **【説明】** フィールドに入力することがあります。これを実行すると、Informatica Intelligent Cloud Services の **【Git Summary (Git サマリ)】** フィールドに、アセットに関連付けられたリリースタグが表示されます。
- 複数のアセットを同時にチェックインするときは、アセット数を 1000 件以下に制限します。  
1000 件を超えるアセットを同時にチェックインすると、Informatica Intelligent Cloud Services と GitHub リポジトリサービスとの間のパフォーマンスが低下する可能性があります。

## 別のユーザーのチェックアウトの取り消し

管理者ロールがある場合、またはユーザーロールに管理者サービスへのチェックアウトの取り消しを強制する機能がある場合、別のユーザーがチェックアウトしたオブジェクトのチェックアウトを取り消すことができま

す。ユーザーがオブジェクトをチェックアウトして、休暇を取る場合、または組織を離れる場合、別のユーザーによりチェックアウトされたオブジェクトのチェックアウトを取り消す必要がある場合があります。

チェックアウトを取り消すと、オブジェクトはソース管理リポジトリにある最後のバージョンに戻ります。オブジェクトのバージョン履歴には、チェックアウトやチェックアウトアクションを取り消した記録は残りません。後で変更したバージョンが必要になる可能性がある場合、チェックアウトを取り消す前にオブジェクトのコピーを作成します。

取り消しアクションは元に戻せません。プロジェクトまたはフォルダのチェックアウトを取り消すと、そのプロジェクトまたはフォルダのロックは解除されますが、プロジェクトまたはフォルダ内にあるオブジェクトはロックされたままになります。

1. ユーザーがオブジェクトをチェックアウトしたサービスを開きます。
2. **[エクスプローラ]** ページで、オブジェクトに移動します。
3. オブジェクトが含まれている行で、**[アクション]** をクリックし、**[チェックアウトの取り消し]** を選択します。

取り消しアクションによってロックが解除されるため、オブジェクトはチェックアウトできる状態になります。

**注:** オブジェクトがチェックアウトされた後に移動または名前が変更された場合、チェックアウトを取り消すとオブジェクトの名前と場所はチェックアウトされる前の名前と場所に戻されます。

## Secure Agent サービスのローリングアップグレード

一部の Secure Agent サービスは、ローリングアップグレードをサポートしています。ローリングアップグレードでは、Secure Agent グループ内のエージェントで実行されているサービスは、順次アップグレードされます。そのため、あるエージェント上でサービスがアップグレードされる間、そのサービスはグループ内の他のエージェント上で使用可能であり続けます。

次の Secure Agent サービスは、ローリングアップグレードをサポートしています。

- プロセスサーバー

Secure Agent グループ内のエージェントで実行されているその他のサービスは、各エージェント上で同時にアップグレードされます。そのため、そのグループ内のエージェントがアップグレードされている間は、サービスを使用できません。グループ内のすべてのエージェントが正常にアップグレードされると、使用できるようになります。

### 例

組織では、次のランタイム環境を使用しています。

- Secure Agent グループ A:

エージェント A1 はデータ統合サーバーおよびプロセスサーバーを実行します。

エージェント A2 はデータ統合サーバー、一括取り込み、およびプロセスサーバーを実行します。

- Secure Agent グループ B:

エージェント B1 はデータ統合サーバー、一括取り込み、およびプロセスサーバーを実行します。

エージェント B2 はデータ統合サーバー、一括取り込み、およびプロセスサーバーを実行します。

組織がアップグレードされる時に、Secure Agent グループ A および B は同時にアップグレードされます。各 Secure Agent グループ内で、プロセスサーバーは順次アップグレードされます。そのため、プロセスサーバーがエージェント A1 および B1 でアップグレードされる間、エージェント A2 および B2 で実行され続けま

す。エージェント A1 および B1 でのアップグレードが完了すると、プロセスサーバーはエージェント A2 および B2 でアップグレードされます。

データ統合サーバーと一括取り込みはローリングアップグレードをサポートしていません。グループ A および B で、データ統合サーバーは各エージェントで同時にアップグレードされます。グループ B で、一括取り込みはエージェント B1 および B2 で同時にアップグレードされます。

## ローリングアップグレードエラーの処理

ローリングアップグレードをサポートするサービスのアップグレード中にエラーが発生した場合、そのサービスのアップグレードを続行するか停止するかを指定できます。エラー処理動作を **【設定】** ページで設定します。

以下のいずれかのオプションを選択することができます。

### エラーが発生した場合、エラーにフラグを設定して、アップグレードを続行する

サービスのアップグレード中にエラーが発生した場合、サービスはエラーが発生したエージェントのエラーで停止します。そのアップグレードは、グループ内の別のエージェント上で続行されます。

**警告:** このオプションを有効にし、グループ内のすべてのエージェント上でエラーが発生した場合、そのサービスは Secure Agent グループでの実行を停止します。これがジョブの中断の原因になる場合があります。

### エラーが発生した場合、アップグレードを停止する

サービスのアップグレード中にエラーが発生した場合、サービスはエラーが発生したエージェントのエラーで停止します。まだアップグレードされていないグループ内の他のすべてのエージェントに対してサービスのアップグレードが停止します。まだアップグレードされていないエージェントは、そのサービスの以前のバージョンで実行し続けます。

これがデフォルトのオプションです。

エラー処理動作を設定するには、**【編集】** を [Secure Agent サービスのアップグレード設定] 領域でクリックし、適切なオプションを選択し、**【保存】** をクリックします。

## Secure Agent サービスの再開スケジュールの設定

プロセスサーバーなどの一部の Secure Agent サービスには、アップグレード後に再開する必要があるものがあります。これらのサービスは、月間アップグレードやパッチリリースなどのマイナーアップグレード後に再開スケジュールを設定できます。再開スケジュールを **【設定】** ページで設定します。

再開スケジュールを設定するときは、サービスを再開する曜日と時刻を選択します。例えば、毎週日曜日の 00:00 GMT の再開をスケジュールできます。

プロセスサーバーサービスの再起動スケジュールを設定できます。再起動スケジュールを設定するには、次の手順を実行します。

1. Administrator で **【設定】** を選択します。
2. **【Secure Agent サービスのアップグレード設定】** 領域で **【編集】** をクリックします。
3. 日時を選択します。
4. **【保存】** をクリックします。

