Informatica® Cloud Data Integration

Amazon S3 V2 コネクタ

Informatica Cloud Data Integration Amazon S3 V2 コネクタ
2022 年 10 月

© 著作権 Informatica LLC 2017, 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 ロゴ、Informatica Cloud、および PowerCenter 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。

特許については、https://www.informatica.com/legal/patents.html を参照してください。

免責: 本文書は、一切の保証を伴わない「現状渡し」で提供されるものとし、Informatica LLC は他社の権利の非侵害、市場性および特定の目的への適合性の黙示の保証などを含めて、一切の明示的および黙示的保証の責任を負いません。Informatica LLC では、本ソフトウェアまたはドキュメントに誤りのないことを保証していません。本ソフトウェアまたはドキュメントに記載されている情報には、技術的に不正確な記述や誤植が含まれる場合があります。本ソフトウェアまたはドキュメントの情報は、予告なしに変更されることがあります。

NOTICES

この Informatica 製品（以下「ソフトウェア」）には、Progress Software Corporation（以下「DataDirect」）の事業子会社である DataDirect Technologies からの特定のドライバ（以下「DataDirect ドライバ」）が含まれています。DataDirect ドライバには、次の用語および条件が適用されます。

1. DataDirect ドライバは、特定物として現存するままの状態で提供され、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任を負わないものとします。国または地域によっては、法律の強行規定により、保証責任の制限が禁じられる場合、強行規定の制限を受けるものとします。
2. DataDirect または第三者は、予見の有無を問わず発生した ODBC ドライバの使用に関するいかなる直接的、間接的、偶発的、特別、あるいは結果的損害に対して責任を負わないものとします。本制限事項は、すべての訴訟原因に適用されます。訴訟原因には、契約違反、保証違反、過失、厳格責任、詐称、その他の不法行為を含みますが、これらに限るものではありません。

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 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。

発行日: 2022-12-05

目次

序文 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

第 1 章 : Amazon S3 V2 コネクタの概要 8

Amazon S3 V2 コネクタアセット 8

Amazon S3 の概要 9

認証メソッド 9

Amazon S3 V2 コネクタの管理 9

サーバーレスランタイム環境でクライアントサイド暗号化を設定するための前提条件 10

詳細モードのマッピングに SSE-KMS 暗号化を設定するための前提条件 10

最小限の Amazon IAM ポリシーの作成 11

IAM 認証 11

AssumeRole を使用した一時的なセキュリティ資格情報 12

資格情報プロファイルファイルの認証 15

Amazon S3 とのプライベート通信 16

第 2 章 : Amazon S3 V2 接続 17

Amazon S3 V2 接続プロパティ 17

AWS リージョンのルールとガイドライン 22

S3 互換ストレージのルールおよびガイドライン 22

プロキシの設定 22

JVMOption を使用したプロキシ設定 23

Windows でのプロキシ設定 23

Linux でのプロキシ設定 24

プロキシ設定のバイパス 24

第 3 章 : Amazon S3 V2 ソースとターゲット 26

Amazon S3 V2 ソース 26

Amazon S3 V2 ソースでのデータ暗号化 27

Amazon S3 V2 ソースのソースタイプ 28

複数のファイルからの読み込み 29

ファイルの増分ロード 31

ワイルドカード文字. 31
ディレクトリからのファイルの再帰読み取り. 32
ソースパーティション. 33
ソースオブジェクトパスの読み取り. 33
プッシュダウンの最適化. 34
Amazon S3 V2 ターゲット. 34
Amazon S3 V2 ターゲットでのデータ暗号化. 34
既存のファイルの上書き. 36
ターゲットのパーティション化. 36
ディレクトリレベルのパーティショニング. 37
パーティションディレクトリへの増分書き込み. 40
分散カラム. 41
複数のターゲットオブジェクトへの書き込み. 41
オブジェクトタグ. 42
Amazon S3 V2 のソースとターゲットでのデータ圧縮. 43
圧縮フラットファイルの読み取り. 44
圧縮 JSON ファイルの読み取り. 45
固定長ファイル形式. 45

第 4 章 : マッピングの Amazon S3 V2 オブジェクト. 47
マッピングでの Amazon S3 V2 ソース. 47
マッピングの Amazon S3 V2 ターゲット. 50
Amazon S3 V2 ルックアップ. 54
ファイル形式オプション. 54
形式オプションの設定に関するルールとガイドライン. 57
ターゲットの指定. 58
ターゲットの作成に関するルールとガイドライン. 58
Amazon S3 V2 ターゲットファイルのパラメータ化. 59
タイムスタンプを使用したパラメータ化 60
パラメータファイルを使用したパラメータ化. 60
詳細モードのマッピングのルールとガイドライン. 61
詳細モードのマッピングの例. 62

第 5 章 : マッピングの移行. 64
移行されたマッピングへの同じオブジェクトパスの使用. 64
同じオブジェクトパスに関するルールとガイドライン. 64
移行されたマッピングへの別のオブジェクトパスの使用. 65
移行オプション. 65
ルールおよびガイドライン. 66

第 6 章 : Amazon S3 V2 コネクタへのアップグレード. 68
接続タイプのアップグレード. 68
接続切り替えの例. 69

切り替え後に保持される詳細プロパティ. 71

第 7 章 : データ型リファレンス. 72

フラットファイルデータ型とトランスフォーメーションデータ型. 72

Avro Amazon S3 ファイルデータ型とトランスフォーメーションデータ型. 73

Date、Decimal、および Timestamp 型の有効化. 74

JSON Amazon S3 ファイルデータ型とトランスフォーメーションデータ型. 75

ORC Amazon S3 ファイルデータ型とトランスフォーメーションデータ型. 76

Parquet Amazon S3 のファイルデータ型とトランスフォーメーションデータ型. 77

第 8 章 : トラブルシューティング. 79

Amazon S3 V2 コネクタのトラブルシューティング. 79

トラブルシューティング FAQ. 80

索引. 82

序文

*Amazon S3 V2 コネクタ*を使用すると、Cloud データ統合を使って Amazon S3 に対して読み書きを行う方法を学べます。また、Cloud データ統合で Amazon S3 V2 接続を作成する方法や、マッピング、マッピングタスク、動的マッピングタスク、およびデータ転送タスクを開発および実行する方法を確認します。処理用のトランスフォーメーションロジックを Amazon Redshift データベースにプッシュダウンする方法についても説明します。

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）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 マーケットプレース

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）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

Amazon S3 V2 コネクタの概要

Amazon S3 V2 コネクタを使用すると、データ統合から Amazon S3 に接続できます。

Windows 上では、Amazon S3 V2 コネクタを使用して Avro、JSON、ORC、および Parquet ファイルを読み書きすることはできません。Avro、Parquet、JSON、および ORC ファイルに対しプリミティブデータ型の読み書きを行うことができます。

Amazon S3 V2 接続を作成し、マッピングまたはマッピングタスクでこの接続を使用できます。詳細モードでは、Mapping Designer で、高度な機能を有効にするためのトランスフォーメーションと関数を含むようにマッピングキャンバスが更新されます。詳細クラスタは、セルフサービスクラスタ、ローカルクラスタであるか、または Amazon Web Services でホストされているクラスタです。

Amazon S3 V2 コネクタを使用して、マッピングでは Avro、フラット、バイナリ、ORC、および Parquet ファイル形式の読み取りまたは書き込みを行い、詳細モードのマッピングでは Avro、フラット、ORC、Parquet、および JSON ファイル形式の読み取りまたは書き込みを行います。詳細モードのマッピングでは Avro、Parquet および JSON に対してのみ、階層データ型の読み書きを行うことができます。

マッピングタスクを作成して、マッピングまたは統合テンプレートで定義されているデータフローロジックに基づきデータを処理します。

注: ローカルクラスタのサポートはプレビューで利用できます。評価目的でのプレビュー機能はサポートされていますが、保証されておらず、本番環境には対応していません。非本番環境でのみ使用することをお勧めします。Informatica は、本番環境用の今後のリリースにプレビュー機能を含める予定ですが、市場や技術的な状況の変化に応じて導入を行わない場合もあります。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。

Amazon S3 V2 コネクタアセット

データ統合でアセットを作成し、Amazon S3 V2 コネクタを使用してデータを統合します。

Amazon S3 V2 コネクタを使用する場合は、次のようなデータ統合アセットを含めることができます。

- データ転送タスク
- 動的マッピングタスク
- マッピング
- マッピングタスク

アセットとトランスフォーメーションの設定に関する詳細については、データ統合のドキュメントの「*マッピング*」、「*トランスフォーメーション*」、および「*タスク*」を参照してください。

Amazon S3 の概要

Amazon Simple Storage Service（Amazon S3）は、ソースからデータをコピーして、任意のターゲットに同時にデータを移動できるストレージサービスです。Amazon S3 を使用して、構成されたソース接続のリストから Amazon S3 ターゲットにファイルを転送できます。AWS Management Console の Web インタフェースを使用してタスクを実行できます。

Amazon S3 は、データをオブジェクトとしてバケット内に格納します。オブジェクトは、ファイルおよび必要に応じてそのファイルを記述する任意のメタデータで構成されます。バケットはオブジェクトのコンテナです。1 つ以上のバケットを持つことができます。AWS Management Console を使用する場合、フォルダを作成してオブジェクトをグループ化しフォルダをネストできます。

認証メソッド

Amazon S3 V2 コネクタは、以下の認証メソッドをサポートしています。

- **基本認証**: 基本認証を設定するには、アクセスキーと秘密鍵の値を指定します。
- **IAM 認証**: Secure Agent が Amazon Elastic Compute Cloud（EC2）システムで実行している場合は、IAM 認証を設定できます。
- **AssumeRole 経由の一時的なセキュリティ資格情報**: **AssumeRole** を使用した一時的なセキュリティ資格情報を設定すると、同じ AWS アカウントまたは異なる AWS アカウントから AWS リソースにアクセスできます。
- **資格情報プロファイルファイルの認証**: アクセスキー、秘密鍵、およびセッショントークンを含む資格情報ファイルから Amazon S3 資格情報にアクセスできます。
- **統合ユーザーシングルサインオン**: 統合ユーザーシングルサインオンで Amazon S3 リソースへのアクセスを安全に制御するように設定できます。

Amazon S3 V2 コネクタの管理

ユーザーは、組織管理者が Amazon S3 V2 コネクタの最小限の Amazon Identity and Access Management（IAM）ポリシーを作成した後、Amazon S3 V2 コネクタを使用できます。これとは別に、組織管理者は次のタスクを実行します。

クライアントサイドおよびサーバーサイドの暗号化の前提条件

- クライアントサイド暗号化を有効にする場合は、マスタ対称キーを作成します。
- Key Management Service（KMS）を使用した暗号化を有効にする場合は、AWS KMS ポリシー、および AWS KMS で管理された顧客マスタキーを作成します。

Informatica Encryption **の前提条件**

- Informatica Encryption 方式を使用してバイナリファイルまたはフラットファイルのデータを暗号化または復号化する場合は、Informatica 暗号ライブラリのライセンスが有効になっていることを確認します。

AssumeRole **経由の一時的なセキュリティ資格情報の前提条件**

- **sts:AssumeRole** 権限を持っていて、AWS アカウント内に一時的なセキュリティ資格情報を使用して AWS リソースにアクセスするための信頼関係が構築されていることを確認します。
- 一時的なセキュリティ資格情報のポリシーを作成し、その一時的なセキュリティ資格情報を使用して AWS リソースにアクセスします。

サーバーレスランタイム環境でクライアントサイド暗号化を設定するための前提条件

Amazon S3 V2 コネクタでサーバーレスランタイム環境を使用して、クライアントサイドの暗号化を設定できます。

サーバーレスランタイム環境を使用してクライアントサイド暗号化を設定する前に、.yml サーバーレス構成ファイルを設定する必要があります。

.yml **サーバーレス構成ファイルを設定する**

次の手順を実行して、サーバーレスランタイム環境で.yml サーバーレス構成ファイルを設定し、Amazon S3 V2 コネクタがクライアントサイド暗号化を使用できるようにします。

1. 次のコードスニペットをテキストエディタにコピーします。

```
version: 1
agent:
  agentAutoApply:
    general:
    jdk:
         security:
         policyJars:
           - local_policy.jar
        - US_export_policy.jar
```

2. 構文とインデントが有効であることを確認してから、ファイルを `serverlessUserAgentConfig.yml` として次の AWS の場所に保存します。

   `<Supplementary file location>/serverless_agent_config`

   .yml ファイルが実行されると、ポリシー jar が AWS の場所からサーバーレスエージェントディレクトリにコピーされます。

3. .yml 構成ファイルを更新した後、サーバーレスランタイム環境を再デプロイします。

接続プロパティでマスタ対称キーを指定し、詳細ソースプロパティおよび詳細ターゲットプロパティでクライアントサイドの暗号化タイプを指定します。

詳細モードのマッピングに SSE-KMS 暗号化を設定するための前提条件

詳細モードのマッピングに SSE-KMS 暗号化を使用するには、次のいずれかのタスクを実行する必要があります。

- `~/.aws/credentials` の場所にある資格情報を使用するには、AWS でマスターインスタンスプロファイルとワーカーインスタンスプロファイルを作成し、KMS ポリシーをワーカープロファイルにアタッチして、クラスタ設定でプロファイルを指定する必要があります。
- Amazon EC2 で Secure Agent を使用し、AWS でマスターインスタンスプロファイルとワーカーインスタンスプロファイルを作成して、KMS ポリシーをワーカープロファイルにアタッチします。
- Amazon EC2 で Secure Agent を使用し、デフォルトの IAM ロールを使用して、KMS ポリシーを Secure Agent ロールにアタッチします。

最小限の Amazon IAM ポリシーの作成

AWS コンソールで IAM ポリシーを設定できます。AWS IAM 認証を使用すると、Amazon S3 リソースへのアクセスを安全に制御できます。

ユーザーが、Amazon S3 バケットからデータを正常に読み取ることができるようにするには、次に示す最低限必要なポリシーを使用します。

- GetObject
- ListBucket

ユーザーが、Amazon S3 バケットにデータを正常に書き込むことができるようにするには、次に示す最低限必要なポリシーを使用します。

- PutObject
- GetObject
- DeleteObject
- ListBucket
- ListBucketMultipartUploads.詳細モードのマッピングにのみ適用されます。

次のサンプルポリシーは、Amazon S3 バケットにデータを書き込むための最小限の Amazon IAM ポリシーを示しています。

```
{
    "Version": "2012-10-17",
    "Statement":
    [
        {
            "Effect": "Allow",
            "Action":[
                "s3:PutObject",
                "s3:GetObject",
                "s3:DeleteObject",
                "s3:ListBucket",
                "s3:ListBucketMultipartUploads"
                    ],
            "Resource": [
                "arn:aws:s3:::<bucket_name>/*",
                "arn:aws:s3:::<bucket_name>"
                        ]
        }
    ]
}
```

詳細モードのマッピングの場合、同じ AWS リージョン内で異なる AWS アカウントを使用できます。マッピングで使用する AWS アカウントへのアクセスが Amazon IAM ポリシーで承認されていることを確認します。

IAM 認証

必要に応じて、接続でアクセスキーと秘密鍵を入力しない場合、Amazon S3 V2 コネクタでは AWS 資格情報プロバイダチェーンが使用され、資格情報が次の順序で検索されます。

1. **AWS_ACCESS_KEY_ID** と **AWS_SECRET_ACCESS_KEY** または **AWS_ACCESS_KEY** と **AWS_SECRET_KEY** 環境変数。
2. **aws.accessKeyId** と **aws.secretKey** java システムプロパティ。
3. デフォルトの場所`~/.aws/credentials` にある資格情報プロファイルファイル。
4. Amazon EC2 メタデータサービスによって配信されるインスタンスプロファイル資格情報。

Secure Agent が Amazon Elastic Compute Cloud（EC2）システムで実行されている場合は、IAM 認証を設定できます。サーバーレスランタイム環境を使用している場合、IAM 認証を設定することはできません。

EC2 で IAM 認証を設定するには、次の手順を実行します。

1. 最小限の Amazon IAM ポリシーを作成します。
2. Amazon EC2 ロールを作成します。Amazon EC2 ロールは、EC2 システムを作成する場合に使用されます。Amazon EC2 ロールの作成の詳細については、AWS のマニュアルを参照してください。
3. 最小限の Amazon IAM ポリシーを Amazon EC2 ロールにリンクします。
4. EC2 インスタンスを作成します。手順 2 で作成した Amazon EC2 ロールを EC2 インスタンスに割り当てます。
5. EC2 システムにセキュアエージェントをインストールします。