再起動スケジュールを設定しない場合、デフォルトでは、ポイントオブデプロイメント (POD) がアップグレードされてから 7 日後にプロセスサーバーサービスが自動的に再起動されます。

# カスタムブランディングの設定

Informatica のデフォルト設定の代わりに、カスタムロゴ、カラーテーマ、およびファビコンを使用してブランディング設定をカスタマイズできます。カスタムブランディングは、**【設定】** ページで設定します。

ブランディング設定をカスタマイズするには、適切なライセンスが必要です。

## ロゴおよびファビコンのガイドライン

組織のロゴとファビコンをアップロードする際は、次のガイドラインを使用してください。

- ロゴおよびファビコンの画像のファイルサイズは 1 MB 未満でなければなりません。
- ロゴ画像の最大サイズは 80 x 325 ピクセルでなければなりません。推奨サイズは 48 x 325 ピクセルです。
- ロゴ画像をアップロードする際、画像は枠内に配置されます。ズームコントロールオプションを使用して、画像が枠内に収まるように画像のサイズを変更してください。
- ファビコン画像の最大サイズは 196 x 196 ピクセルでなければなりません。推奨サイズは 32 x 32 ピクセルです。

## 組織のカスタムブランディングの設定

**【設定】** ページで、ロゴやファビコンをアップロードして、カラーテーマを選択できます。

1. 管理者の **【設定】** ページで、**【カスタムブランディング】** 領域の **【編集】** をクリックします。
2. **【カスタムブランディングの有効化】** を選択します。
3. サブ組織が、親組織からブランディング設定を継承するようにするには、**【サブ組織はカスタムブランディングを継承する】** を選択します。
4. ロゴ画像を更新するには、**【アップロード】** をクリックし、ロゴファイルを選択します。ロゴのガイドラインの詳細については、[「ロゴおよびファビコンのガイドライン」 \(ページ 51\)](#) を参照してください。
5. ファビコン画像を更新するには、**【アップロード】** をクリックし、ファビコンファイルを選択します。ファビコンのガイドラインの詳細については、[「ロゴおよびファビコンのガイドライン」 \(ページ 51\)](#) を参照してください。
6. ロゴとファビコンに合うカラーテーマを選択します。自分でテーマを作成することもできます。
7. カスタムブランディング設定を適用する前に、**【プレビュー】** セクションで変更をプレビューして確認します。
8. **【保存】** をクリックします。

# 第 6 章

## 権限

権限によって、Secure Agent、Secure Agent グループ、接続、スケジュール、またはアセットに対するユーザーのアクセス権が決まります。また、オブジェクトに対する追加またはカスタムのセキュリティを追加します。権限によって、オブジェクトに対する権限の読み取り、更新、削除、実行、および変更が可能なユーザーおよびグループが定義されます。

オブジェクトの権限を構成するには、次のライセンスと特権が必要です。

- プロジェクト内のすべてのアセットについてプロジェクトレベルで権限を構成するには、プロジェクトレベルでセキュリティ権限の設定または設定解除を行うためのライセンスが組織に必要です。
- プロジェクト内のすべてのアセットについてフォルダレベルで権限を構成するには、フォルダレベルでセキュリティ権限の設定または設定解除を行うためのライセンスが組織に必要です。
- 個々のアセットの権限を構成するには、セキュリティを詳細に設定するためのライセンスが組織に必要です。
- ユーザーアカウント、または管理者がメンバとなっているグループに割り当てられたロールには、オブジェクトタイプに対する権限の設定特権が必要です。例えば、Secure Agent の権限を構成するには、Secure Agent に対する権限の設定特権を持つロールが割り当てられる必要があります。

オブジェクトの権限を構成するには、オブジェクトに移動して適切な権限を設定します。例えば、開発チームのユーザーグループのユーザーだけが開発データフォルダのアセットにアクセスできるようにします。フォルダに移動し、権限を編集し、フォルダに開発チームのユーザーグループの権限を付与します。

権限は、オブジェクトのコピーではなく、権限を構成するオブジェクトに適用します。したがって、アセットをコピーまたはエクスポートする場合、その権限はアセットと一緒にコピーまたはエクスポートされません。例えば、ユーザー rjones が実行権限を持っているマッピングタスクをエクスポートします。マッピングタスクをインポートすると、インポートされたマッピングには割り当てられた権限がありません。したがって、マッピングタスクを実行する特権を持つユーザーは、インポートされたタスクを実行できます。

オブジェクトに対して次の権限を構成できます。

権限	説明
読み取り	オブジェクトを開いて表示します。 オブジェクトがソース管理されている場合、この権限によって、ユーザーまたはグループはオブジェクトをソース管理リポジトリからプルまたはチェックアウトできます。 タスクを選択すると、この権限によって、ユーザーまたはグループがタスク内の接続またはスケジュールを使用することもできます。
更新	オブジェクトを編集します。 オブジェクトがソース管理されている場合、この権限によって、ユーザーまたはグループは、オブジェクトをチェックイン、チェックアウト、プル、リンク解除、またはロールバックできます。 読み取り権限が必要です（自動的に付与される）。

権限	説明
削除	オブジェクトを削除します。
実行	オブジェクトを実行します。 マッピング、タスク、タスクフロー、および Cloud 統合ハブアセットに適用されます。マッピング、タスク、またはタスクフローのインスタンスを監視、停止、および再起動します。
権限の変更	オブジェクトに割り当てられている権限を変更します。

**注:** これらの権限は、Informatica Intelligent Cloud Services 内で制御されます。Windows や Linux で Secure Agent を起動、停止、または設定する場合の権限のような、オペレーティングシステムの権限を制御するものではありません。

## 権限のルールおよびガイドライン

権限には、次の規則とガイドラインを使用します。

- オブジェクトの権限を構成するときに、権限を付与するユーザーまたはグループに、そのオブジェクトタイプに対する適切な特権を持つロールが割り当てられていることを確認します。例えば、ユーザーに特定のフォルダに対するサービスコンシューマロールの更新特権があっても、サービスコンシューマロールにはフォルダの更新特権がないため、ユーザーはフォルダを更新できません。
- アセットを編集するには、アセット内で使用されているすべてのアセットに対する読み取り権限がユーザーに与えられている必要があります。例えば、同期タスクに対する読み取りおよび更新の権限をユーザーに割り当てた場合、そのユーザーにタスクで使用されている接続、マップレット、スケジュール、および保存されたクエリに対する読み取り権限もあることを確認します。
- ユーザーがタスクを編集すると、読み取り権限のないアセットは表示されません。予期しない結果を回避するには、ユーザーが適切な読み取り権限を付与されるまで、すべての変更をキャンセルし、タスクの編集を回避する必要があります。
- タスクフローを構成する場合、ユーザーは、タスクフローに追加するすべてのタスクに対する実行権限を必要とします。
- タスクフローを編集するには、タスクフローのすべてのタスクに対して実行権限が必要です。すべてのタスクに対して実行権限がない場合、ユーザーはタスクフローに変更を保存できません。
- タスクフローを実行するには、ユーザーにタスクフローに対する読み取り権限と実行権限が必要です。
- ジョブを監視したり、実行中のジョブを停止したりするには、ユーザーはマッピング、タスク、またはタスクフローの実行権限を必要とします。
- データ統合タスクにカスタム権限を割り当てて、アプリケーション統合プロセスまたはガイドを介してデータ統合タスクを呼び出す場合は、次のいずれかのタスクを実行する必要があります。
  - アプリケーション統合の匿名ユーザーに、関連するデータ統合アセットの実行権限を付与します。
  - アプリケーション統合の匿名ユーザーを、関連するデータ統合アセットの実行権限を持つユーザーグループに追加します。

# 権限の設定

オブジェクトタイプに対する権限の設定特権を持つロールが割り当てられている場合は、オブジェクトの権限を構成できます。例えば、フォルダの権限を構成するには、フォルダの権限の設定特権を持つロールが割り当てられている必要があります。

1. 権限を構成するオブジェクトに移動します。

例:

- Secure Agent または Secure Agent グループの権限を構成するには、管理者で **【ランタイム環境】** を選択します。
- 接続の権限を構成するには、管理者で **【接続】** を選択します。
- マッピングの権限を構成するには、データ統合でマッピングを含むプロジェクトとフォルダを開きます。

2. オブジェクトを含む行で、**【アクション】** をクリックして **【権限】** を選択するか、**【権限の変更】** アイコンをクリックします。

**【権限】** ダイアログボックスには、オブジェクトに対する権限を持つユーザーとグループが一覧表示されます。

**【権限】** ダイアログボックスにユーザーまたはグループが一覧表示されない場合は、そのオブジェクトに対して権限が構成されていません。オブジェクトタイプに対して適切な特権を持つユーザーは、オブジェクトにアクセスできます。

次の図は、マッピングの **【権限】** ダイアログボックスを示しています。

<input type="checkbox"/>	User Name	First Name	Last Name	Read	Update	Delete	Execute	Change Permissions
<input type="checkbox"/>	mclark	Melissa	Clark	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	ajones	Adam	Jones	<input checked="" type="checkbox"/>				
<input type="checkbox"/>	dsmith	David	Smith	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

3. オブジェクトに対するユーザー権限を構成するには:

- a. **【ユーザー】** を選択します。
- b. ユーザーが **【ユーザー】** の一覧に表示されていない場合は、**【追加】** をクリックし、ユーザーを選択します。
- c. ユーザーに対する適切な権限を有効または無効にします。

**注:** オブジェクトに対するユーザー権限を付与すると、Informatica Intelligent Cloud Services によって管理者もオブジェクトに対するアクセス権限を持つユーザーとして追加されます。これにより、権限を構成するときにオブジェクトへのアクセスが失われるのを防ぎます。

4. オブジェクトに対するユーザーグループの権限を構成するには:

- a. **【グループ】** を選択します。
- b. グループが **【グループ】** の一覧に表示されていない場合は、**【追加】** をクリックし、グループを選択します。
- c. グループに対する適切な権限を有効または無効にします。

**注:** オブジェクトに対するグループの権限を付与すると、Informatica Intelligent Cloud Services によって管理者もオブジェクトに対するアクセス権限を持つユーザーとして追加されます。これにより、権限を構成するときにオブジェクトへのアクセスが失われるのを防ぎます。

5. オブジェクトの権限の制限をすべて削除するには、**【権限】** ダイアログボックスからすべてのユーザーとグループを削除します。

すべてのユーザーとグループを削除すると、そのオブジェクトタイプに対して適切な特権を持つすべてのユーザーがオブジェクトにアクセスできるようになります。

6. **【保存】** をクリックします。

# 第 7 章

## スケジュール

タスクまたはタスクフローを、指定した時間または一定の間隔で実行するようにスケジュールを作成できます。また、スケジュールされたタスクまたはジョブが実行されないブラックアウト期間を定義することもできます。

スケジュールを作成し、**Administrator** の管理者ページでブラックアウト期間を設定します。スケジュールを作成した後で、データ統合などの別のサービスのタスクおよびタスクフローに関連付けることができます。

スケジュールを作成するときは、日付と時刻を指定します。関連付けられたアセットを午前 12:00 から午後 11:55 の間の一日中実行するようにスケジュールすることができます。Informatica Intelligent Cloud Services によって、開始時刻、終了時刻などのすべての時間設定に短いスケジュールオフセットが追加される場合があります。その結果、スケジュールされたタスクとタスクフローは、予想よりも後で開始される場合があります。たとえば、正午まで 1 時間ごとに実行するようにスケジュールを設定し、組織のスケジュールオフセットが 10 秒であるとし、Informatica Intelligent Cloud Services では、スケジュールの終了時刻が午後 12:00:10 に延長されます。1 時間ごとの最後のタスクまたはタスクフローは午後 12:00:10 に開始されます。組織のスケジュールオフセットを確認するには、データ統合サービスの **【スケジュールオフセット】** 組織プロパティを確認してください。

スケジュールでは次のタスクを実行できます。

### スケジュールとタスクまたはタスクフローの関連付け

タスクまたはタスクフローにスケジュールを関連付けるには、タスクまたはタスクフローを編集します。例えば、スケジュールをマッピングタスクに関連付けるには、データ統合でマッピングタスクを編集し、**【スケジュール】** ページでスケジュールを選択します。