セッションを実行するときに、Amazon S3 リソースへのアクセスを安全に制御するために IAM 認証を使用します。

AssumeRole を使用した一時的なセキュリティ資格情報

AssumeRole を使用した一時的なセキュリティ資格情報を使用すると、同じ AWS アカウントまたは異なる AWS アカウントから AWS リソースにアクセスできます。

sts:AssumeRole 権限を持っていて、AWS アカウント内に一時的なセキュリティ資格情報を使用するための信頼関係が構築されていることを確認します。信頼関係は、IAM ロールを作成するときに、IAM ロールの信頼ポリシーで定義されます。IAM ロールは、IAM ユーザーを信頼されたエンティティとして追加し、IAM ユーザーに一時的なセキュリティ資格情報の使用と AWS アカウントへのアクセスを許可します。信頼関係を構築する方法の詳細については、AWS のマニュアルを参照してください。

信頼された IAM ユーザーが一時的なセキュリティ資格情報を要求すると、AWS Security Token Service（AWS STS）が、指定した期間有効な一時的なセキュリティ資格情報を動的に生成し、その資格情報を信頼された IAM ユーザーに提供します。一時的なセキュリティ資格情報は、アクセスキー ID、シークレットアクセスキー、シークレットトークンで構成されます。

動的に生成された一時的なセキュリティ資格情報を使用するには、Amazon S3 V2 接続を作成するときに **[IAM ロール ARN]** 接続プロパティの値を入力します。IAM ロール ARN は、AWS リソースを一意に識別します。次に、**[一時的な資格情報の期間]** 詳細ソースプロパティおよびターゲットプロパティで、一時的なセキュリティ資格情報を使用できる期間を秒単位で指定します。

外部 ID

Amazon S3 バケットが別の AWS アカウントにある場合に、Amazon S3 バケットへのより安全なクロスアカウントアクセスを確立するための外部 ID を指定できます。

必要に応じて、AWS Security Token Service（STS）への AssumeRole 要求で外部 ID を指定できます。

外部 ID は文字列である必要があります。

次のサンプルは、引き継がれた IAM ロールの信頼ポリシー内の外部 ID 条件を示しています。

```
"Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::AWS_Account_ID : user/user_name"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "sts:ExternalId": "dummy_external_id"
        }
      }
```

```
    }
  ]
```

一時的なセキュリティ資格情報のポリシー

一時的なセキュリティ資格情報を使用して AWS リソースにアクセスするには、IAM ユーザーと IAM ロールの両方にポリシーが必要です。

次のセクションに、IAM ユーザーと IAM ロールに必要なポリシーを示します。

IAM **ユーザー**

IAM ユーザーは、同じ AWS アカウントまたは異なる AWS アカウントで一時的なセキュリティ資格情報を使用するために、`sts:AssumeRole` ポリシーを持っている必要があります。

次のサンプルポリシーでは、IAM ユーザーに AWS アカウントで一時的なセキュリティ資格情報を使用することを許可しています。

```
{
"Version":"2012-10-17", "Statement":{ "Effect":"Allow", "Action":"sts:AssumeRole",
"Resource":"arn:aws:iam::<ACCOUNT-HYPHENS>:role/<ROLE-NAME>" }
}
```

次のサンプルポリシーでは、中国地域の IAM ユーザーに AWS アカウントで一時的なセキュリティ資格情報を使用することを許可しています。

```
{
"Version":"2012-10-17", "Statement":{ "Effect":"Allow", "Action":"sts:AssumeRole", "Resource":"arn:aws-
cn:iam::<ACCOUNT-HYPHENS>:role/<ROLE-NAME>" }
}
```

IAM **ロール**

IAM ロールは、IAM ユーザーに一時的なセキュリティ資格情報を使用して AWS リソースにアクセスすることを許可するために、`sts:AssumeRole` ポリシーと、IAM ロールにアタッチされた信頼ポリシーを持っている必要があります。ポリシーは、IAM ユーザーがアクセスできる AWS リソースと、IAM ユーザーが実行できるアクションを指定します。信頼ポリシーは、AWS リソースにアクセスできる AWS アカウントの IAM ユーザーを指定します。

次のポリシーは、サンプルの信頼ポリシーです。

```
{
"Version":"2012-10-17", "Statement":[{ "Effect":"Allow", "Principal":{ "AWS":"arn:aws:iam::AWS-account-
ID:root" },
"Action":"sts:AssumeRole" }
 ]
  }
   }
```

このポリシーでは、`Principal` 属性で、動的に生成された一時的なセキュリティ資格情報を使用できる IAM ユーザーの ARN も入力することができ、それ以上のアクセスを制限できます。以下に例を示します。

```
"Principal" : { "AWS" : "arn:aws:iam:: AWS-account-ID :user/ user-name " }
```

AWS Key Management Service（AWS KMS）で管理された顧客マスターキーを使用する一時的なセキュリティ資格情報を使用し、KMS を使用した暗号化を有効にするには、KMS ポリシーを作成する必要があります。

次の操作を実行すると、一時的なセキュリティ資格情報を使用し、KMS を使用した暗号化を有効にすることができます。

- GenerateDataKey
- DescribeKey
- 暗号化
- 復号化

- ReEncrypt

サンプルポリシー:

```
{
"Version":"2012-10-17", "Statement":[{ "Effect":"Allow", "Action":[ "kms:GenerateDataKey", "kms:DescribeKey",
"kms:Encrypt", "kms:Decrypt", "kms:ReEncrypt*" ], "Resource": ["arn:aws:kms:region:account:key/<KMS_key>"]
    }
  ]
   }
```

KMS を設定し、中国地域の Amazon S3 エンドポイントにアクセスする場合は、次のサンプルポリシーを使用します。

```
{
"Version":"2012-10-17", "Statement":[{ "Effect":"Allow", "Action":[ "kms:GenerateDataKey", "kms:DescribeKey",
"kms:Encrypt", "kms:Decrypt", "kms:ReEncrypt*" ], "Resource": ["arn:aws-cn:kms:region:account:key/<KMS_key>"]
    }
  ]
   }
```

EC2 の AssumeRole を使用した一時的なセキュリティ資格情報

AssumeRole を使用して一時的なセキュリティ認証情報を使用し、Amazon EC2 ロールが同じ AWS アカウントまたは異なる AWS アカウントから AWS リソースにアクセスすることができます。

Amazon EC2 ロールは、永続的なアクセスキーと秘密鍵を必要とせずに、同じ AWS アカウントまたは異なる AWS アカウントから別の IAM ロールを引き受けることができるようになります。Amazon EC2 ロールは、別のリージョンから別の IAM ロールを引き受けることもできます。

AssumeRole for EC2 を使用して一時的なセキュリティ認証情報を使用する場合は、次の前提条件を考慮してください。

- AssumeRole for EC2 を使用して一時的なセキュリティ認証情報を使用するには、Amazon EC2 などの AWS サービスに Secure Agent をインストールします。
- AWS EC2 サービスにアタッチされた EC2 ロールは、Amazon S3 へのアクセス権を持っていてはいけませんが、別の IAM ロールを引き受ける権限が必要です。
- EC2 ロールが引き受ける必要のある IAM ロールには、アクセス許可ポリシーと信頼ポリシーがアタッチされている必要があります。
  EC2 ロールおよび IAM ロールのポリシーの詳細については、「一時的なセキュリティ資格情報のポリシー」(ページ 13)を参照してください。

[IAM ロール ARN] 接続プロパティで指定した IAM ロールを引き受けるように EC2 ロールを設定するには、接続プロパティの **[ロールの引き受けに EC2 ロールを使用]** チェックボックスをオンにします。

一時セキュリティ資格情報の使用に関するルールおよびガイドライン

一時セキュリティ資格情報の使用については、次のガイドラインを参照してください。

- 一時的なセキュリティ認証情報を要求する IAM ユーザーまたは IAM ロールは、AWS リソースへのアクセス権を持っていてはいけません。
- 認証済み IAM ユーザーまたは IAM ロールのみ、AWS Security Token Service（AWS STS）から一時セキュリティ資格情報を要求できます。
- タスクを実行する前に、一時セキュリティ資格情報の有効期間が、そのタスクを実行するのに十分な長さであることを確認してください。実行中のタスクに対して、一時セキュリティ資格情報の有効期間を延長することはできません。例えば、Amazon Redshift との間で読み取りと書き込みを行い、一時的なセキュリティ認証情報の有効期限が切れた場合、一時的なセキュリティ認証情報の期間を延長することはできないので、タスクが失敗する原因となります。

- 一時セキュリティ資格情報の有効期限が切れると、AWS は、その資格情報を使ったリソースへのアクセスを IAM ユーザーまたは IAM ロールに許可しません。マッピングで現在使用している一時セキュリティ資格情報の有効期限が切れる前に、新しい一時セキュリティ資格情報を要求する必要があります。
- 詳細モードのマッピングの場合、**[一時的な資格情報の期間]** の詳細なソースプロパティで設定した時間が経過した後でも、一時的なセキュリティ資格情報は期限切れにはなりません。
- 一時セキュリティ資格情報を使用するのに、AWS アカウントのルートユーザー資格情報を使用しないでください。一時セキュリティ資格情報を使用するには、IAM ユーザーの資格情報を使用する必要があります。
- 一時セキュリティ資格情報を使って Avro、ORC、Parquet 形式などの複合ファイルからデータを読み取ったり、これらのファイルにデータを書き込むには、現在の環境に Hadoop ディストリビューションが必要です。ただし、一時セキュリティ資格情報を使ってフラットファイルからデータを読み取ったり、フラットファイルにデータを書き込む場合については、Amazon S3 V2 コネクタは Hadoop ディストリビューションを必要としません。
- マッピング内のソースとターゲットの両方が同じ Amazon S3 バケットを指している場合は、ソーストランスフォーメーションとターゲットトランスフォーメーションで同じ Amazon S3 接続が使用されます。異なる 2 つの Amazon S3 接続を使用する場合は、両方の接続に対して接続プロパティで同じ値を設定します。
- マッピング内のソースとターゲットが異なる Amazon S3 バケットを指している場合、異なる 2 つの Amazon S3 接続を使用できます。
  両方の接続に対して、接続プロパティで異なる値を設定できます。ただし、接続プロパティで **[ロールの引き受けに EC2 ロールを使用]** チェックボックスをオンにする必要があります。また、ソースプロパティとターゲットプロパティの **[一時的な資格情報の期間]** フィールドにも同じ値を指定する必要があります。
- マッピングで、異なる IAM ロールを持つ同じ Amazon S3 バケットに対して 2 つ以上の Amazon S3 データソースを設定した場合、いずれかの IAM ロールに他のデータソースへのアクセス権を持つようにする必要があります。
- マッピングで、一方の Amazon S3 データソースをユーザー認証情報で設定し、もう一方の Amazon S3 データソースを IAM ロールで設定する場合は、次のルールを考慮してください。
  - 最初のデータソースのユーザー認証情報は、2 番目の Amazon S3 データソースの IAM ロールを引き受けることもできるようにする必要があります。
  - 2 番目のデータソース用に設定した IAM ロールは、最初の Amazon S3 データソースへのアクセス権を持つようにする必要もあります。

資格情報プロファイルファイルの認証

アクセスキーと秘密鍵を含む認証情報プロファイルファイルを介して、Amazon S3 との接続を確立するために必要な認証情報を指定できます。一時的なセキュリティ資格情報を使用する場合、資格情報プロファイルファイルには、アクセスキー、秘密鍵、およびセッショントークンが含まれます。

資格情報プロファイルファイルの認証を使用する場合は、セッショントークンで永続的な IAM 資格情報または一時的なセキュリティ資格情報を使用できます。

資格情報プロファイルファイルのパスを指定しない場合は、デフォルトの資格情報ファイルのパスが使用されます。プロファイル名を指定しない場合、資格情報は資格情報ファイルのデフォルトプロファイルから使用されます。

資格情報プロファイルファイルについては、次のルールを考慮してください。

- 資格情報ファイルは、Secure Agent をインストールしたマシンと同じマシン上にある必要があります。
- 資格情報プロファイルファイル名は、`.credentials` で終わる必要があります。

- 資格情報プロファイルのパスを指定しない場合、Secure Agent はホームディレクトリの次のデフォルトの場所にある資格情報プロファイルファイルを使用します。
  `~/.aws/credentials`

  注: Windows では、環境変数%UserProfile%を使用してホームディレクトリを参照できます。Unix 系のシステムでは、環境変数$HOME を使用できます。

サンプルの資格情報プロファイルファイル:

```
[default]

aws_access_key_id = 1233333

aws_secret_access_key = abcabcabc


[test-profile]

aws_access_key_id = 1233333

aws_secret_access_key = abcabcabc

aws_session_token = jahaheieomdrtflmlioerp
```

aws_access_key_id と aws_secret_access_key により、ユーザーを認証するための認証情報の一部として使用される AWS アクセスキーと秘密鍵を指定します。

aws_session_token により、ユーザーを認証するための認証情報の一部として使用される AWS セッショントークンを指定します。セッショントークンは、一時的なセキュリティ資格情報を指定する場合にのみ必要です。

Amazon S3 とのプライベート通信

Amazon S3 とのプライベート通信は、AWS コンソールと Amazon S3 V2 接続で、ゲートウェイエンドポイントまたはインタフェースエンドポイントを設定することで有効にできます。

トラフィックをパブリックインターネットに公開せずに Amazon S3 とのプライベート通信を確立するように Amazon S3 V2 コネクタを設定できます。Amazon S3 にアクセスするには、Secure Agent が AWS Virtual Private Cloud（VPC）のサブネットの一部であることを確認します。AWS S3 VPC エンドポイントを使用すると、サブネットをインターネットゲートウェイに接続せずに、S3 要求を Amazon S3 サービスにルーティングできます。インタフェースエンドポイントまたはゲートウェイエンドポイントを作成できます。

詳細については、Configuring private communication with Amazon S3 using the Amazon S3 V2 Connector を参照してください。

第 2 章

Amazon S3 V2 接続

Amazon S3 V2 接続を使用すると、Amazon S3 とのデータの読み取りまたは書き込みを行うことができます。

Amazon S3 V2 接続を使用して、マッピングおよびマッピングタスクで、ソースおよびターゲットを指定します。

AWS Identity and Access Management（IAM）認証を使用すると、Amazon S3 リソースへのアクセスを安全に制御できます。Amazon S3 リソースへのアクセスを安全に制御するために、一時的なセキュリティ資格情報と統合ユーザーシングルサインオンも使用できます。

[接続] ページで Amazon S3 V2 接続を作成し、マッピングまたはマッピングタスクに関連付けます。Amazon S3 に対してデータの読み取りまたは書き込みを行うために、ソースおよびターゲットのプロパティを定義します。

Amazon S3 V2 接続プロパティ

Amazon S3 V2 接続をセットアップする際には、接続プロパティを設定します。

次の表に、Amazon S3 V2 接続プロパティを示します。

プロパティ	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 255 文字です。
説明	接続の説明。最大長は 4000 文字です。
タイプ	Amazon S3 V2 接続タイプ。
ランタイム環境	タスクを実行するランタイム環境の名前。 Secure Agent、Hosted Agent、またはサーバーレスランタイム環境を選択します。