スケジュールを含むタスクまたはタスクフローをコピーすると、そのスケジュールは新しいアセットに関連付けられません。スケジュールを新しいアセットに関連付けるには、アセットを編集します。

### スケジュール済みタスクの監視

モニタの **【すべてのジョブ】** ページからスケジュールされたタスクを監視することができます。スケジュールされたタスクは、**【マイジョブ】** ページには表示されません。

### スケジュールのエクスポート

組織からスケジュールをエクスポートして、別の組織にインポートできます。**【スケジュール】** ページでスケジュールをエクスポートします。スケジュールがタスクまたはタスクフローに関連付けられている場合、タスクまたはタスクフローはエクスポートファイルに含まれません。

### スケジュールの削除

**【スケジュール】** ページでスケジュールを削除します。

**注:** タスクまたはタスクフローで使用されているスケジュールを削除することはできません。スケジュールを削除する前に、すべてのタスクとタスクフローからスケジュールを削除します。

# ブラックアウト期間の設定

ブラックアウト期間を設定すると、指定した期間中は組織内のすべてのスケジュールされたタスクおよびタスクフローが実行できなくなります。組織には1つのブラックアウト期間を設定できます。

ブラックアウト期間を設定するには、管理者で【スケジュール】を選択し、【ブラックアウト期間】をクリックします。ブラックアウト期間が【スケジュール】ページに表示されます。

## 繰り返し頻度

繰り返し頻度では、タスクを実行する頻度を決定します。以下の表に、繰り返し頻度のオプションを示します。

オプション	説明
繰り返さない	タスクをスケジュールどおりに実行しますが、繰り返しません。
N分ごと	指定した時間（分単位）に基づく間隔でタスクを実行します。以下のオプションを設定することができます。 <ul style="list-style-type: none"><li>- 繰り返し頻度。頻度を分単位で選択します。オプションは、5、10、15、20、30、45です。</li><li>- 日。タスクを実行する曜日。1つ以上の曜日を選択できます。</li><li>- 時間範囲。タスクを開始する時間。[終日]を選択するか、時間範囲を設定します。時間範囲は00時00分から23時55分で設定できます。</li><li>- 繰り返しオプション。タスクを実行する日の範囲。[無期限に繰り返す]を選択するか、終了日時を設定できます。</li></ul>
n時間ごと	スケジュールの開始時刻に基づき、タスクを1時間間隔で実行します。 以下のオプションを設定することができます。 <ul style="list-style-type: none"><li>- 繰り返し頻度。頻度を時間単位で選択します。オプションは、1、2、3、4、6、8、12です。</li><li>- 日。タスクを実行する曜日。1つ以上の曜日を選択できます。</li><li>- 時間範囲。タスクを開始する時間。[終日]を選択するか、時間範囲を設定します。時間範囲は00時00分から23時55分で設定できます。</li><li>- 繰り返しオプション。タスクを実行する日の範囲。[無期限に繰り返す]を選択するか、終了日時を設定できます。</li></ul>
日次	毎日スケジュールで設定した開始時刻にタスクを実行します。 以下のオプションを設定することができます。 <ul style="list-style-type: none"><li>- 繰り返し頻度。タスクを実行する頻度。[毎日]または[すべての平日]を選択します。</li><li>- 繰り返しオプション。タスクを実行する日の範囲。[無期限に繰り返す]を選択するか、終了日時を設定できます。</li></ul>
週次	スケジュールの開始時刻に基づき、1週間間隔でタスクを実行します。 以下のオプションを設定することができます。 <ul style="list-style-type: none"><li>- 日。タスクを実行する曜日。1つ以上の曜日を選択できます。</li><li>- 繰り返しオプション。タスクを実行する日の範囲。[無期限に繰り返す]を選択するか、終了日時を設定できます。</li></ul> <p>曜日を指定しない場合、タスクは開始日と同じ曜日に定期的に行われます。</p>

オプション	説明
隔週	<p>スケジュールの開始時刻に基づき、タスクを 2 週間隔で実行します。</p> <p>以下のオプションを設定することができます。</p> <ul style="list-style-type: none"> <li>- 日。タスクを実行する曜日。1 つ以上の曜日を選択できます。少なくとも 1 つの日を選択する必要があります。</li> <li>- 繰り返しオプション。タスクを実行する日の範囲。[無期限に繰り返す] を選択するか、終了日時を設定できます。</li> </ul> <p>午後 5:00 に開始する隔週スケジュールを火曜日に設定し、タスクを 2 週間隔で月曜日に実行する場合、このスケジュールのタスク実行は次の月曜日に開始します。</p>
月次	<p>スケジュールの開始時刻に基づき、1 カ月間隔でタスクを実行します。</p> <p>以下のオプションを設定することができます。</p> <ul style="list-style-type: none"> <li>- 日付。タスクを実行する日付。次のいずれかのオプションを設定できます。 <ul style="list-style-type: none"> <li>- 1~28 の間で正確な日付を選択します。月の後半のある曜日にタスクを実行する場合は、&lt;n&gt; &lt;day of the week&gt; オプションを使用します。</li> <li>- &lt;n&gt; &lt;day of the week&gt; を選択します。&lt;n&gt; のオプションは、[第 1]、[第 2]、[第 3]、[第 4]、[最終] です。&lt;day of the week&gt; のオプションは、[日]、[日曜日] - [土曜日] です。</li> </ul> <p>ヒント: [日付] オプションでは、月の初日または最終日にタスクを実行するように設定できません。</p> </li> <li>- 繰り返しオプション。タスクを実行する日の範囲。[無期限に繰り返す] を選択するか、終了日時を設定できます。</li> </ul>

## タイムゾーンとスケジュール

Informatica Intelligent Cloud Services は、時間を世界協定時刻 (UTC) で保存します。ログインすると、Informatica Intelligent Cloud Services で時間が変換され、ユーザープロファイルに関連付けられたタイムゾーンで表示されます。

スケジュールを作成するときに、使用するスケジューラのタイムゾーンを選択します。自分のタイムゾーンまたは組織のタイムゾーンとは異なるタイムゾーンを選択できます。

## 夏時間への移行とスケジュール

Informatica Intelligent Cloud Services は、隔週のタスクを除くすべてのタスクに夏時間の変更を適用しません。

夏時間を有効にすると、午前 2 時 00 分 - 午前 2 時 59 分に実行するようにスケジュールされたタスクは、時刻が午前 2 時 00 分から午前 3 時 00 分に変更される日は実行されません。タスクが隔週で午前 2 時に実行するようにスケジュールされている場合は、時刻が変更される日の午前 3 時にそのタスクが実行され、次回は午前 2 時に実行されます。

夏時間により、標準時が開始されるときに午前 1 時 00 分 - 午前 1 時 59 分に実行するようにスケジュールされたタスクが再実行されることはありません。例えば、毎日午前 1 時半に実行するようにスケジュールされたタスクがあるとします。時刻が午前 2 時から午前 1 時に変更されても、このタスクが午前 1 時半に再実行されることはありません。

**ヒント:** Informatica Intelligent Cloud Services で午前 2 時前後の時刻変更時にスケジュールされた実行がスキップされないようにするため、午前 12:59 から午前 3:01 の間はジョブの実行をスケジュールしないでください。

## スケジュールの設定

**【スケジュール】** ページでスケジュールを設定します。マッピングタスクおよび同期タスクの場合は、タスクを構成するときに新しいスケジュールを作成することもできます。スケジュールは、1 回だけ実行するように設定したり、指定した間隔で無期限に、または指定した終了時刻まで実行するように設定したりすることができます。

1. 管理者で **【スケジュール】** を選択します。
2. スケジュールを作成するには、**【新しいスケジュール】** をクリックします。  
スケジュールを編集するには、スケジュールを含む行の編集アイコンをクリックします。
3. 以下のプロパティを設定します。

プロパティ	説明
スケジュール名	スケジュールの名前。 各スケジュール名は組織内で一意である必要があります。スケジュール名には、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。名前の大文字と小文字は区別されません。
説明	スケジュールの説明。 最大長は 255 文字です。
開始	スケジュールを開始する日付と時刻。 日付の形式は MM/DD/YYYY です。時刻は 24 時間形式です。 [カレンダー] ボタンをクリックし、開始日付を選択します。開始日時は、一定間隔で繰り返すタスクおよびタスクフロージョブの繰り返し頻度に影響することがあります。 例えば、開始日が 11 月 10 日で、繰り返し頻度が毎月の場合、スケジュールは毎月 10 日に関連付けられたアセットを実行します。開始時刻を 3 時 10 分、繰り返し頻度を 1 時間にした場合、アセットは毎時 10 分に実行されます。 デフォルトは、スケジュールを作成するユーザーの現在の日付、現在の時刻、およびタイムゾーンです。

プロパティ	説明
タイムゾーン	使用するスケジュールのタイムゾーンを選択します。タイムゾーンは、組織のタイムゾーンやユーザーのタイムゾーンとは異なるものにすることができます。
繰り返す	スケジュールの繰り返し頻度。次のいずれかのオプションを選択します。 <ul style="list-style-type: none"> <li>- 繰り返さない</li> <li>- N分ごと</li> <li>- n時間ごと</li> <li>- 日次</li> <li>- 週次</li> <li>- 隔週</li> <li>- 月次</li> </ul> デフォルトは「繰り返さない」です。

4. **【保存】** をクリックします。

## スケジュールのエクスポート

組織からスケジュールをエクスポートし、それらのスケジュールを他の組織にインポートできます。スケジュールに関連付けられているアセットは、エクスポートファイルには含まれません。**【スケジュール】** ページでスケジュールをエクスポートします。

1. 管理者で **【スケジュール】** を選択します。
2. **【エクスポート】** をクリックします。
3. **【スケジュールのエクスポート】** ダイアログボックスで、エクスポートするスケジュールを選択します。
4. オプションとして、エクスポートジョブ名を更新します。  
デフォルトでは、ジョブ名は SchedulesExport\_<日付>です。
5. **【エクスポート】** をクリックします。  
管理者によって、スケジュールをエクスポートするためのエクスポートジョブが作成されます。
6. エクスポートジョブのステータスを確認し、エクスポートファイルをダウンロードするには、モニタで **【インポート/エクスポートログ】** ページを開き、**【エクスポート】** タブをクリックします。  
エクスポートジョブを含む行で、またはジョブの詳細ページでエクスポートファイルをダウンロードできます。

データ統合など、別のサービスの **【エクスプローラ】** ページでスケジュールをインポートできます。アセットのインポートについて詳しくは、そのサービスのヘルプを参照してください。

スケジュールをインポートした後、それらをターゲット組織のアセットに関連付けることができます。

## スケジュール済みタスクのトラブルシューティング

タスクがスケジュールされた時間に実行されません。

スケジュールがタスクを開始しようとしたときに、タスクの別のインスタンスがすでに実行されている場合、タスクはタスクがスケジュールされた時間に実行されません。例えば、5分ごとに実行するようにタスクをスケジュールしたとします。最初のタスクは12 pm に開始しますが、12:06 pm まで完了しません。最初のインスタンスが完了しないため、タスクの2番目のインスタンスは12:05 pm に実行されません。データ統合は、次のタスクを午後12:10 に開始します。

この問題を解決するには、次のタスクの実行が開始される前にタスクが完了するように、スケジュールを変更します。

## 第 8 章

# バンドル管理

バンドルは関連するマッピング、マッピングタスク、マップレット、および Visio テンプレートのセットであり、データ統合ユーザーがデータ統合プロジェクトで使用できます。データ統合ユーザーはバンドルを設計、作成、およびパブリッシュします。管理者はバンドルを管理します。

組織の管理者である場合は、次の操作を実行してバンドルを管理できます。

### バンドルをインストールする。

バンドル設計者が参照として使用するよう構成した公開、非公開、または非表示バンドルをインストールできます。バンドルはデータ統合のアドオンバンドルプロジェクトにインストールされます。組織のユーザーはバンドル内のアセットを使用できますが、編集することはできません。