プロパティ	説明
アクセスキー	Amazon S3 バケットにアクセスするためのアクセスキー。 次の認証方法に基づいてアクセスキー値を入力します。 - 基本認証。実際のアクセスキー値を入力します。 - IAM 認証。アクセスキー値は入力しないでください。 - ロールの引き受けを使用した一時的なセキュリティ資格情報。Amazon S3 バケットへのアクセス権限なしで、IAM ユーザーのシークレットアクセスキーを入力します。 - EC2 用のロールの引き受け。アクセスキー値は入力しないでください。 - 資格情報プロファイルファイルの認証 [1]。アクセスキー値は入力しないでください。 - 統合ユーザーシングルサインオン [1]。シークレットアクセスキー値は入力しないでください。
秘密鍵	Amazon S3 バケットにアクセスするためのシークレットアクセスキー。秘密鍵はアクセスキーに関連付けられており、アカウントを一意に識別します。 次の認証方法に基づいてシークレットアクセスキー値を入力します。 - 基本認証。実際のアクセスシークレット値を入力します。 - IAM 認証。アクセスシークレット値は入力しないでください。 - ロールの引き受けを使用した一時的なセキュリティ資格情報。Amazon S3 バケットへのアクセス権限なしで、IAM ユーザーのアクセスシークレットを入力します。 - EC2 用のロールの引き受け。アクセスキー値は入力しないでください。 - 資格情報プロファイルファイルの認証 [1]。アクセスシークレット値は入力しないでください。 - 統合ユーザーシングルサインオン [1]。アクセスシークレット値は入力しないでください。
IAM ロール ARN	動的に生成された一時的なセキュリティ資格情報を使用するためにユーザーに引き継がれた AWS Identity and Access Management（IAM）ロールの Amazon リソース名（ARN）。 一時的なセキュリティ資格情報を使用して AWS リソースにアクセスする場合はこのプロパティの値を入力します。 **注**: エージェントによる Amazon S3 バケットへのアクセスを有効にする IAM ロールを削除して接続を作成してもテスト接続は成功します。 IAM ロールの ARN の取得方法の詳細については、AWS のマニュアルを参照してください。
外部 ID	Amazon S3 バケットが別の AWS アカウントにある場合に、Amazon S3 バケットへのより安全なアクセスを提供します。
ロールの引き受けに EC2 ロールを使用	EC2 ロールが、［IAM ロール ARN］オプションで指定された別の IAM ロールを引き受けることができるようにします。 **注**: EC2 ロールには、同じアカウントまたは異なるアカウントから IAM ロールを引き受けるためのアクセス許可がアタッチされたポリシーが必要です。 デフォルトでは、［ロールの引き受けに EC2 ロールを使用］チェックボックスは選択されていません。
フォルダパス	Amazon S3 オブジェクトへのバケット名または完全なフォルダパス。 フォルダパスの末尾にスラッシュを使用しないでください。例: <バケット名>/<フォルダ名>
マスタ対称キー	クライアントサイド暗号化を使用する場合の、Base64 形式で示す 256 ビットの AES 暗号化キー。暗号化キーは、サードパーティ製ツールを使用して生成できます。

プロパティ	説明
顧客マスタキー ID	AWS Key Management Service（AWS KMS）によって生成された顧客マスタキー ID またはエイリアス名、またはアカウント間アクセス用のカスタムキーの Amazon リソース名（ARN）。 **注**: 詳細モードのマッピングでは、クロスアカウントアクセスは使用できません。 Amazon S3 バケットが存在するリージョンの顧客マスタキーを生成する必要があります。 次のマスタキーを指定できます。 - 顧客が生成した顧客マスタキー。クライアントサイドまたはサーバーサイドの暗号化を有効にします。 - デフォルトの顧客マスタキー。クライアントサイドまたはサーバーサイドの暗号化を有効にします。アカウントの管理者ユーザーのみがデフォルトの顧客マスタキー ID を使用してクライアントサイド暗号化を有効にできます。
S3 アカウントタイプ	Amazon S3 アカウントのタイプ。 次のオプションから選択します。 - Amazon S3 ストレージ。Amazon S3 サービスを使用できるようにします。 - S3 互換ストレージ。Scality RING や MinIO などのサードパーティのストレージプロバイダのエンドポイントを使用できるようにします。 デフォルトは Amazon S3 ストレージです。
REST エンドポイント	S3 互換ストレージに必要な S3 ストレージエンドポイント。 S3 ストレージエンドポイントを HTTP または HTTPS 形式で入力します。 例えば、http://s3.isv.scality.com と指定します。

プロパティ	説明
リージョン名	アクセス先のバケットの AWS リージョン。 次のいずれかのリージョンを選択します。 - アジアパシフィック（ムンバイ） - アジアパシフィック（ジャカルタ） - アジアパシフィック（大阪） - アジアパシフィック（ソウル） - アジアパシフィック（シンガポール） - アジアパシフィック（シドニー） - アジアパシフィック（東京） - アジアパシフィック（香港） - AWS GovCloud（米国） - AWS GovCloud（米国東部） - カナダ（中部） - 中国（北京） - 中国（寧夏） - 欧州（アイルランド） - 欧州（フランクフルト） - EU（ロンドン） - 欧州（ミラノ） - EU（パリ） - EU（ストックホルム） - 南米（サンパウロ） - 中東（バーレーン） - 米国東部（バージニア北部） - 米国東部（オハイオ） - 米国 ISO 東部 - 米国 ISOB 東部（オハイオ） - 米国 ISO 西部 - 米国西部（北カリフォルニア） - 米国西部（オレゴン） デフォルトは［米国東部（バージニア北部）］です。 **注**: 中東（バーレーン）およびアフリカ（ケープタウン）地域は、詳細モードでのマッピングには適用されません。
統合 SSO IdP[1]	AWS アカウントで使用する、統合ユーザーシングルサインオンの SAML 2.0 対応 ID プロバイダ。 Amazon S3 V2 コネクタは、ADFS 3.0 ID プロバイダのみをサポートします。統合ユーザーシングルサインオンを使用しない場合は、**［なし］**を選択します。 **注**: 統合ユーザーシングルサインオンは、詳細モードのマッピングには適用されません。
その他の認証タイプ [1]	次のいずれかの認証タイプを選択します。 - なし - 認証情報プロファイルファイルの認証 アクセスキーと秘密鍵を含む認証情報ファイルから Amazon S3 認証情報にアクセスするには、［資格情報プロファイルファイルの認証］オプションを選択します。 資格情報プロファイルファイルのパスとプロファイル名を入力して、Amazon S3 との接続を確立します。 資格情報プロファイルファイルの認証を設定する際に、永続的な IAM 資格情報または一時的なセッショントークンを使用できます。 デフォルトは［なし］です。

プロパティ	説明
資格情報プロファイルのファイルパス [1]	資格情報プロファイルファイルのパスを指定します。 資格情報プロファイルのパスを入力しない場合、Secure Agent はホームディレクトリの次のデフォルトの場所にある資格情報プロファイルファイルを使用します。 `~/.aws/credentials`
プロファイル名 [1]	資格情報の取得に使用される資格情報プロファイルファイル内のプロファイルの名前。 プロファイル名を入力しない場合、資格情報プロファイルファイルのデフォルトプロファイルの資格情報が使用されます。
S3 VPC エンドポイントタイプ [1]	Amazon S3 の VPC エンドポイントタイプ。 VPC エンドポイントを選択することで、Amazon S3 とのプライベート通信を有効にできます。 次の VPC エンドポイントタイプのいずれかを選択します。 - なし - ゲートウェイエンドポイント - インタフェースエンドポイント デフォルトは［なし］です。
Amazon S3 のエンドポイント DNS 名 [1]	Amazon S3 インタフェースエンドポイントの DNS 名。 DNS 名は以下の形式で入力します。 `bucket.<インタフェースエンドポイントの DNS 名>`
STS VPC エンドポイントタイプ [1]	S3 VPC インタフェースエンドポイントを選択する場合に適用されます。 AWS STS の VPC エンドポイントタイプ。 ［IAM **ロール** ARN］または［**フェデレーション** SSO IDp］を選択した場合は、STS VPC エンドポイントを設定します。
AWS STS サービスのエンドポイント DNS 名 [1]	AWS STS インタフェースエンドポイントの DNS 名。
KMS VPC エンドポイントタイプ [1]	インタフェースエンドポイントを選択する場合に適用されます。 AWS KMS の VPC エンドポイントタイプ。 ［**顧客マスタキー** ID］を選択した場合は、KMS VPC エンドポイントを設定します。
AWS KMS サービスのエンドポイント DNS 名 [1]	AWS KMS インタフェースエンドポイントの DNS 名。
[1] マッピングにのみ適用されます。	

統合ユーザーシングルサインオン接続のプロパティ

［統合 SSO IdP］で［ADFS 3.0］を選択した場合は、次のプロパティを設定します。

プロパティ	説明
統合ユーザー名	ID プロバイダ経由で AWS アカウントにアクセスする統合ユーザーのユーザー名。
統合ユーザーパスワード	ID プロバイダ経由で AWS アカウントにアクセスする統合ユーザーのパスワード。
IdP SSO URL	AWS に使用する ID プロバイダのシングルサインオン URL。
SAML ID プロバイダ ARN	ID プロバイダを信頼できるプロバイダとして登録するために AWS 管理者が作成した、SAML ID プロバイダの ARN。
ロール ARN	統合ユーザーに引き継がれた IAM ロールの ARN。

AWS リージョンのルールとガイドライン

接続プロパティでバケットのリージョン名を設定する場合は、次のルールとガイドラインを考慮してください。

- 既存の接続のランタイム環境を変更すると、リージョンはデフォルトのリージョン `US East (N. Virginia)`に変更されます。リージョンを手動で選択して、デフォルトのリージョンを変更します。
- Secure Agent マシンの次の場所にある最新の AWSSDK をコピーすることで、Amazon S3 バケット用のスペースを含むリージョンを使用できます。

  `<Secure agent installation directory>/downloads/<package.AmazonS3V2.zip>/package/s3/thirdparty/infa.amazon.s3`
- 既存の接続を編集すると、リージョンのエントリが重複して表示されます。これらのリージョンは AWSSDK から入力されるため、スペースを含むリージョンを使用します。例えば、`US West (Oregon)`ではなく `US West(Oregon)`を使用します。

S3 互換ストレージのルールおよびガイドライン

Amazon S3 V2 接続で S3 互換のストレージを設定する場合は、次のルールとガイドラインを考慮してください。

- S3 互換ストレージを使用する場合にのみ、基本認証を設定できます。
- Scality RING S3 互換ストレージに SSE-KMS 暗号化を設定することはできません。MinIO S3 互換ストレージに SSE および SSE-KMS 暗号化を設定することはできません。
- Amazon S3 ソースから Amazon Redshift にデータをロードするようにプッシュダウンの最適化を設定することはできません。

プロキシの設定

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。HTTP プロキシと SOCKS プロキシの両方を有効にすると、デフォルトでは SOCKS プロキシが使用されます。SOCKS プロキシの代わりに HTTP プロキシを使用する場合は、システムプロパティで［**DisableSocksProxy**］プロパティの値を true に設定します。

設計時および実行時にプロキシを有効にするには、proxy.ini ファイルおよび JVM オプションでプロキシの詳細を設定します。

プロキシ設定を構成するには、次の方法を使用します。

- **proxy.ini ファイル。**設計時にプロキシサーバーを使用するには、Secure Agent Manager を使用して、Windows 上の proxy.ini ファイルにプロキシ値を渡します。proxy.ini ファイルの値が更新されます。Linux では、proxy.ini ファイルに値を直接設定します。
- **JVM オプション。**実行時にプロキシサーバーを使用するには、Windows または Linux で JVM オプションを使用してプロキシサーバーの詳細を設定します。

プロキシサーバーを設定するときは、次のルールを考慮してください。

- 認証されていないプロキシサーバーのみを使用して Informatica Intelligent Cloud Services に接続できます。
- サーバーレスランタイム環境を使用する場合、プロキシサーバーを使用して Informatica Intelligent Cloud Services に接続することはできません。
- プロキシ設定は、詳細モードのマッピングには適用されません。

JVMOption を使用したプロキシ設定

Windows または Linux マシンの Secure Agent の JVMOptions を使用して、プロキシサーバー設定を構成できます。

1. Informatica Intelligent Cloud Services にログインします。
2. ［管理］を開いて**［ランタイム環境］**を選択します。
3. プロキシサーバーを設定する Secure Agent を選択します。
4. ページの右上隅にある**［編集］**をクリックします。
5. **［システム構成の詳細］**セクションで、データ統合サービスの**［タイプ］**に**［DTM］**を選択します。
   - **JVMOption** フィールドに次のパラメータを追加し、各パラメータに適した値を指定します。

パラメータ	説明
-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。

   以下に例を示します。

   ```
   JVMOption1=-Dhttps.proxyHost=<proxy_server_hostname>
   JVMOption2=-Dhttps.proxyPort=<proxy_port>
   ```

6. **［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。

Windows でのプロキシ設定

Windows マシンで Secure Agent のプロキシサーバーの設定を行うには、Secure Agent を介してプロキシサーバー設定を構成します。

1. **［開始］** > **［すべてのプログラム］** > **［Informatica Cloud Secure Agent］** > **［Informatica Cloud Secure Agent］**をクリックして、Secure Agent Manager を起動します。

   Secure Agent Manager に Secure Agent のステータスが表示されます。

2. ［Secure Agent Manager］ページで**［プロキシ］**をクリックします。
3. **［プロキシサーバーを使用］**をクリックして、プロキシサーバーの設定を入力します。
4. 次のプロキシサーバーの詳細を設定します。

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。

5. **［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。

Linux でのプロキシ設定

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。Secure Agent に定義されているプロキシサーバーの設定は、コマンドラインから更新できます。

Linux マシンで Secure Agent のプロキシサーバーを設定するには、`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て、プロキシの設定項目を決めてください。

1. 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`
2. 認証されていないプロキシの詳細を proxy.ini ファイルで直接更新するか、次のコマンドを実行して proxy.ini ファイルのプロキシの詳細を更新します。

   `./consoleAgentManager.sh configureProxy <プロキシホスト> <プロキシポート>`
3. Secure Agent を再起動します。

プロキシ設定のバイパス

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、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。

ただし、特定の IP アドレスとホスト名をプロキシから除外する場合は、プロキシをバイパスできます。`proxy.ini` ファイルで *InfaAgent.NonProxyHost* プロパティを設定し、Secure Agent プロパティの JVM オプションで *-Dhttp.nonProxyHosts* プロパティを設定して、除外する IP アドレスとホスト名を含めます。

次の表は、proxy.ini ファイルと JVM オプションを使用してプロキシを設定するためのプロキシフラグの設定を示しています。

プロキシ設定	プロキシフラグの設定
Proxy.ini	InfaAgent.NonProxyHost=localhost| <your_bucket_name>.s3.|127.*|[\:\:1] 例えば、単一の S3 バケット iam.qa.bucket をバイパスするには、次のプロキシフラグ設定を使用します。 InfaAgent.NonProxyHost=localhost|**iam.qa.bucket.s3.**|127.*|[\:\:1] すべての S3 バケットをバイパスするには、次のプロキシフラグ設定を使用します。 InfaAgent.NonProxyHost=localhost|***.s3.***|127.*|[\:\:1]
JVM オプション	-Dhttp.nonProxyHosts=localhost| <your_bucket_name>.s3.|127.* |[\:\:1] 例えば、単一の S3 バケット iam.qa.bucket をバイパスするには、次のプロキシフラグ設定を使用します。 -Dhttp.nonProxyHosts=localhost|**iam.qa.bucket.s3.**|127.*|[\:\:1] すべての S3 バケットをバイパスするには、次のプロキシフラグ設定を使用します。 -Dhttp.nonProxyHosts=localhost|***.s3.***|127.*|[\:\:1]

第 3 章

Amazon S3 V2 ソースとターゲット

Amazon S3 V2 のソースとターゲットを設定して、Amazon S3 との間で読み取りと書き込みを行うことができます。

Amazon S3 V2 ソース

マッピングまたはマッピングタスクのソースとして Amazon S3 V2 オブジェクトを使用できます。

詳細ソースプロパティを設定するとき、Amazon S3 V2 固有のプロパティを設定します。Amazon S3 からデータを読み取る場合、Amazon S3 V2 ファイルを複数のパーツに分けてダウンロードし、ステージングディレクトリの場所を指定して、データを解凍できます。

次の表に、さまざまなファイルタイプでサポートされる暗号化タイプを示します。

暗号化タイプ	Avro **ファイル**	**バイナリファイル** [1]	**フラット**	JSON **ファイル** [2]	ORC **ファイル**	Parquet **ファイル**
クライアントサイド暗号化	いいえ	はい	○	×	×	いいえ
サーバーサイド暗号化	○	○	○	○	○	はい
KMS を使用したサーバーサイド暗号化	○	○	○	○	○	はい
Informatica Encryption	いいえ	はい	○	×	×	いいえ

[1] 詳細モードのマッピングには適用されません。
[2] 詳細モードのマッピングに適用されます。

Amazon S3 V2 ソースでのデータ暗号化

Amazon S3 からバイナリファイルソースおよびフラットファイルソースを読み取る場合、データを暗号化できます。

Amazon S3 V2 ソースのクライアントサイド暗号化

クライアントサイド暗号化は、データを Amazon S3 サーバーに送信する前にデータを暗号化する方法です。

Amazon S3 バケットの、クライアントサイド暗号化が行われたファイルを読み取ることができます。クライアントサイド暗号化が行われたファイルを読み取るには、接続プロパティでマスタ対称キーまたは顧客マスタキーを指定する必要があります。Secure Agent は、マスタ対称キーまたは顧客マスタキーを使用してデータを復号化します。