### バンドルをコピーする。

バンドル設計者がコピー用に構成した公開、非公開、または非表示バンドルをコピーできます。バンドルをコピーするときに、バンドルの内容をコピーするデータ統合フォルダを選択します。バンドルを複数回コピーし、その内容を毎回別のプロジェクトまたはフォルダに保存することができます。バンドルをコピーすると、組織内のユーザーはアセットを編集できます。

### バンドルをアップグレードする。

バンドルをインストールし、新しいバージョンのバンドルが使用できるようになると、バンドルをアップグレードして最新バージョンを入手できます。

### バンドルをアンインストールする。

インストール済みのバンドルが組織で不要になった場合は、アンインストールすることができます。

インストール済み、または組織で使用可能なバンドルを表示するには、管理者で **【アドオンバンドル】** を選択します。**【アドオンバンドル】** ページには、インストール済みバンドル、コピーされたバンドル、インストールまたはコピーに使用可能なバンドルに関する情報が表示されます。

バンドルタイプの詳細、バンドルの作成、またはバンドルのパブリッシュについては、データ統合サービスのヘルプの「マッピング」を参照してください。

## バンドルのインストール

バンドル設計者が参照として使用するよう構成した公開、非公開、または非表示バンドルをインストールできます。**【アドオンバンドル】** ページの **【使用可能なバンドル】** タブでバンドルをインストールします。

非表示バンドルをインストールする前に、バンドルのアクセスコードを取得します。組織内で作成されたバンドルのアクセスコードを取得するには、データ統合で **【バンドル】** ページを開き、バンドル名をクリックして

**【アクセスコードのコピー】** をクリックします。組織の外部で作成されたバンドルのアクセスコードを取得するには、バンドルパブリッシャに問い合わせてください。

1. 管理者で、**【アドオンバンドル】** を選択します。
2. **【使用可能なバンドル】** をクリックします。  
【使用可能なバンドル】 タブには、インストールまたはコピーに使用できる公開および非公開バンドルが一覧表示されます。
3. インストールするバンドルが非表示バンドルの場合は、**【検索】** フィールドにバンドルのアクセスコードを入力します。
4. バンドル名をクリックして、**【バンドルの詳細】** ページを開きます。
5. **【許可】** フィールドが **【参照】** または **【参照とコピー】** に設定されていることを確認します。  
コピー専用で構成されたバンドルをインストールすることはできません。
6. **【インストール】** をクリックします。

データ統合でバンドルがアドオンバンドルプロジェクトに追加され、アセットが使用できる状態になります。また、バンドルは管理者の **【アドオンバンドル】** ページにある **【インストール済みバンドル】** タブに一覧表示されます。

## バンドルのコピー

バンドル設計者がコピー用に構成した公開、非公開、または非表示バンドルをコピーできます。**【アドオンバンドル】** ページの **【使用可能なバンドル】** タブでバンドルをコピーします。バンドルをコピーするたびに、**【コピーされたバンドル】** タブにイベントが記録されます。

非表示バンドルをコピーする前に、バンドルのアクセスコードを取得してください。組織内で作成されたバンドルのアクセスコードを取得するには、データ統合で **【バンドル】** ページを開き、バンドル名をクリックして **【アクセスコードのコピー】** をクリックします。組織の外部で作成されたバンドルのアクセスコードを取得するには、バンドルパブリッシャに問い合わせてください。

1. 管理者で、**【アドオンバンドル】** を選択します。
2. **【使用可能なバンドル】** をクリックします。  
【使用可能なバンドル】 タブには、インストールまたはコピーに使用できる公開および非公開バンドルが一覧表示されます。
3. コピーするバンドルが非表示バンドルの場合は、**【検索】** フィールドにバンドルのアクセスコードを入力します。
4. バンドル名をクリックして、**【バンドルの詳細】** ページを開きます。
5. **【許可】** フィールドが **【コピー】** または **【参照とコピー】** に設定されていることを確認します。  
参照のみとして使用するように構成されているバンドルをコピーすることはできません。
6. **【バンドルの内容を次の場所にコピー...】** をクリックします。
7. **【参照】** ダイアログボックスで、バンドルの内容をコピーするデータ統合プロジェクトまたはフォルダを選択します。
8. **【選択】** をクリックします。  
バンドル内のアセットが、選択したプロジェクトまたはフォルダにコピーされます。

## バンドルのアップグレード

更新バージョンが入手可能になった時点で、インストール済みバンドルをアップグレードできます。バンドルステータスは、**[アドオンバンドル]** ページの **[インストール済みバンドル]** タブで確認できます。

1. 管理者で、**[アドオンバンドル]** を選択します。
2. **[インストール済みバンドル]** をクリックします。  
[バンドルステータス] 列は、バンドルが最新かどうか、またはアップグレードが利用可能かどうかを示します。
3. バンドル名をクリックして、**[バンドルの詳細]** ページを開きます。
4. **[アップグレード]** をクリックします。

## バンドルのアンインストール

組織内のユーザーがバンドルを必要としなくなった場合は、アンインストールします。**[アドオンバンドル]** ページの **[インストール済みバンドル]** タブでバンドルをアンインストールします。

**注:** バンドルをアンインストールすると、組織のすべてのバンドルアセットが削除されます。バンドル内のアセットを使用するタスクを保持する場合は、タスクでそのアセットを削除してからバンドルをアンインストールします。

1. 管理者で、**[アドオンバンドル]** を選択します。
2. **[インストール済みバンドル]** をクリックします。
3. バンドル名をクリックして、**[バンドルの詳細]** ページを開きます。
4. **[Uninstall (アンインストール)]** をクリックします。

バンドルをアンインストールすると、**[使用可能なバンドル]** タブに一覧表示されます。

## 第 9 章

# イベント監視

アセットおよびセキュリティログを使用して、組織内のアセット、ライセンス、ユーザー、および Secure Agent のイベントを監視できます。ログを表示するには、「監査ログ-表示」特権を持つロールを割り当てる必要があります。

次のログを使用してイベントを監視できます。

### アセットログ

次の情報が表示されます。

- 各アセットが作成、更新、コピー、または削除されたときや、アセットを変更したユーザー名など、アセットのイベント。
- ライセンスが追加、削除、または変更されたときなど、ライセンスに関連するイベント。