サードパーティのツールを使用してクライアントサイド暗号化が行われたファイルを生成すると、暗号化されたファイルのメタデータが生成されます。Amazon S3 から暗号化されたファイルを読み取るには、暗号化されたファイルと暗号化されたファイルのメタデータを AmazonS3 バケットにアップロードする必要があります。

暗号化されたファイルをアップロードする場合は、メタデータに次のキーが必要です。

- Content-Type
- x-amz-meta-x-amz-key
- x-amz-meta-x-amz-unencrypted-content-length
- x-amz-meta-x-amz-matdesc
- x-amz-meta-x-amz-iv

クライアントサイド暗号化が行われたファイルの読み取り

クライアントサイド暗号化が行われたファイルを読み取るには、次のタスクを実行します。

1. Amazon S3 V2 接続を作成するときに、マスタ対称キーを指定します。
   必ず、Base64 形式の 256 ビット AES 暗号化キーを指定してください。
2. 次のディレクトリから `local_policy.jar` ファイルと `US_export_policy.jar` ファイルをコピーします。
   `<Secure Agent installation directory>/jdk/jre/lib/security/policy/unlimited/`
3. ファイルを次のディレクトリに貼り付けます。
   `<Secure Agent installation directory>/jdk/jre/lib/security/`
4. ソーストランスフォーメーションの詳細プロパティでクライアントサイドの暗号化を有効にします。
5. Secure Agent を再起動します。

Amazon S3 V2 ソースのサーバーサイド暗号化

サーバーサイド暗号化は、Amazon S3 が管理する暗号化キーを使用してデータを暗号化する方法です。KMS を使用したサーバーサイド暗号化は、AWS KMS が管理する顧客マスタキーを使用してデータを暗号化する方法です。

サーバーサイド暗号化

サーバーサイド暗号化ファイルを読み取るには、Amazon S3 V2 ソースで暗号化されたファイルを選択します。

KMS **を使用したサーバーサイド暗号化**

KMS でサーバーサイド暗号化ファイルを読み取るには、AWS KMS が管理する顧客マスタキーを［**顧客マスタキー ID**］接続プロパティで指定し、Amazon S3 V2 ソースで暗号化されたファイルを選択します。

注: 詳細ソースプロパティで暗号化タイプを指定する必要はありません。

Amazon S3 V2 ソースの Informatica Encryption

Informatica 暗号ライブラリを使用して暗号化されたバイナリソースファイルまたはフラットソースファイルをローカルマシンまたはステージングロケーションにダウンロードし、ソースファイルを復号化できます。

Informatica Encryption は、Secure Agent マシンでマッピングを実行する場合にのみ適用されます。Informatica 暗号ライブラリを使用して暗号化されたソースファイルを読み取るには、次のタスクを実行します。

1. Amazon S3 V2 接続を作成するときに、組織の管理者が Informatica 暗号ライブラリのライセンスに対する権限を持っていることを確認します。
2. 詳細ソースプロパティで、暗号化タイプに［**Informatica Encryption**］を選択します。

Informatica で暗号化されたソースファイルを読み取り、暗号化タイプに［**Informatica Encryption**］を選択すると、データプレビューが失敗します。

データをプレビューできるようにするには、Informatica で暗号化された読み取りたいソースファイルにあるメタデータと同じメタデータを含むダミーソースファイルを選択します。Informatica で暗号化されたソースファイルのファイル名を［**ファイル名**］詳細ソースプロパティに入力し、ダミーソースファイルのファイル名を上書きします。次に、詳細ソースプロパティで、暗号化タイプに［**Informatica Encryption**］を選択します。

注: マッピングで IInformatica Encryption を使用した場合、1000 個を超えるファイルを復号することはできません。

Amazon S3 V2 ソースのソースタイプ

データの読み取り元のソースのタイプを選択できます。

Amazon S3 V2 詳細ソースプロパティの［**ソースタイプ**］オプションから次のソースタイプを選択できます。

ファイル

Amazon S3 ファイルを含むバケット名を入力する必要があります。該当する場合は、<bucket_name>/<folder_name>形式にターゲットファイルが含まれるフォルダ名を追加します。

Amazon S3 V2 コネクタには、実行時に［**フォルダパス**］と［**ファイル名**］プロパティの値を上書きできるオプションがあります。

バケット名を指定せずに、/<folder_name>形式でスラッシュ（/）から始まるフォルダパスを指定した場合、このフォルダパスは接続プロパティで指定したフォルダパスに付加されます。

例えば、このプロパティでフォルダパスを/<dir2>と指定し、接続プロパティでフォルダパスを<my_bucket1>/<dir1>と指定すると、このフォルダパスは、<my_bucket1>/<dir1>/<dir2>形式で接続プロパティで指定したフォルダパスに付加されます。

接続プロパティでフォルダパスを<my_bucket1>/<dir1>と指定し、このプロパティでフォルダパスを<my_bucket2>/<dir2>と指定すると、Secure Agent はこのプロパティで指定したフォルダパス<my_bucket2>/<dir2>にファイルを書き込みます。

ディレクトリ

マッピングを作成して、実行時にソースタイプを［**ディレクトリ**］として選択する場合は、ソースファイルを選択する必要があります。［**ソースタイプ**］オプションを［**ディレクトリ**］として選択すると、ワイルドカード文字を使用してフォルダパスまたはファイル名を指定する場合、またはディレクトリからファイルを再帰的に読み取る場合にのみ［**ファイル名**］の値が優先されます。

読み取り操作では、実行時に［**フォルダパス**］の値を指定すると、Secure Agent は詳細ソースプロパティから［**フォルダパス**］の値を使用します。実行時に［**フォルダパス**］の値を指定しないと、Secure Agent は接続作成中に指定した［**フォルダパス**］の値を使用します。

ソースタイプとして［**ディレクトリ**］を選択するには、次のルールとガイドラインを使用します。

- ディレクトリ内のすべてのソースファイルに同じメタデータが含まれている必要があります。
- すべてのファイルに同じ形式のデータが含まれている必要があります。例えば、区切り記号、ヘッダーフィールド、およびエスケープ文字は同じである必要があります。
- 指定されたディレクトリ内のすべてのファイルが解析されます。サブディレクトリ下のファイルは、ディレクトリからファイルを再帰的に読み取る場合にのみ解析されます。

複数のファイルからの読み込み

Amazon S3 からフラット形式タイプの複数のファイルを読み取り、マッピングのターゲットにデータを書き込むことができます。

次のタイプのマニフェストファイルを使用できます。

- カスタムマニフェストファイル
- Amazon Redshift マニフェストファイル

カスタムマニフェストファイル

Amazon S3 からフラットフォーマットタイプの複数のファイルを読み取り、ターゲットにデータを書き込むことができます。複数のフラットファイルを読み取るには、すべてのファイルが同じ Amazon S3 バケットに存在している必要があります。

Amazon S3 バケットの複数のソースを読み取る場合は、すべてのソースファイルを含んだ、それぞれの絶対パスまたはディレクトリパスを持つ.manifest ファイルを作成する必要があります。.manifest ファイル名は、<file_name>.manifest という形式で指定する必要があります。

例えば、.manifest ファイルには次の形式でソースファイルが含まれます。

```
{
    "fileLocations":
    [
        {
            "URIs":
            [
                "dir1/dir2/dir3/file_1.csv",
                "dir1/dir2/dir3/file_2.csv",
                "dir1/file_3.csv"
            ]
        },
        {
            "URIPrefixes":
            [
                "dir1/dir2/dir3/",
                "dir1/dir2/dir4/"
            ]
        },
        {
            "WildcardURIs":
            [
                "dir1/dir2/dir3/*.csv"
            ]
        }
    ],
    "settings":
    {
        "stopOnFail": "true"
    }
}
```

カスタムマニフェストファイルのには、次のタグが含まれています。

- URI。バケット名に関連するファイルのパスを指定します。
- URIPrefix。バケット名に関連するディレクトリのパスを指定します。
- WildcardURI。フラット形式タイプのファイル名にアスタリスク（*）ワイルドカードを指定して、Amazon S3 バケットからファイルを取得します。アスタリスク（*）ワイルドカードを指定すると、すべてのファイルまたは名前のパターンに一致するファイルのみを取得します。

.manifest ファイルの URIs、URIPrefixes、WildcardURIs、または fileLocations 内のすべてのセクションを指定できます。

フォルダ名の指定には、ワイルドカード文字を使用できません。例: { "WildcardURIs": ["multiread_wildcard/dir1*/", "multiread_wildcard/*/"] }。

[データプレビュー] タブには、.manifest ファイルで指定された URI に存在する最初のファイルのデータが表示されます。URI セクションが空の場合、URIPrefixes で指定されたフォルダの最初のファイルが表示されます。

Amazon Redshift マニフェストファイル

UNLOAD コマンドで作成された Amazon Redshift マニフェストファイルを使用して、Amazon S3 から複数のフラットファイルを読み取ることができます。すべてのフラットファイルは同じメタデータを持ち、同じ Amazon S3 バケットで利用可能である必要があります。

.manifest ファイルを作成して、ファイルのバケット名と完全なオブジェクトパスを含んだ URL を使用してすべてのソースファイルを一覧表示します。.manifest ファイル名は、<file_name>.manifest という形式で指定する必要があります。

例えば、Amazon Redshift マニフェストファイルには次の形式でソースファイルが含まれます。

```
{
    "entries": [
            {"url": "s3://mybucket-alpha/2013-10-04-custdata", "mandatory":true},
            {"url": "s3://mybucket-alpha/2013-10-05-custdata", "mandatory":true},
            {"url": "s3://mybucket-beta/2013-10-04-custdata", "mandatory":true},
            {"url": "s3://mybucket-beta/2013-10-05-custdata", "mandatory":true},
    ]
}
```

Redshift マニフェストファイルの形式には、次のタグが含まれています。

url

url タグは、次の形式のソースファイルで構成されています。

"url": "<エンドポイント名>://<フォルダパス>/<ファイル名>", "mandatory":<値>

mandatory

Amazon S3 V2 コネクタは、mandatory タグを使用して、.manifest ファイル内のファイルの読み取りを続行するかどうかを次のシナリオに基づいて決定します。

- mandatory タグの値が true で、S3 バケットに指定されたソースファイルがない場合、Amazon S3 V2 コネクタは.manifest ファイル内の残りのファイルも読み取りません。マッピングタスクは失敗します。
- mandatory タグの値が false で、S3 バケットに指定されたファイルがない場合、Amazon S3 V2 コネクタは.manifest ファイル内の残りのファイルの読み取りを順番に続行します。
- .manifest ファイルにファイルが含まれていない場合、マッピングタスクは失敗します。

デフォルトでは、mandatory タグの値は false です。

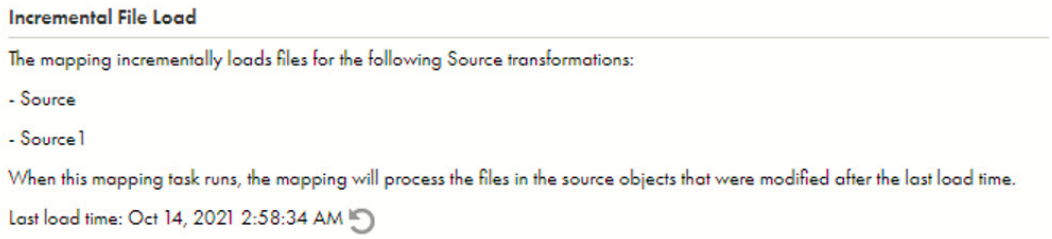
ファイルの増分ロード

ディレクトリにソースファイルを増分ロードして、マッピングタスクが最後に実行されてから変更されたファイルのみを読み取って処理することができます。

ソースファイルを増分ロードするには、Amazon S3 V2 データオブジェクトの詳細読み取りプロパティの［**増分ファイルロード**］オプションを選択します。ファイルを増分ロードできるのは詳細モードのマッピングの場合のみです。すべてのマッピングソースは、同じクラウド環境にある必要があります。

Amazon S3 からファイルを増分ロードする場合、ジョブは、最終ロード時刻からジョブの実行を開始する 15 分前までに変更されたファイルをロードします。例えば、午後 2 時にジョブを実行すると、ジョブは午後 1 時 45 分より前に変更されたファイルをロードします。Amazon S3 上でオブジェクトのアップロードが完了するまでに数分かかることがあるため、この 15 分のバッファにより、ジョブが完全なファイルのみをロードすることが保証されます。

マッピングタスクを設定すると、［**増分ファイルロード**］セクションには、ファイルを増分ロードするソーストランスフォーメーションと、最後のジョブがファイルのロードを完了した時刻が一覧表示されます。デフォルトでは、実行される次のジョブは、最終ロード時刻の後に変更されたファイルを確認します。次のジョブですべてのソースファイルをロードするには、最終ロード時刻をリセットします。



詳細モードのマッピングを実行して、Parquet や Avro などの複合ファイル形式を含むディレクトリを増分ロードする場合、前回の実行以降にソースに新しいファイルまたは変更されたファイルがないと、マッピングは失敗します。

詳細モードのマッピングでソースファイルを増分ロードした後に、ジョブを実行して、特定の時間間隔で変更されたファイルを再処理できます。ファイルを再処理するジョブを作成する場合、変更されたファイルを確認するための時間間隔を選択します。

増分ファイルロードの詳細については、データ統合のドキュメントの「*タスク*」を参照してください。

ワイルドカード文字

詳細モードのマッピングを実行して、Avro ファイル、フラットファイル、JSON ファイル、ORC ファイル、または Parquet ファイルからデータを読み取る場合は、? および*というワイルドカード文字を使用してフォルダパスまたはファイル名を指定できます。

フォルダパスまたはファイル名にワイルドカード文字を使用するには、Amazon S3 V2 データオブジェクトの詳細読み取りプロパティで［**ワイルドカード文字を許可**］オプションを選択します。

? **（疑問符）**

疑問符（?）の部分に文字を 1 つ含む文字列を検索します。例えば、ソースファイル名に `a?b.txt` と入力すると、Secure Agent は次のような名前のファイルからデータを読み取ります。

- `a1b.txt`
- `a2b.txt`
- `aab.txt`

***（アスタリスク）**

アスタリスクマーク（*）の部分に文字のない文字列、または文字を 1 つ以上含む文字列を検索します。例えば、ソースファイル名に a*b.txt と入力すると、Secure Agent は次のような名前のファイルからデータを読み取ります。

- aab.txt
- a1b.txt
- ab.txt
- abc11b.txt

アスタリスク（*）ワイルドカードを使用すると、すべてのファイルまたは名前のパターンに一致するファイルのみを取得できます。次の形式でワイルドカード文字を指定します。

- abc*.txt
- abc.*

abc*.txt を指定すると、Secure Agent は、abc という語から始まり、.txt というファイル拡張子で終わるすべてのファイル名を読み取ります。abc.*を指定すると、Secure Agent は、拡張子に関係なく、abc という語から始まるすべてのファイル名を読み取ります。

ワイルドカード文字のルールとガイドライン

ワイルドカード文字を使用してフォルダパスまたはファイル名を指定する場合は、次のルールとガイドラインを考慮してください。

- バケット名にワイルドカード文字を指定することはできません。
- フォルダパスにワイルドカード文字を指定し、Amazon S3 バケットに名前のパターンに一致するフォルダが含まれていない場合、マッピングは失敗します。
- ファイル名にワイルドカード文字を指定し、Amazon S3 バケットに名前のパターンに一致するファイルが含まれていない場合、マッピングは失敗します。
- 詳細モードのマッピングのフォルダパスでワイルドカード文字を使用すると、Secure Agent は名前のパターンに一致するフォルダとファイルからデータを読み取ります。

ディレクトリからのファイルの再帰読み取り

詳細モードの Amazon S3 V2 マッピングのサブディレクトリに保存されているオブジェクトを読み取ることができます。フラットファイル、Avro ファイル、JSON ファイル、ORC ファイル、および Parquet ファイルに対しては、再帰読み取りを使用できます。再帰読み取りを使用して読み取るファイルは、同じメタデータを持っている必要があります。