アセットログを開くには、管理者を開いて **【ログ】** を選択し、ページ上部の **【アセットログ】** を選択します。

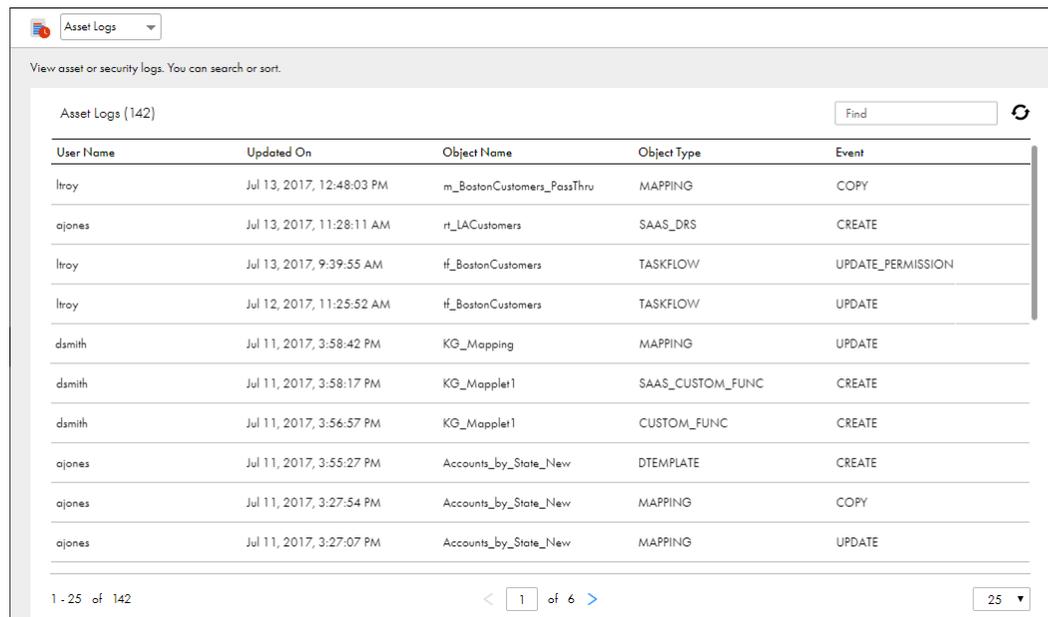
### セキュリティログ

次の情報が表示されます。

- 組織内のユーザーが Informatica Intelligent Cloud Services にログインまたはログアウトしたときなど、ユーザーの認証イベント。
- 各エージェントが作成または更新されたとき、組織情報が更新されたとき、エージェントまたは組織を変更したユーザーの名前など、Secure Agent および組織のイベント。

セキュリティログを開くには、管理者を開いて **【ログ】** を選択し、ページ上部の **【セキュリティログ】** を選択します。

次の図は、アセットログを示しています。



Asset Logs (142)

View asset or security logs. You can search or sort.

User Name	Updated On	Object Name	Object Type	Event
ltroy	Jul 13, 2017, 12:48:03 PM	m_BostonCustomers_PassThru	MAPPING	COPY
ajones	Jul 13, 2017, 11:28:11 AM	rt_LACustomers	SAAS_DRS	CREATE
ltroy	Jul 13, 2017, 9:39:55 AM	if_BostonCustomers	TASKFLOW	UPDATE_PERMISSION
ltroy	Jul 12, 2017, 11:25:52 AM	if_BostonCustomers	TASKFLOW	UPDATE
dsmith	Jul 11, 2017, 3:58:42 PM	KG_Mapping	MAPPING	UPDATE
dsmith	Jul 11, 2017, 3:58:17 PM	KG_Mapplet1	SAAS_CUSTOM_FUNC	CREATE
dsmith	Jul 11, 2017, 3:56:57 PM	KG_Mapplet1	CUSTOM_FUNC	CREATE
ajones	Jul 11, 2017, 3:55:27 PM	Accounts_by_State_New	DTEMPLATE	CREATE
ajones	Jul 11, 2017, 3:27:54 PM	Accounts_by_State_New	MAPPING	COPY
ajones	Jul 11, 2017, 3:27:07 PM	Accounts_by_State_New	MAPPING	UPDATE

1 - 25 of 142

< 1 of 6 >

25 ▼

アセットログには、過去 90 日間のイベントが表示されます。セキュリティログには、過去 400 日間のイベントが表示されます。

ログに表示されるプロパティは、次の方法でカスタマイズできます。

- 列を非表示にするには、列見出し領域を右クリックし、非表示にする列をオフにします。
- ログイベントをソートするには、ソート基準にするプロパティの列見出しをクリックします。ソート順序を逆転させるには、列見出しをもう一度クリックします。
- 特定のイベントのログを検索するには、検索文字列を **[検索]** フィールドに入力します。オブジェクト名またはイベントタイプを検索できます。

## 第 10 章

# セキュリティのトラブルシューティング

次のセキュリティ違反エラーを受信しました。

There may have been a security violation while accessing the site. Verify that there are no malicious scripts running in your browser. This error also appears when you submit the form multiple times through a browser reload.

このエラーは、ページのオプションをクリックしたときに、そのページが前回のクリックによるロードを実行中であるときに発生します。データ統合に戻るには、[\[ここ\]](#) のリンクをクリックしてください。

接続、レプリケーションタスクなどのオブジェクトに関する詳細を表示しようとする、[\[オブジェクトが見つかりません\]](#) ページが表示されます。

オブジェクトは最近削除されました。オブジェクトが存在しないと、[\[オブジェクトが見つかりません\]](#) ページが表示されます。ページを更新して、現在のオブジェクトを表示します。

タスクを実行しようとする、[\[アクセスが拒否されました\]](#) ページが表示されます。

使用しているユーザーアカウントでの実行許可がないタスクを実行しようとする、[\[アクセスが拒否されました\]](#) ページが表示されます。タスクを実行するための適切なロールまたはアセットの権限がない可能性があります。タスクを実行する必要がある場合は、組織の管理者にユーザーアカウントの確認を依頼してください。

# 索引

## A

Administrator サービス

概要 [8](#)

Azure DevOps ユーザー資格情報 [47](#)

Azure のデータアクセラレータ

Enterprise Data Catalog との統合 [16](#)

## C

Cloud Application Integration コミュニティ

URL [6](#)