再帰読み取りを有効にするには、詳細ソースプロパティでソースタイプを［**ディレクトリ**］として選択します。サブディレクトリに格納されているオブジェクトを読み取るには、［**再帰的なディレクトリの読み取り**］詳細ソースプロパティを有効にします。

また、フォルダパスまたはファイル名にワイルドカード文字を指定して、再帰読み取りを使用することもできます。例えば、ワイルドカード文字を使用すると、次のような方法でファイルを再帰的に読み取ることができます。

- フォルダパスを**/abc*/**とした場合。フォルダ名の先頭にパターン abc があるフォルダまたはサブフォルダ内のすべてのファイルを返します。
- フォルダパスを**/abc*/**として、ファイル名を **myfile***とした場合。フォルダまたはサブフォルダ内のファイル名の先頭にパターン myfile があり、フォルダ名の先頭にパターン abc があるすべてのファイルを返します。

ソースパーティション

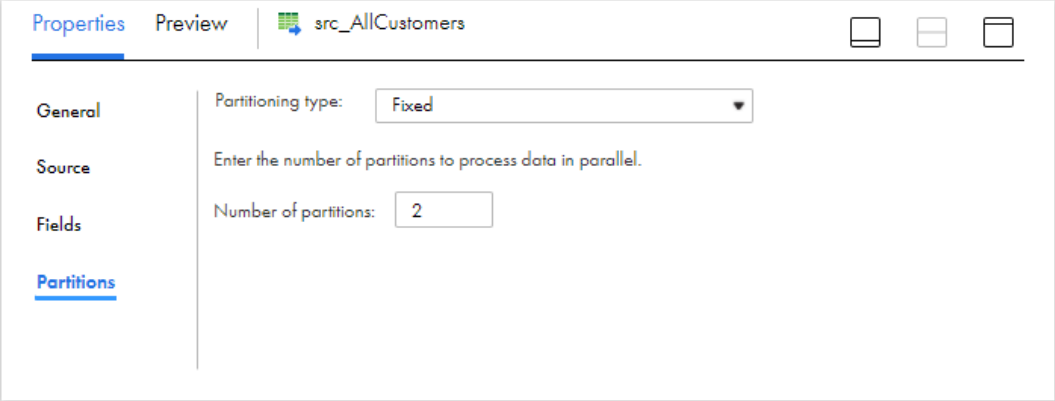
フラットファイル、Avro ファイル、ORC ファイル、または Parquet ファイルからデータを読み取る場合に、実行時にマッピングのパフォーマンスを最適化するように固定パーティションを設定できます。固定パーティションは、マッピングでのみ設定できます。

パーティションタイプによって、パーティションポイントでパーティションにデータを配布する方法を制御します。パーティション化が設定されていると、Secure Agent は、パーティションとして定義したスレッドの数に基づいてソースデータの行を配布します。

Mapping Designer でソーストランスフォーメーションを設定する際に、パーティション化を有効にします。

ソーストランスフォーメーションの［**パーティション**］タブで、固定パーティションを選択し、読み取るデータの容量に基づいてパーティションの数を入力します。デフォルトでは、［**パーティションの数**］フィールドの値は 1 です。

次の図に、設定されたパーティショニングを示します。



Secure Agent は、Amazon S3 V2 ソースファイルのサイズに応じてパーティションを有効にします。ファイル名には、`<file name>_<number>`形式で、0 から始まる数字が付加されます。

パーティション化を有効にした場合に、ソースカラムの精度がそのカラムの最大データ長より小さいと、予期しない結果が発生することがあります。予期しない結果が発生しないようにするには、パーティション化が期待通りに機能するようにするために、ソースカラムの精度を、そのカラムの最大データ長と同じかそれより大きくする必要があります。

注: マニフェストファイル、圧縮された.gz ファイル、または読み取りディレクトリファイルから読み取るようにマッピングで Amazon S3 V2 ソースのパーティションを設定すると、Secure Agent はパーティションを無視します。ただし、タスクは正常に実行されます。

ソースオブジェクトパスの読み取り

ソースオブジェクトをインポートするときに、Secure Agent はインポートされたソースオブジェクトにファイル名フィールドを追加します。ファイル名フィールドには、Secure Agent がランタイムにデータを読み取るソースファイルの絶対パスが格納されます。

例えば、読み取り対象の複数のレコードが格納された多数のファイルがあるディレクトリになるとします。Amazon S3 V2 ソースの詳細プロパティで、ソースタイプとしてこのディレクトリを選択します。マッピングを実行するときに、Secure Agent は各レコードを読み取り、対応するソースファイルの絶対パスをファイル名フィールドに格納します。

ファイル名フィールドは、次のファイル形式に適用されます。

- Avro

- バイナリ。マッピングのみに適用されます。
- ORC
- Parquet

注: ソースデータのカラム名に FileName は使用しないでください。FileName は予約済みのキーワードです。この名前は、大文字と小文字が区別されます。

ソースオブジェクトで FileName フィールドを使用すると、Secure Agent はマッピングと詳細モードのマッピングではそれぞれ異なる方法でファイル名とディレクトリ名を読み取ります。

特徴	マッピング	詳細モードのマッピング
ファイル名	xyz.amazonaws.com/aa.bb.bucket/1024/characterscheckfor1024	s3a://<bucket_name>/customer.avro
ディレクトリ名	<ファイル名を含むファイルの絶対パス>	s3a://<bucket_name>/avro/<directory_name>/<file_name>

注: ソースオブジェクトの［FileName］フィールドは、デフォルトで-を使用した形式を使用します。例: s3-us-west-2.amazonaws.com/<bucket_name>/automation/customer.avro

を使用するように［FileName］フィールドの形式を変更します。、JVM オプション changeS3EndpointForFileNamePort = true を設定します。例: s3.us-west-2.amazonaws.com/<bucket_name>/automation/customer.avro

プッシュダウンの最適化

データを Amazon S3 ソースから Amazon Redshift のデータウェアハウスにロードする場合に完全なプッシュダウン最適化を有効にすることができます。Amazon Redshift にデータをロードするときに、データウェアハウスモデルおよび要件ごとにデータを変換できます。マッピングタスクで完全プッシュダウンを有効にすると、マッピングロジックが AWS 環境にプッシュされ、AWS コマンドが利用されます。詳細モードで設定されたマッピングに基づいて、タスクにプッシュダウンの最適化を設定することはできません。

プッシュダウンの最適化の詳細については、Amazon Redshift V2 コネクタのヘルプを参照してください。サポートされている他のクラウドデータウェアハウスにデータをロードする必要がある場合は、該当するクラウドデータウェアハウスのコネクタのヘルプを参照してください。

Amazon S3 V2 ターゲット

マッピングまたはマッピングタスクのターゲットとして Amazon S3 V2 オブジェクトを使用できます。

Amazon S3 V2 ターゲットの名前と説明を指定します。ターゲットオブジェクトの Amazon S3 V2 ターゲットと詳細プロパティを設定します。

Amazon S3 V2 ターゲットでのデータ暗号化

データを保護するために、ファイルをターゲットに書き込むときに Amazon S3 ファイルを暗号化できます。マスタ対称キーと顧客マスタキーを同時に使用しないでください。

暗号化のタイプは、Amazon S3 V2 詳細ターゲットプロパティにある［**暗号化タイプ**］フィールドで選択します。

以下のタイプの暗号化を選択できます。

なし

データは暗号化されません。

サーバーサイド暗号化

ターゲットに書き込むときに、Amazon S3 が管理する暗号化キーを使用して Amazon S3 でデータを暗号化する場合は、暗号化タイプとして［**サーバーサイド暗号化**］を選択します。

接続プロパティで顧客マスタキー ID を指定しない場合は、暗号化タイプとして［**サーバーサイド暗号化**］を選択する必要があります。

KMS **を使用したサーバーサイド暗号化**

ターゲットに書き込むときに、AWS KMS が管理する顧客マスタキー暗号化キーを使用して Amazon S3 でデータを暗号化する場合は、暗号化タイプとして［**KMS を使用したサーバーサイド暗号化**］を選択します。

接続プロパティで指定した AWS KMS が管理する顧客マスタキーは、Amazon S3 をホストする地域と同じ地域に属する必要があります。

例えば、Amazon S3 が［**米国西部（オレゴン）**］リージョンでホストされている場合、同じリージョンで有効にされた AWS KMS が管理する顧客マスタキーを使用する必要があります。

クライアントサイド暗号化

ターゲットに書き込むときに、Secure Agent でデータを暗号化する場合は、暗号化タイプとして［**クライアントサイド暗号化**］を選択します。クライアントサイド暗号化では、Base64 形式の 256 ビット AES 暗号化キーまたは顧客マスタキーであるマスタ対称キーを使用します。

Informatica Encryption

ターゲットに書き込むときに、Informatica 暗号ライブラリを使用してデータを暗号化する場合は、暗号化タイプとして［**Informatica Encryption**］を選択します。Informatica Encryption は、Secure Agent マシンでマッピングを実行する場合にのみ適用されます。

Informatica Encryption 方式を使用してファイルを暗号化するには、次のタスクを実行します。

1. Amazon S3 V2 接続を作成するときに、組織の管理者が Informatica 暗号ライブラリに対する権限を持っていることを確認します。
2. 詳細ターゲットプロパティで、暗号化タイプに［**Informatica Encryption**］を選択します。

次の表に、さまざまなファイルタイプでサポートされる暗号化タイプを示します。

暗号化タイプ	Avro **ファイル**	**バイナリファイル** [1]	**フラット**	JSON **ファイル** [2]	ORC **ファイル**	Parquet **ファイル**
クライアントサイド暗号化	いいえ	はい	○	×	×	いいえ
サーバーサイド暗号化	○	○	○	○	○	はい
KMS を使用したサーバーサイド暗号化	○	○	○	○	○	はい

暗号化タイプ	Avro ファイル	バイナリファイル [1]	フラット	JSON ファイル [2]	ORC ファイル	Parquet ファイル
Informatica Encryption	いいえ	はい	○	×	×	いいえ

[1] 詳細モードのマッピングには適用されません。
[2] 詳細モードのマッピングにのみ適用されます。

Amazon S3 V2 ターゲットでのデータ暗号化のルールとガイドライン

Amazon S3 V2 ターゲットでデータ暗号化を設定する場合は、次のルールとガイドラインを考慮してください。

- マッピングで Informatica Encryption を使用した場合、詳細モードのマッピングのターゲットディレクトリに_SUCCESS ファイルは生成されません。
- マッピングで Informatica Encryption を使用した場合、1000 個を超えるファイルを暗号化することはできません。

Amazon S3 クライアント暗号化ポリシーの詳細については、*Amazon S3 ドキュメント*を参照してください。

既存のファイルの上書き

既存のターゲットファイルを上書きできます。

Amazon S3 V2 ターゲット詳細プロパティで［**存在する場合はファイルを上書き**］オプションを選択し、既存のファイルを上書きします。デフォルトでは、［**存在する場合はファイルを上書き**］チェックボックスの値は［true］です。

［**存在する場合はファイルを上書き**］オプションを選択した場合、Secure Agent は上書きするファイルと同じファイル名の既存のファイルを削除し、ターゲットディレクトリ内に同じファイル名の新しいファイルを作成します。

Secure Agent は、設計時に作成されたファイル名と同じプレフィックスを持つすべてのファイルとフォルダも削除します。これは、Avro ファイル、ORC ファイル、および Parquet ファイルに適用されます。

［**存在する場合はファイルを上書き**］オプションを選択しない場合、Secure Agent はターゲットディレクトリ内の既存のファイルを削除しません。Secure Agent は、`YYYYMMDD_HHMMSS_millisecond` 形式で各ターゲットファイル名の末尾にタイムスタンプを追加します。例えば、Secure Agent は、`output.txt-20171220_091900_69844051` 形式でターゲットファイル名の名前を変更します。

ターゲットのパーティション化

フラット形式タイプのファイルにデータを書き込む場合、実行時のマッピングパフォーマンスを最適化するために、パーティション化を設定できます。ターゲットのパーティション化は、マッピングでのみ設定できます。

パーティションタイプによって、パーティションポイントでパーティションにデータを配布する方法を制御します。パーティションタイプをパススルーパーティションとして定義できます。パーティション化が設定されていると、Secure Agent は、パーティションとして定義したスレッドの数に基づいてターゲットデータの行を配布します。

詳細ターゲットプロパティの［**パーティションファイルのマージ**］オプションを設定できます。データを Amazon S3 V2 ターゲットに書き込むとき、Secure Agent で複数のパーティションファイルを 1 つのファイルにマージするか、指定されたパーティションの数に基づいて個々のファイルを維持するかを指定できます。

[パーティションファイルのマージ] オプションを選択しない場合、指定されたパーティション数に基づいて個々のファイルが作成されます。ファイル名には、<file name>_<number>形式で、0 から始まる数字が付加されます。

例えば、Region.csv ファイルのスレッド数は 3 です。**[パーティションファイルのマージ]** オプションを選択しない場合、Secure Agent は、3 つのファイルを次の形式で Amazon S3 V2 ターゲットに書き込みます。

```
<Region_0>
<Region_1>
<Region_2>
```

[パーティションファイルのマージ] オプションを設定した場合、Secure Agent はパーティション化されたすべてのファイルを 1 つのファイルにマージし、そのファイルを Amazon S3 V2 ターゲットに書き込みます。

ディレクトリレベルのパーティショニング

詳細モードのマッピングを使用すると、パーティションカラムの読み取りと書き込みができます。

テーブルまたはデータセットをパーティションに編成して、カラムまたはパーティションキーに基づいて同じタイプのデータをグループ化できます。テーブルまたはデータセット内の 1 つ以上のパーティションカラムを選択できます。

パーティションカラムから読み取るには、パーティションディレクトリを選択し、パーティションカラムを特定します。パーティションカラムに書き込むには、フィールドのリストからパーティションカラムを追加して、必要に応じてパーティションの順序を変更します。

次のファイル形式で、パーティションカラムに対してデータを読み書きすることができます。

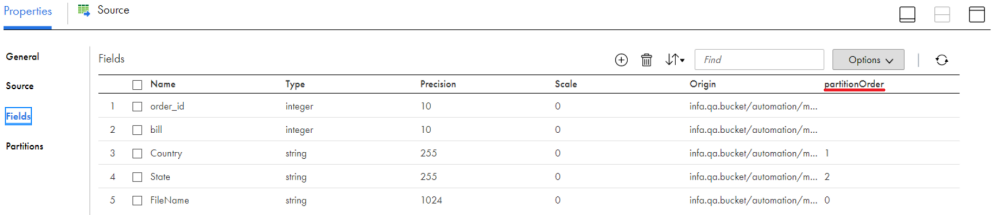
- Avro
- Parquet
- ORC
- JSON

パーティションカラムからの読み取り

パーティションカラムからデータを読み取るには、次の手順を実行します。

1. ソースオブジェクトのリストからディレクトリを選択します。
2. 詳細ソースプロパティで **[ディレクトリ]** としてソースタイプを選択します。

3. ［フィールド］タブでは、パーティションの数を表示できます。次の図に示すように、パーティション化されたフィールドのリストに［**partitionOrder**］カラムが表示されます。



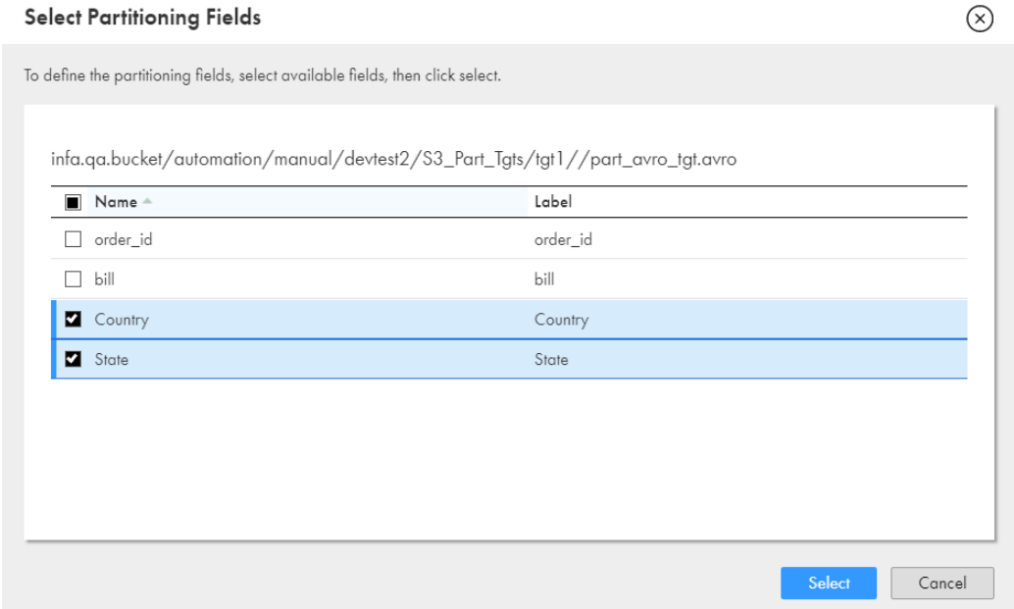
［**partitionOrder**］カラムは、カラムがパーティション化されているかどうかを示します。
上の画像では、2 つのパーティションカラムが存在しています。パーティション順序の値 1 と 2 は、パーティション化のために［国］フィールドと［州］フィールドが選択された順序を示しています。
［FileName］フィールドのパーティション順序は 0 です。

パーティションカラムへの書き込み

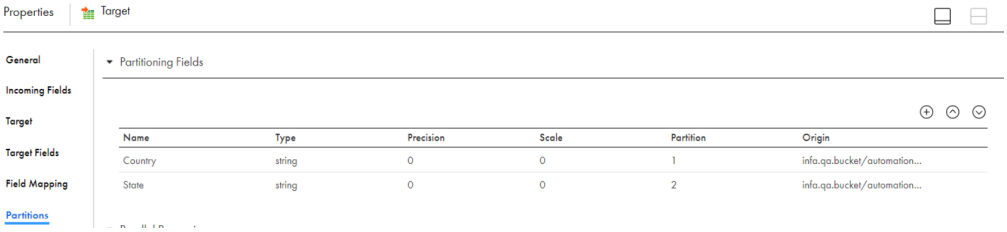
パーティションカラムに書き込むには、次の手順を実行します。

1. ⊕ ［**パーティション**］タブのアイコンをクリックして、ターゲットのパーティションカラムを追加します。次の画像は、パーティションカラムを追加する方法を示しています。

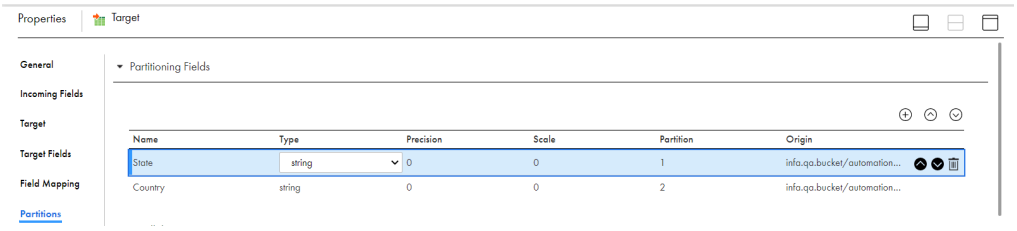
2. ［パーティション］タブで、使用可能なフィールドのリストからパーティションフィールドを選択します。



3. **［選択］**をクリックします。
［パーティション］タブに、選択したパーティションカラムが次のように表示されます。



注: 次の図に示すように、上下の矢印を使用してパーティションの順序を変更できます。



パーティションフォルダからの読み取りとパーティションフォルダへの書き込みに関するルールとガイドライン

パーティションフォルダからの読み取りおよびパーティションフォルダへの書き込みを行う場合は、次のルールとガイドラインを考慮してください。

- パーティションフォルダのみを含むディレクトリをインポートし、詳細ソースプロパティでソースタイプを**［ディレクトリ］**として選択する必要があります。
- データのないパーティションディレクトリをインポートすると、検証エラーが発生します。
- ファイルのみを含み、パーティションフォルダを含まないパーティションディレクトリをインポートすると、検証エラーが発生します。
- パーティションフォルダはあってもパーティションフォルダにファイルがないパーティションディレクトリをインポートすると、検証エラーが発生します。
- Avro、Parquet、および Orc ファイルを使用して、パーティションフォルダからデータを読み書きできます。
- ［FileName］フィールドのパーティション順序は 0 です。
- 選択したパーティションディレクトリには、「FileName」という名前のパーティションカラムを含めることはできません。この名前は、大文字と小文字が区別されません。
- 既存のターゲットオブジェクトをインポートするか、パーティションディレクトリを使用して新しいターゲットオブジェクトを作成すると、ターゲットオブジェクトの［ファイル名］フィールドは表示されません。［FileName］フィールドは、ソースオブジェクトをインポートする場合にのみ表示されます。
- Amazon S3 ソースのパーティションカラムでフィルタトランスフォーメーションをプッシュダウンできます。
- パーティションカラムにタイムスタンプ値を渡すと、値がエンコードされます。例えば、`03:26:01` は `03%3A26%3A01` としてエンコードされます。
- パーティションカラムに特殊文字を含む値を渡した場合、値はエンコードされます。例えば、`@#$#$%%?*`は`@%23$%23$%25%25%3F%2A` としてエンコードされます。
- パーティションフォルダのあるディレクトリをインポートすると、パーティションカラムのデータ型が文字列としてインポートされます。
- パーティションカラムのデータ型を編集することはできません。

- パーティションカラムで［**メタデータの編集**］オプションを使用することはできません。
- ソース側とターゲット側のパーティションディレクトリに［**スキーマの表示**］オプションを使用することはできません。
- スキーマファイルにはパーティションカラムの情報がないため、ソースのパーティションディレクトリに［**スキーマファイルからインポートする**］オプションを使用することはできません。
- パーティションカラムで［**データプレビュー**］オプションを使用することはできません。
- ターゲットオブジェクトがパラメータ化されている場合、マッピングタスクでパーティションカラムを選択することはできません。
- ［**ターゲットの作成**］では、パーティションフィールドを追加し、パーティションカラムを順番に配置できます。パーティションフィールドを追加することや既存のターゲットの順序でパーティションカラムを配置することはできません。
- ［**ターゲットの作成**］で、［**パーティション**］タブの［**ラベル**］カラムはパーティションカラム名を示します。
- パーティションカラムを持つ Amazon S3 オブジェクトをインポートすると、パーティションフィールドがリストの最後に表示されます。
- パーティションカラムに 255 文字を超えるデータが含まれている場合、データは切り捨てられ、255 文字のみがパーティションカラムに書き込まれます。
- パーティションカラム名に 74 文字を超える文字が含まれている場合、名前は切り捨てられ、パーティションカラム名には 74 文字のみが書き込まれます。
- パーティションカラム名パーティションディレクトリ内のターゲットファイルの組み合わせを使用して形成されるパーティションディレクトリファイルパスの値は、1024 文字を超えないようにする必要があります。それ以外の場合、マッピングは失敗します。

パーティションディレクトリへの増分書き込み

詳細モードのマッピング用にパーティションディレクトリに増分的に書き込み、データをパーティションディレクトリに追加できます。

Amazon S3 V2 ターゲットの詳細プロパティの［**存在する場合はファイルを上書き**］オプションを選択しない場合、パーティションディレクトリに段階的に書き込み、データをパーティションディレクトリに追加できます。

実行時にターゲットを作成し、ファイル名が/で終わる場合、Secure Agent は、受信ソースパーティションを既存の親ディレクトリに追加し、ターゲットファイル名にタイムスタンプを追加しません。既存のターゲットの場合、Secure Agent は、受信ソースパーティションを既存の親ディレクトリに追加し、ターゲットファイル名にタイムスタンプを追加しません。

実行時に作成するターゲットのフォルダパスをオーバーライドできます。/で終わるファイル名を指定し、フォルダパスをオーバーライドすると、Secure Agent はパスをフォルダと見なします。ファイル名にフォルダパスは付加されません。

既存のターゲットまたは実行時に作成するターゲットの両方に対して、ファイル名をオーバーライドすることはできません。

分散カラム

マッピングの 1 つのソースから、複数のフラットファイルを Amazon S3 ターゲットに書き込むことができます。詳細ターゲットプロパティで［**分散カラム**］オプションを設定します。

［**分散カラム**］フィールドに 1 つのカラム名を指定して、実行時に複数のターゲットファイルを作成できます。カラム名を指定すると、Secure Agent は、［**分散カラム**］で指定したカラム値に基づいてカラムに複数のターゲットファイルを作成します。

各ターゲットファイル名には、次の形式で［**分散カラム**］の値が付加されます。

```
<Target_fileName>+_+<Distribution column value>+<file extension>
```

各ターゲットファイルには、［**分散カラム**］フィールドで指定したカラムを含む、テーブルのすべてのカラムが含まれます。

例えば、ターゲットファイルの名前が Region.csv で、ファイルに North America および South America という値が含まれるとします。［**分散カラム**］フィールドの値に基づいて次のターゲットファイルが作成されます。

```
Region_North America.csv
Region_South America.csv
```

［**分散カラム**］フィールドに、カラム名を 2 つ指定することはできません。ターゲットフィールドのカラムに存在しないカラム名を指定すると、タスクが失敗します。

値に特殊文字が含まれるカラムを［**分散カラム**］フィールドに指定し、対応するオペレーティングシステムでその特殊文字がサポートされていない場合、Secure Agent はターゲットファイルを作成できません。

例えば、カラムに YYYY/MM/DD 形式の日付値が含まれていると、Secure Agent はターゲットファイルを作成できません。

複数のターゲットオブジェクトへの書き込み

ターゲットオブジェクトをインポートするときに、Secure Agent はインポートされたターゲットオブジェクトにファイル名フィールドを追加します。ターゲットオブジェクトのファイル名フィールドを受信フィールドにマッピングすると、Secure Agent は、ファイル名フィールドに基づいて、フォルダ構造とターゲットファイルを作成します。以下に例を示します。

構文:

```
<tgt_filename_folder>/<tgt_filename=incoming_value_folder>/part_file
```

サンプル:

```
emp_tgt.parquet/emp_tgt.parquet=128000/part-0000-e9ca8-6af-efd43-455c-8709.c000.parquet
```

ファイル名フィールドは、次のファイル形式に適用されます。

- Avro
- ORC
- Parquet

マッピングでターゲットファイル名フィールドを使用する場合は、次のガイドラインを考慮します。

- ソースオブジェクトのファイル名フィールドを、ターゲットオブジェクトのファイル名フィールドにマッピングしないでください。ターゲットオブジェクトのファイル名フィールドを受信フィールドにマッピングした場合、Secure Agent はディレクトリ構造を想定されるようには作成しません。
- ターゲットオブジェクトで FileName フィールドを使用すると、Secure Agent は、NULL 値に対して次のような異なる名前を持つフォルダを作成します。

  - マッピングの場合: _EMPTY_

- 詳細モードのマッピングの場合: _HIVE_DEFAULT_PARTITION_

- ターゲットオブジェクトのファイル名フィールドに、日付タイプの受信フィールドをマッピングした場合、Secure Agent は、ターゲットオブジェクトの受信日付の値に基づいて、ネストされたフォルダ構造を作成します。
- ターゲットオブジェクトのファイル名フィールドに受信フィールドをマッピングした場合、初回のマッピングは正常に実行されます。それ以降の実行で、マッピングは次のエラーで失敗します。
  操作が失敗しました: インデックス: 0、サイズ: 0。

  マッピングを正常に再実行するには、設計時にダミーのターゲットファイルを使用し、詳細ターゲットプロパティでダミーのターゲットファイルを上書きします。

オブジェクトタグ

Amazon S3 バケットに保存されているオブジェクトにタグを追加できます。各タグには、キー値のペアが含まれます。フラットファイルにはオブジェクトタグを使用できます。

オブジェクトにタグを付けると、ストレージの分類に役立ちます。オブジェクトタグの追加は、詳細ターゲットプロパティの［**オブジェクトタグ**］フィールドで行うことができます。Key=Value 形式でオブジェクトタグを入力します。また、次の形式を使って、複数のオブジェクトタグを入力することもできます。

key1=Value1;key2=Value2

キー値のペアを入力するか、キー値のペアを含むファイルパスを指定することができます。例えば、ファイルパスを C:\object\tags.txt 形式で指定できます。Secure Agent がインストールされている任意のファイルパスを指定できます。

Amazon S3 バケットに新しいオブジェクトをアップロードするときに、新しいオブジェクトにタグを追加したり、既存のオブジェクトにタグを追加したりできます。Secure Agent が、Amazon S3 バケット内のタグが含まれるファイルをオーバーライドした場合、そのタグは保持されません。オーバーライドされたファイルに対して新しいタグを追加する必要があります。Amazon S3 バケットに複数のファイルをアップロードする場合、アップロードする各ファイルには、複数のオブジェクトに関連付けられた同じタグセットが必要です。

Amazon S3 V2 ターゲットオブジェクトにタグを追加するには、Amazon S3 ポリシーに s3:PutObjectTagging 権限を追加する必要があります。次に、サンプルポリシーを示します。

```
{
"Version": "2012-10-17",
"Id": "Policy1500966932533",
"Statement": [
{
"Sid": "Stmt1500966903029",
"Effect": "Allow",
"Action": [
"s3:DeleteObject",
"s3:GetObject",
"s3:ListBucket",
"s3:PutObject",
"s3:PutObjectTagging"
],
"Resource": [
"arn:aws:s3:::<bucket_name>/*",
"arn:aws:s3:::<bucket_name>"
]
}
]
}
```

次の表に、キー値のペアを入力する際に Amazon S3 V2 コネクタでサポートされる特殊文字を示します。

特殊文字	サポート
+	○
-	○
=	×
。	○
_	○
:	○
/	○

オブジェクトのタグ付けに関するルールおよびガイドライン

オブジェクトのタグ付けには、次のルールとガイドラインを使用します。

- 1 つのオブジェクトに最大 10 個のタグを追加できます。
- オブジェクトにタグを入力する場合、タグには一意のタグキーが含まれている必要があります。
- タグキーには、最大で 128 文字の Unicode 文字を含めることができ、タグの値には、最大 256 文字の Unicode 文字を含めることができます。
- キーと値では大文字小文字が区別されます。

Amazon S3 V2 のソースとターゲットでのデータ圧縮

Amazon S3 からデータを読み取る場合にデータを解凍し、Amazon S3 にデータを書き込む場合にデータを圧縮します。

次の表に、サポートされるソースの圧縮形式を示します。

圧縮形式	Avro ファイル	バイナリファイル [1]	フラット	JSON ファイル [2]	ORC ファイル	Parquet ファイル
なし	はい	×	はい	○	○	はい
Bzip2	×	×	×	○	×	いいえ
Deflate	はい	×	×	×	×	いいえ
Gzip	×	×	○	×	×	はい
Lzo	×	×	×	×	×	いいえ
Snappy	はい	×	×	×	はい	はい

圧縮形式	Avro ファイル	バイナリファイル [1]	フラット	JSON ファイル [2]	ORC ファイル	Parquet ファイル
Zlib	×	×	×	×	○	いいえ
[1] 詳細モードのマッピングには適用されません。 [2] 詳細モードのマッピングにのみ適用されます。						

次の表に、サポートされるターゲットの圧縮形式を示します。

圧縮形式	Avro ファイル	バイナリファイル [1]	フラット	JSON ファイル [2]	ORC ファイル	Parquet ファイル
なし	はい	×	はい	○	○	はい
Bzip2	×	×	×	○	×	いいえ
Deflate	はい	×	×	○	×	いいえ
Gzip	×	×	はい	○	×	はい
Lzo	×	×	×	×	×	いいえ
Snappy	はい	×	×	はい	○	はい
Zlib	×	×	×	×	○	いいえ
[1] 詳細モードのマッピングには適用されません。 [2] 詳細モードのマッピングにのみ適用されます。						

詳細ソースプロパティと詳細ターゲットプロパティの［**圧縮形式**］オプションで圧縮形式を設定します。

Avro、ORC および Parquet のファイル形式の場合、詳細ソースプロパティの［**圧縮形式**］オプションに表示されていなくても、次の圧縮形式は暗黙的にサポートされます。

圧縮形式	Avro ファイル	ORC ファイル	Parquet ファイル
Deflate	はい	×	いいえ
Snappy	○	○	はい
Zlib	いいえ	○	×

圧縮フラットファイルの読み取り

圧縮フラットファイルからデータを読み取るマッピングを実行する際には、スキーマファイルをアップロードし、圧縮形式として Gzip を選択する必要があります。Gzip 圧縮形式を使用してフラットファイルからデータを読み取る際には**.GZ** ファイル名拡張子を使用します。