Cloud 開発者コミュニティ

URL [6](#)

## E

Enterprise Data Catalog

Informatica Intelligent Cloud Services との統合 [16](#)

## G

GitHub ユーザー資格情報 [47](#)

## I

Informatica Intelligent Cloud Services

Web サイト [6](#)

Informatica グローバルカスタマサポート

連絡先情報 [7](#)

IPU メーター [36](#), [38](#)

IPU 使用率

レポート [39](#)

IPU 使用量

監視 [37](#)

IP アドレスフィルタリング

設定 [14](#)

## S

Secure Agent

接続プロパティの保存 [15](#)

Secure Agent サービス

アップグレード設定 [41](#)

ローリングアップグレード [49](#)

ローリングアップグレードエラーの処理 [50](#)

再開スケジュールの設定 [50](#)

## W

Web サイト [6](#)

## あ

アセットログ

最大ログエントリ [15](#)

表示 [65](#)

アップグレード通知 [7](#)

アドオンバンドル

バンドルを参照してください。 [62](#)

アプリケーションの統合

メータリングの使用状況レポート [34](#)

## い

イベント

監視 [65](#)

## か

ガイドライン

ロゴおよびファビコン [51](#)

カスタムブランディング

設定 [41](#)

組織の設定 [51](#)

## さ

サーバーレスランタイム環境

サーバーレスコンピューティングユニット [33](#)

メータリングの使用状況レポート [34](#)

サブ組織

ライセンスの同期 [27](#)

Enterprise Data Catalog 統合プロパティ [16](#)

アセットのエクスポートとインポート [22](#)

アドオンコネクタ [21](#)

カスタムブランディングの設定 [51](#)

スケジュールオフセット [15](#)

ソース管理の無効化 [46](#)

ソース管理の有効化 [44](#)

ソース管理リポジトリの変更 [45](#)

ソース管理設定 [41](#), [43](#)

データ統合サービスのプロパティ [15](#)

プロパティ [12](#)

メータリング [29](#)

ライセンス [26](#)

ライセンスの編集 [27](#)

ライセンスの有効期限 [28](#)

既存サブ組織の削除 [20](#)

既存組織のリンク [19](#)

## サブ組織 (続く)

- 作成 [18](#)
- 作成する理由 [17](#)
- 削除 [19](#)
- 親組織からのリンク解除 [20](#)
- 親組織のアクセスを拒否 [21](#)
- 接続プロパティの保存 [15](#)
- 全般プロパティ [13](#)
- 組織タイプ [27](#)
- 追加 [18](#)
- 認証プロパティ [14](#)
- 別の組織への切り替え [21](#)
- 無効化および有効化 [20](#)
- 例 [17](#)

## し

- システムステータス [7](#)
- ジョブの使用状況
- 監視 [30](#)
- ジョブの制限数
- 監視 [30](#)

## す

- スカラ
- IPU メーター [37](#)
- スケジュール
- Secure Agent サービスの再開 [50](#)
- インポート [60](#)
- エクスポート [60](#)
- スケジュールオフセット [15](#)
- スケジュール済みタスクの監視 [56](#)
- タイムゾーン [58](#)
- タスクまたはタスクフローとの関連付け [56](#)
- ブラックアウト期間の設定 [57](#)
- 夏時間 [58](#)
- 繰り返し頻度 [57](#)
- 削除 [56](#)
- 設定 [59](#)
- 説明 [56](#)
- ステータス
- Informatica Intelligent Cloud Services [7](#)

## せ

- セキュリティ
- トラブルシューティング [67](#)
- セキュリティログ
- 最大ログエントリ [15](#)
- 表示 [65](#)
- セッションのアイドルタイムアウト
- 設定 [14](#)

## そ

- ソース管理
- OAuth を使用したアクセスの設定 [43](#)
- オンプレミスリポジトリ [43](#)
- サブ組織の設定 [43](#)
- チェックアウトの取り消し [49](#)
- ベストプラクティス [47](#)
- リポジトリ URL の変更 [45](#)
- リポジトリへのアクセスの設定 [47](#)

## ソース管理 (続く)

- リポジトリへの読み取り/書き込みアクセスの設定 [41](#)
- リポジトリへの読み取り専用アクセスの設定 [41](#)
- 開発ガイドライン [47](#)
- 設定 [41](#)
- 設定のガイドライン [47](#)
- 組織の設定 [41](#)
- 組織の無効化 [46](#)
- 組織の有効化 [44](#)

## た

- タイムゾーン
- 説明 [58](#)

## て

- データ統合のデータカタログページ
- 表示と非表示 [16](#)

## と

- トラブルシューティング
- セキュリティ [67](#)

## は

- パスワード
- 再利用 [14](#)
- 最小混合文字数 [14](#)
- 最小長 [14](#)
- 有効期限 [14](#)
- バンドル
- アップグレード [64](#)
- アンインストール [64](#)
- インストール [62](#)
- コピー [63](#)
- 管理 [62](#)
- 表示 [62](#)

## ふ

- ブラックアウト期間
- 組織用の設定 [57](#)

## め

- メータリング
- IPU スカラ [37](#)
- IPU メーター [36, 38](#)
- IPU メトリックの表示 [37](#)
- IPU 使用率レポート [39](#)
- IPU 使用量の表示 [37](#)
- サーバーレスコンピューティングユニット [33](#)
- すべてのメーターの表示 [30](#)
- メーター定義 [31](#)
- ライセンスメトリックの表示 [30](#)
- 使用状況のグラフの表示 [35](#)
- 使用状況の詳細の表示 [35](#)
- 使用状況レポート [34](#)
- 組織とサブ組織 [29](#)

メータリングの使用状況レポート  
ダウンロード [34](#)  
情報 [34](#)  
メンテナンスの停止 [7](#)

## ら

ライセンス  
サブ組織 [26](#)  
サブ組織タイプの設定 [27](#)  
サブ組織のライセンスの編集 [27](#)  
タイプ [26](#)

ライセンス (続く)  
管理 [25](#)  
有効期限 [28](#)  
ライセンスメーター [29](#)  
ライセンスメトリック  
表示 [30](#)

## ろ

ログインの拒否  
トラブルシューティング [67](#)