1. 必要な圧縮フラットファイルを選択します。
2. ［**形式オプション**］プロパティフィールドに移動します。

3. **［スキーマファイルからインポートする］**オプションを選択し、スキーマをアップロードします。

   フラットファイルのサンプルスキーマファイルを以下に示します。

```
{"Columns":[{"Name":"f_varchar","Type":"string","Precision":"256","Scale":"0"},
{"Name":"f_char","Type":"string","Precision":"256","Scale":"0"},
{"Name":"f_smallint","Type":"string","Precision":"256","Scale":"0"},
{"Name":"f_integer","Type":"string","Precision":"256","Scale":"0"},
{"Name":"f_bigint","Type":"string","Precision":"256","Scale":"0"},
{"Name":"f_decimal_default","Type":"string","Precision":"256","Scale":"0"},
{"Name":"f_real","Type":"string","Precision":"256","Scale":"0"},
{"Name":"f_double_precision","Type":"string","Precision":"256","Scale":"0"},
{"Name":"f_boolean","Type":"string","Precision":"256","Scale":"0"},
{"Name":"f_date","Type":"string","Precision":"256","Scale":"0"},
{"Name":"f_timestamp","Type":"string","Precision":"256","Scale":"0"}]}
```

4. 詳細ソースプロパティの**［圧縮形式］**で**［GZIP］**を選択します。

圧縮 JSON ファイルの読み取り

圧縮 JSON ファイルからデータを読み取るマッピングを実行する際には、スキーマファイルをアップロードし、圧縮形式として Bzip2 を選択する必要があります。Bzip2 圧縮形式を使用して JSON ファイルを読み取る際には**.BZ2** ファイル名拡張子を使用します。

1. 必要な圧縮 JSON ファイルを選択します。
2. **［形式オプション］**プロパティフィールドに移動します。
3. **［スキーマファイルからインポートする］**オプションを選択し、スキーマをアップロードします。

   次の図は、JSON ファイルのサンプルスキーマファイルを示しています。

```
{"Field1":"<string>","Field2":"<string>","Field3":<integer>}
```

   すべてのカラムのデータを含む行を JSON スキーマとして使用します。

4. 詳細ソースプロパティの**［圧縮形式］**で**［Bzip2］**を選択します。

固定長ファイル形式

固定長フラットファイルは、マッピングとマッピングタスクのソースまたはターゲットとして使用できます。

ソーストランスフォーメーションまたはターゲットトランスフォーメーションを設定し、固定長フラットファイルタイプを選択する場合は、固定長フラットファイルのデータに基づいて、使用する最も適切な固定長ファイル形式を選択する必要があります。

固定長フラットファイルについては、次のルールとガイドラインを考慮してください。

- 固定長フラットファイルを、詳細モードのマッピングおよびデータ転送タスクのソースまたはターゲットとして使用することはできません。
- 実行時にフラットファイルターゲットを作成し、固定長ファイル形式を選択すると、Secure Agent は、固定長フラットファイル形式に指定した固定長カラムの境界を無視し、新しいターゲットオブジェクトに追加の固定長属性を適用します。
- 固定長フラットファイルソースから、同じ固定長ファイル形式を使用する空の固定長フラットファイルターゲットに数値データ型のカラムを書き込むと、Secure Agent は、ターゲットの数値カラムの値に Null 文字を追加します。

- 固定長ファイル形式を作成すると、サンプルファイルは、Secure Agent がインストールされているオペレーティングシステムに応じて、改行記号に異なる文字を使用します。ソースファイルが同じ記号を使用していることも確認してください。

  - Linux マシンの場合は、サンプルファイルでの改行記号に\n 文字を使用してください。

  - Windows マシンの場合は、サンプルファイルでの改行記号に\r\n 文字を使用してください。
- 固定長フラットファイルをソースまたはターゲットとして使用する場合、フィールドのメタデータは編集できません。
- datetime データ型のデータを読み取る場合、date 値はミリ秒までしか読み取ることができません。
- 固定長ファイルから double データ型のデータを読み取り、そのデータを Parquet ファイルまたは Avro ファイルに書き込むと、double データ型はターゲットで decimal データ型にマップされます。したがって、データは正しく書き込まれません。
  データをターゲットに正しく書き込むには、ターゲットトランスフォーメーションのメタデータを編集し、decimal データ型を double データ型に変更します。
- 固定長ファイル形式を作成する際は、サンプルフラットファイルが UTF-8 文字セットエンコーディングのみを使用していることを確認してください。

第 4 章

マッピングの Amazon S3 V2 オブジェクト

マッピングを作成する場合、Amazon S3 V2 オブジェクトを表すようにソース、ターゲット、およびルックアップトランスフォーメーションを設定できます。

データ統合の Mapping Designer を使用して、マッピングキャンバスにソース、ターゲット、またはルックアップトランスフォーメーションを追加し、Amazon S3 のソース、ターゲット、およびルックアップのプロパティを設定します。詳細モードでは、Mapping Designer で、高度な機能を有効にするためのトランスフォーメーションと関数を含むようにマッピングキャンバスが更新されます。

マッピングでの Amazon S3 V2 ソース

マッピングでは、Amazon S3 からデータを読み取るソースとして Amazon S3 V2 オブジェクトを表すようにソーストランスフォーメーションを設定できます。

次の表に、ソーストランスフォーメーションで設定できる Amazon S3 V2 ソースのプロパティを示します。

プロパティ	説明
接続名	Amazon S3 V2 ソース接続の名前。ソース接続を選択するか、**[新しいパラメータ]** をクリックしてソース接続の新しいパラメータを定義します。
ソースタイプ	ソースタイプ。次のいずれかのタイプを選択します。 - 単一オブジェクト - パラメータ。マッピングタスクを設定する際に、ソースタイプを定義するには、[パラメータ] を選択します。
オブジェクト	ソースオブジェクトの名前。 オブジェクトを選択する場合に、複数のファイルから読み取るには.manifest ファイルオブジェクトを選択することもできます。
パラメータ	ソースオブジェクトの既存のパラメータを選択するか、**[新しいパラメータ]** をクリックしてソースオブジェクトの新しいパラメータを定義します。パラメータをソースタイプとして選択する場合にのみ、パラメータプロパティが表示されます。実行時にパラメータを上書きする場合は、**[パラメータを上書き]** オプションを選択します。

プロパティ	説明
形式	Amazon S3 V2 コネクタが Amazon S3 からデータを読み取るために使用するファイル形式を指定します。 次のファイル形式タイプを選択できます。 - なし [1] - Flat - Avro - ORC - Parquet - JSON[2] - 構造の検出 [2] デフォルトは［**なし**］です。形式タイプとして［**なし**］を選択すると、Secure Agent は Amazon S3 ファイルからバイナリ形式でデータを読み取ります。 ［構造の検出］形式を選択した場合、パラメータ化されたソースを使用することはできません。 **［形式オプション］**ダイアログボックスを開き、ファイルの形式を定義します。 詳細については、「ファイル形式オプション」 (ページ 54)を参照してください。
インテリジェント構造モデル [2]	［構造の検出］形式タイプに適用できます。インテリジェント構造モデルを選択します。 詳細については、「*コンポーネント*」を参照してください。
[1] 詳細モードのマッピングには適用されません。 [2] 詳細モードのマッピングにのみ適用されます。	

次の表に、Amazon S3 V2 ソースの詳細プロパティを示します。

プロパティ	説明
ソースタイプ	データの読み取り元のソースのタイプ。 次のソースタイプを選択することができます。 - ファイル - ディレクトリ デフォルトは［**ファイル**］です。 詳細については、「Amazon S3 V2 ソースのソースタイプ」 (ページ 28)を参照してください。
フォルダパス	Amazon S3 ソースファイルのバケット名またはフォルダパスを上書きします。 該当する場合は、<bucket_name>/<folder_name>形式にソースファイルが含まれるフォルダ名を追加します。 バケット名を指定せずに、/<folder_name>形式でスラッシュ（/）から始まるフォルダパスを指定した場合、このフォルダパスは接続プロパティで指定したフォルダパスに付加されます。 例えば、このプロパティでフォルダパスを/<dir2>と指定し、接続プロパティでフォルダパスを<my_bucket1>/<dir1>と指定すると、このフォルダパスは、<my_bucket1>/<dir1>/<dir2>形式で接続プロパティで指定したフォルダパスに付加されます。 接続プロパティでフォルダパスを<my_bucket1>/<dir1>と指定し、このプロパティでフォルダパスを<my_bucket2>/<dir2>と指定すると、Secure Agent はこのプロパティで指定したフォルダパス<my_bucket2>/<dir2>のファイルを読み取ります。
ファイル名	Amazon S3 ソースファイルの名前を上書きします。

プロパティ	説明
増分ファイルロード [2]	ディレクトリを詳細モードのマッピングのソースとして使用する場合に、ファイルを増分ロードするかどうかを示します。ファイルを段階的にロードすると、マッピングタスクは、マッピングタスクが最後に実行されてから変更されたディレクトリ内のファイルのみを読み取って処理します。 詳細については、「ファイルの増分ロード」 (ページ 31)を参照してください。
ワイルドカード文字を許可 [2]	ディレクトリソースタイプにワイルドカード文字を使用するかどうかを指定します。 このオプションを選択すると、フォルダパスまたはファイル名に疑問符（?）およびアスタリスク（*）というワイルドカード文字を使用できるようになります。 詳細については、「ワイルドカード文字」 (ページ 31)を参照してください。
再帰読み取りを有効にする [2]	指定されたフォルダとそのサブフォルダおよびファイルから、フラットファイル、Avro ファイル、JSON ファイル、ORC ファイル、または Parquet ファイルを再帰的に読み取るかどうかを指定します。ディレクトリソースタイプを選択する場合に適用されます。 詳細については、「ディレクトリからのファイルの再帰読み取り」 (ページ 32)を参照してください。
Encryption Type(暗号化タイプ)	データの復号化に使用する方法。 以下のいずれかの暗号化タイプを選択できます。 - なし - Informatica Encryption デフォルトは［**なし**］です。 **注**: クライアントサイド暗号化、サーバーサイド暗号化、および KMS 暗号化タイプを使用したサーバーサイド暗号化は選択できません。
ステージングディレクトリ [1]	ローカルステージングディレクトリのパス。 ユーザーがディレクトリに対する書き込み権を持っていることを確認します。さらに、ファイル全体をステージングするのに十分な領域があることを確認します。デフォルトのステージングディレクトリは、Secure Agent をホストするマシンの/temp ディレクトリです。 ディレクトリパスを指定すると、Secure Agent は、次の形式で指定したパーティションの数に応じてフォルダを作成します。 InfaS3Staging<00/11><timestamp>_<partition number>。ここで、00 は読み取り操作を表し、11 は書き込み操作を表します。 例えば、InfaS3Staging000703115851268912800_0 のようになります。。 新しいディレクトリに一時ファイルが作成されます。 ステージングディレクトリのソースプロパティは、Avro、ORC、および Parquet ファイルには適用されません。
Hadoop パフォーマンスチューニングオプション	このプロパティは Amazon S3 V2 コネクタに適用できません。

プロパティ	説明
圧縮形式	Amazon S3 からデータを読み取るときにデータを圧縮解除します。 次の形式でのデータ解凍を選択できます。 - なし - Bzip2[2] - gzip - lzo デフォルトは［**なし**］です。 マッピングで Bzip2 形式の JSON ファイルからデータを読み取る場合に、詳細モードのマッピングのデータを解凍できます。 **注**: このプロパティに Lzo のオプションが表示されていても、Amazon S3 V2 コネクタはこの圧縮形式をサポートしません。 詳細については、「Amazon S3 V2 のソースとターゲットでのデータ圧縮」 (ページ 43)を参照してください。
ダウンロードパートサイズ [1]	Amazon S3 オブジェクトのダウンロードパートサイズをバイト単位で指定します。 デフォルトは 5 MB です。フラット形式タイプのファイルを読み取るマッピングを実行する場合は、このプロパティを使用します。
複数ダウンロードしきい値 [1]	Amazon S3 オブジェクトを複数のパートに分けてダウンロードするための最小しきい値サイズ。 オブジェクトを複数のパートで並行してダウンロードするには、Amazon S3 オブジェクトのファイルサイズが、このプロパティで指定した値よりも大きいことを確認してください。デフォルトは 10MB です。
一時的な資格情報の期間	IAM ユーザーが動的に生成された一時的な資格情報を使用して AWS リソースにアクセスできる期間。期間を秒単位で入力します。 デフォルトは 900 秒です。 900 秒以上が必要な場合、AWS コンソールで期間を最大 12 時間まで設定できます。設定した後で、同じ期間をこのプロパティに入力してください。
トレースレベル	このプロパティは Amazon S3 V2 コネクタに適用できません。

[1] 詳細モードのマッピングには適用されません。
[2] 詳細モードのマッピングにのみ適用されます。

マッピングの Amazon S3 V2 ターゲット

マッピングでは、Amazon S3 にデータを書き込むターゲットとして Amazon S3 V2 オブジェクトを表すようにターゲットトランスフォーメーションを設定できます。

Amazon S3 V2 ターゲットの名前と説明を指定します。ターゲットオブジェクトの Amazon S3 V2 ターゲットと詳細プロパティを設定します。

以下の表に、ターゲットトランスフォーメーションで設定できる Amazon S3 V2 ターゲットプロパティを示します。

プロパティ	説明
接続	Amazon S3 V2 ターゲット接続の名前。ターゲット接続を選択するか、**[新しいパラメータ]** をクリックしてターゲット接続の新しいパラメータを定義します。
ターゲットタイプ	ターゲットのタイプ。次のいずれかのタイプを選択します。 - 単一オブジェクト - パラメータ: マッピングタスクを設定する際に、ターゲットタイプを定義するには、**[パラメータ]** を選択します。
オブジェクト	ターゲットオブジェクトの名前。 既存のオブジェクトを選択するか、ランタイム時にオブジェクトを作成できます。実行時にオブジェクトを作成するときは、ターゲットオブジェクトの名前とパスを入力します。
パラメータ	ターゲットオブジェクトの既存のパラメータを選択するか、**[新しいパラメータ]** をクリックしてターゲットオブジェクトの新しいパラメータを定義します。パラメータをターゲットタイプとして選択する場合にのみ、パラメータプロパティが表示されます。実行時にパラメータを上書きする場合は、**[パラメータを上書き]** オプションを選択します。
ターゲットの作成	ターゲットを作成します。 ターゲットオブジェクトの名前とパスを入力します。ターゲット名では、パラメータファイルに定義したパラメータを使用できます。 詳細については、「ターゲットの作成に関するルールとガイドライン」 (ページ 58)を参照してください。
形式	Amazon S3 V2 コネクタが Amazon S3 のデータを書き込むために使用するファイル形式を指定します。 次のファイル形式タイプを選択できます。 - なし [1] - Flat - Avro - ORC - Parquet - JSON[2] デフォルトは **[なし]** です。形式タイプとして **[なし]** を選択すると、Secure Agent はバイナリ形式でデータを Amazon S3 ファイルに書き込みます。 **[形式オプション]** ダイアログボックスを開き、ファイルの形式を定義します。 形式オプションの詳細については、「ファイル形式オプション」 (ページ 54)を参照してください。
操作	ターゲット操作のタイプ。 Amazon S3 V2 ターゲットでは、挿入操作のみを実行できます。

[1] 詳細モードのマッピングには適用されません。
[2] 詳細モードのマッピングにのみ適用されます。

以下の表に、ターゲットトランスフォーメーションで設定できる Amazon S3 V2 詳細ターゲットプロパティを示します。

プロパティ	説明
存在する場合はファイルを上書き	既存のターゲットファイルを上書きします。 デフォルトは true です。既存のファイルの上書きの詳細については、「既存のファイルの上書き」 (ページ 36)を参照してください。
フォルダパス	Amazon S3 ターゲットファイルの書き込み先のバケット名またはフォルダパス。ここに入力するパスは、実行時に作成するように設定されたターゲットに指定されたパスより優先されます。 該当する場合は、<bucket_name>/<folder_name>形式にターゲットファイルが含まれるフォルダ名を追加します。 バケット名を指定せずに、/<folder_name>形式でスラッシュ（/）から始まるフォルダパスを指定した場合、このフォルダパスは接続プロパティで指定したフォルダパスに付加されます。 例えば、このプロパティでフォルダパスを/<dir2>と指定し、接続プロパティでフォルダパスを<my_bucket1>/<dir1>と指定すると、このフォルダパスは、<my_bucket1>/<dir1>/<dir2>形式で接続プロパティで指定したフォルダパスに付加されます。 接続プロパティでフォルダパスを<my_bucket1>/<dir1>と指定し、このプロパティでフォルダパスを<my_bucket2>/<dir2>と指定すると、Secure Agent はこのプロパティで指定したフォルダパス<my_bucket2>/<dir2>にファイルを書き込みます。
ファイル名	新しいファイル名を作成するか、既存のターゲットファイル名を上書きします。
暗号化タイプ	データの暗号化に使用する方法。 次のいずれかの暗号化タイプを選択します。 - なし - クライアントサイドの暗号化 [1] - サーバーサイドの暗号化 - KMS を使用したサーバーサイド暗号化 - Informatica Encryption デフォルトは［**なし**］です。 暗号化タイプの詳細については、「Amazon S3 V2 ターゲットでのデータ暗号化」 (ページ 34)を参照してください。
ステージングディレクトリ [1]	ローカルステージングディレクトリのパスを入力します。 ユーザーがディレクトリに対する書き込み権を持っていることを確認します。さらに、ファイル全体をステージングするのに十分な領域があることを確認します。デフォルトのステージングディレクトリは、Secure Agent をホストするマシンの/temp ディレクトリです。 ディレクトリパスを指定すると、Secure Agent は、次の形式で指定したパーティションの数に応じてフォルダを作成します。 InfaS3Staging<00/11><timestamp>_<partition number>。ここで、00 は読み取り操作を表し、11 は書き込み操作を表します。 例えば、InfaS3Staging00070311585126891280 0_0 のようになります。 新しいディレクトリに一時ファイルが作成されます。 ステージングディレクトリのターゲットプロパティは、Avro、ORC、および Parquet ファイルには適用されません。
ファイルマージ	このプロパティは Amazon S3 V2 コネクタに適用できません。

プロパティ	説明
Hadoop パフォーマンスチューニングオプション	このプロパティは Amazon S3 V2 コネクタに適用できません。
圧縮形式	データを Amazon S3 に書き込むときに圧縮します。 次の形式でデータを圧縮することができます。 - なし - Bzip2[2] - Deflate - gzip - lzo - Snappy - Zlib デフォルトは［なし］です。 **注**: このプロパティに Lzo のオプションが表示されていても、Amazon S3 V2 コネクタはこの圧縮形式をサポートしません。 圧縮形式の詳細については、「Amazon S3 V2 のソースとターゲットでのデータ圧縮」 (ページ 43)を参照してください。
オブジェクトタグ	Amazon S3 バケットに格納されるオブジェクトに 1 つまたは複数のタグを追加するためのキーと値のペア。 キー値のペアを入力するか、キー値のペアを含むファイルパスを指定することができます。 フラット形式タイプのファイルを書き込むマッピングを実行する場合は、このプロパティを使用します。オブジェクトタグの詳細については、「オブジェクトタグ」 (ページ 42)を参照してください。
TransferManager スレッドプールサイズ [1]	データを並行して書き込むスレッドの数。 デフォルトは 10 です。フラット形式タイプのファイルを書き込むマッピングを実行する場合は、このプロパティを使用します。 Amazon S3 V2 コネクタは `AWS TransferManager API` を使用して、大きなオブジェクトを複数パーツに分けて Amazon S3 にアップロードします。 ファイルサイズが 5MB を超える場合、マルチパートアップロードを設定して、複数パーツに分けたオブジェクトを並行してアップロードできます。 ［TransferManager **スレッドプールサイズ**］を 50 よりも大きく設定した場合、値は 50 に戻ります。
パーティションファイルのマージ [1]	データを Amazon S3 V2 ターゲットに書き込むときに、Secure Agent で複数のパーティションファイルを 1 つのファイルにマージするか、指定されたパーティションの数に基づいて個々のファイルを維持するかを指定します。
一時的な資格情報の期間	IAM ユーザーが動的に生成された一時的な資格情報を使用して AWS リソースにアクセスできる期間。期間を秒単位で入力します。 デフォルトは 900 秒です。 900 秒以上が必要な場合、AWS コンソールで期間を最大 12 時間まで設定できます。設定した後で、同じ期間をこのプロパティに入力してください。
パーツサイズ [1]	Amazon S3 オブジェクトのアップロードパートサイズをバイト単位で指定します。 デフォルトは 5 MB です。フラット形式タイプのファイルを書き込むマッピングを実行する場合は、このプロパティを使用します。

プロパティ	説明
拒否された行の転送	このプロパティは Amazon S3 V2 コネクタに適用できません。
[1] 詳細モードのマッピングには適用されません。 [2] 詳細モードのマッピングにのみ適用されます。	

マッピングを作成した際に Amazon S3 ソースオブジェクトまたは Amazon S3 ターゲットオブジェクトのカラム名に特殊文字が含まれている場合、それらの文字は Secure Agent によってアンダースコア（_）に置き換えられ、マッピングは失敗します。

Amazon S3 V2 ルックアップ

接続済みおよび未接続のキャッシュされたルックアップトランスフォーメーションで Amazon S3 V2 オブジェクトを使用できます。

ルックアップトランスフォーメーションの詳細については、『*トランスフォーメーション*』を参照してください。

ファイル形式オプション

Amazon S3 ファイルの形式を選択する際には、形式オプションを設定できます。

次の表に、Avro、Parquet、JSON、ORC、および区切りフラットファイルの形式オプションを示します。

プロパティ	説明
スキーマソース	ソースファイルまたはターゲットファイルのこのスキーマ。以下のいずれかのオプションを選択して、スキーマを指定することができます。 - データファイルから読み取る。Amazon S3 のファイルからスキーマをインポートします。 - スキーマファイルからインポートする。ローカルマシンのスキーマ定義ファイルからスキーマをインポートします。
スキーマファイル	スキーマ定義ファイルをアップロードします。実行時にターゲットを作成するときに、スキーマファイルをアップロードすることはできません。

次の表に、フラットファイルの形式オプションを示します。

プロパティ	説明
データファイルから読み取る	Amazon S3 のファイルからスキーマをインポートします。 **［データファイルから読み取る］**を選択して JSON[2] ファイル形式を使用する場合は、次のいずれかのオプションを選択できます。 - サンプリングするデータ要素。メタデータから読み取る行数。 - データの処理に使用可能なメモリ。パーサーが JSON サンプルスキーマを読み取って処理するために使用するメモリ。パーサーメモリは増やすことができます。デフォルトは 2MB です。
スキーマファイルからインポートする	ローカルマシンのスキーマ定義ファイルからスキーマをインポートします。 **［スキーマファイルからインポートする］**を選択した場合、**［スキーマファイル］**を選択してスキーマファイルをアップロードできます。 Amazon S3 にデータを書き込む際に**［ターゲットの作成］**オプションを選択した場合は、スキーマファイルをアップロードすることはできません。
フラットファイルタイプ	フラットファイルのタイプ。 次のいずれかのオプションを選択します。 - 区切り。カラム区切り文字を含むフラットファイルを読み取ります。 - 固定長。固定長のフィールドを含むフラットファイルを読み取ります。 **［固定長ファイル形式］**オプションのファイル形式を選択する必要があります。 固定長ファイル形式がない場合、**［新規］** > **［コンポーネント］** > **［固定長ファイル形式］**をクリックして作成します。
区切り文字	データのカラムを区切るために使用される文字。カンマ、タブ、コロン、セミコロンなどのパラメータを設定できます。タブを区切り文字として設定するには、任意のテキストエディタでタブ文字を入力する必要があります。その後、そのタブ文字をコピーして［区切り文字］フィールドに貼り付けます。 ソースオブジェクトの区切り文字としてマルチバイト文字を指定しないでください。
エスケープ文字	引用符で囲まれていない文字列におけるカラム区切り文字の直前の文字、または引用符で囲まれた文字列内における引用符の直前の文字。 文字または\<10 進数値>を指定できます。\<10 進数値>を指定すると、エージェントは、10 進値の ASCII 文字をエスケープ文字と見なします。 例えば、\64 を指定すると、エージェントは ASCII 文字@と見なします。 エスケープ文字を無視するには、\0 と指定します。
修飾子	データの境界を定義する引用符。 修飾子は、一重引用符または二重引用符で設定できます。
修飾子モード	ターゲットオブジェクトの修飾子の動作を指定します。 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。 - 最小。区切り文字の値があるデータに修飾子を適用します。特殊文字がない場合、Secure Agent はターゲットへのデータ書き込み時に修飾子を適用しません。 - すべて。空でないすべてのカラムに修飾子を適用します。 デフォルトモードは最小です。

プロパティ	説明
コードページ	エージェントがデータの読み取りまたは書き込みに使用する必要があるコードページを選択します。 Amazon S3 V2 コネクタは、以下のコードページをサポートしています。 - MS Windows Latin 1。ISO 8859-1 Western European データの場合に選択します。 - UTF-8。Unicode および Unicode 以外のデータの場合に選択します。 - Shift-JIS。ダブルバイト文字データの場合に選択します。 - ISO 8859-15 Latin 9（Western European）。 - ISO 8859-2 Eastern European。 - ISO 8859-3 Southeast European。 - ISO 8859-5 Cyrillic。 - ISO 8859-9 Latin 5（Turkish）。 - IBM EBCDIC International Latin-1。
ヘッダー行番号	Amazon S3 からのデータの読み取り時にヘッダーとして使用する行番号を指定します。ヘッダーがないファイルを読み取ることもできます。 ヘッダーのないファイルからデータを読み取るには、**［ヘッダー行番号］** フィールドの値を 0 に指定します。ヘッダーのあるファイルからデータを読み取るには、**［ヘッダー行番号］** フィールドの値を 1 以上の値に設定します。 このプロパティは、ソースデータをプレビューするとき、およびマッピングの実行時に適用されます。 デフォルトは 1 です。
最初のデータ行 [1]	Secure Agent がデータの読み取りを開始する行番号を指定します。1 以上の値を入力する必要があります。 ヘッダーからデータを読み取るには、**［ヘッダー行番号］** と **［最初のデータ行］** のフィールドに同じ値を指定する必要があります。デフォルトは 1 です。 このプロパティは、実行時およびファイルを読み取るためのデータプレビュー時に適用されます。このプロパティは、ファイルを書き込むためのデータプレビュー時に適用されます。
ターゲットヘッダー	フラットファイルでヘッダーを含むターゲットとヘッダーを含まないターゲットのどちらにデータを書き込むかを指定します。**［ヘッダーあり］** オプションまたは **［ヘッダーなし］** オプションを選択できます。 このプロパティは、Amazon S3 ソースからデータを読み取るときには適用されません。
分散カラム [1]	実行時に複数ターゲットファイルの作成に使用するカラムの名前を指定します。 このプロパティは、Amazon S3 ソースからデータを読み取るときには適用されません。分散カラムの詳細については、「分散カラム」（ページ 41）を参照してください。
エスケープ文字データを保持	Amazon S3 V2 コネクタには適用されません。
プレビューする最大行数	Amazon S3 V2 コネクタには適用されません。
行区切り文字	Amazon S3 V2 コネクタには適用されません。

[1] 詳細モードのマッピングには適用されません。
[2] 詳細モードのマッピングにのみ適用されます。

次の表に、JSON ファイルの形式オプションを示します。

プロパティ	説明
サンプリングするデータ要素 [1]	メタデータを取り込むための最良の一致を見つけるために読み取る行数を指定します。
データの処理に使用可能なメモリ [1]	パーサーが JSON サンプルスキーマを読み取って処理するために使用するメモリ。 デフォルト値は 2 MB です。 ファイルサイズが 2 MB を超える場合、エラーが発生する可能性があります。読み取るファイルサイズに値を設定します。
複数行の JSON ファイルの読み取り	該当なし。
[1] 詳細モードのマッピングにのみ適用されます。	

形式オプションの設定に関するルールとガイドライン

Amazon S3 ファイル形式タイプを選択するときは、適切な形式オプションを設定する必要があります。

形式タイプを選択し、形式オプションを設定するときは、以下のガイドラインを使用します。

- JSON 形式は、詳細モードのマッピングにのみ使用できます。
- マッピングを作成し、**[形式オプション]** タブをクリックしなかった場合、Secure Agent はデフォルトの **[入力形式]** を **[なし]** と見なします。
- Avro、JSON、ORC、または Parquet の形式タイプを選択し、**[スキーマソース]** 形式オプションの値に **[データファイルから読み取る]** を選択した場合、区切り文字、エスケープ文字、および修飾子の各オプションを設定することはできません。
- [入力形式] で Avro、JSON、ORC、または Parquet を選択し、**[スキーマソース]** 形式オプションの値に **[スキーマファイルからインポートする]** を選択した場合、**[スキーマファイル]** プロパティフィールドでスキーマファイルのアップロードのみを行えます。区切り文字、エスケープ文字、および修飾子の各オプションを設定することはできません。
- フラット形式タイプを選択し、**[スキーマソース]** 形式オプションの値に **[スキーマファイルからインポートする]** を選択した場合、JSON 形式でスキーマファイルのみをアップロードできます。
  次のサンプルは、フラットファイルのスキーマファイルを示しています。

  ```
  {"Columns":[{"Name":"f_varchar","Type":"string","Precision":"256","Scale":"0"},
  {"Name":"f_char","Type":"string","Precision":"256","Scale":"0"},
  {"Name":"f_smallint","Type":"string","Precision":"256","Scale":"0"},
  {"Name":"f_integer","Type":"string","Precision":"256","Scale":"0"},
  {"Name":"f_bigint","Type":"string","Precision":"256","Scale":"0"},
  {"Name":"f_decimal_default","Type":"string","Precision":"256","Scale":"0"},
  {"Name":"f_real","Type":"string","Precision":"256","Scale":"0"},
  {"Name":"f_double_precision","Type":"string","Precision":"256","Scale":"0"},
  {"Name":"f_boolean","Type":"string","Precision":"256","Scale":"0"},
  {"Name":"f_date","Type":"string","Precision":"256","Scale":"0"},
  {"Name":"f_timestamp","Type":"string","Precision":"256","Scale":"0"}]}
  ```

- 次の例外を避けるために、選択する Avro、JSON、ORC、または Parquet の形式タイプに適した **[形式オプション]** を設定します。

  ```
  invalid character encapsulated
  ```

- Amazon S3 V2 はこの機能をサポートしていないため、形式オプションで **[複数行の JSON ファイルの読み取り]** チェックボックスを選択することはできません。

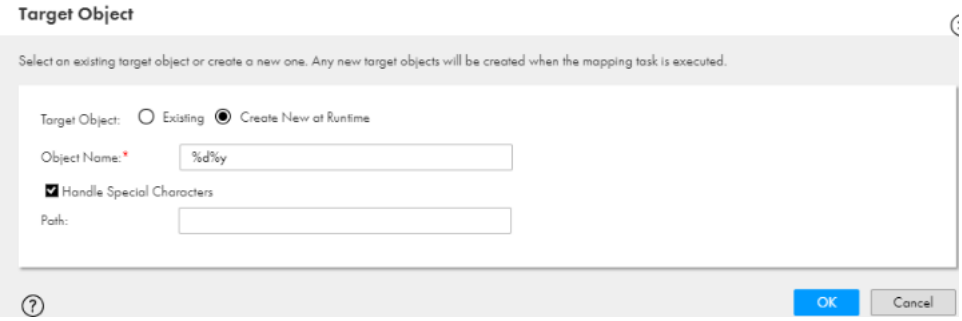
ターゲットの指定

マッピングの結果は、既存のターゲットに保存することも、新たにターゲットを作成して保存することもできます。ターゲットを作成することを選択した場合、Secure Agent はタスクの実行時にターゲットを作成します。

ターゲットのプロパティを指定するには、次の手順に従います。

1. マッピングでターゲットトランスフォーメーションを選択します。
2. **[受信フィールド]** タブで、ターゲットに含めるフィールドを指定するフィールドルールを設定します。
3. ターゲットを指定するには、**[ターゲット]** タブをクリックします。
4. ターゲット接続を選択します。
5. ターゲットタイプとして **[単一オブジェクト]** または **[パラメータ]** を選択します。
6. ターゲットオブジェクトまたはパラメータを指定します。.csv ターゲットファイル名を指定する必要があります。
   - 実行時にターゲットファイルを作成するには、Accounts.csv のように、拡張子を含めてターゲットファイルの名前を入力します。
7. ファイルの形式オプションを設定する場合は、**[形式オプション]** をクリックし、**[OK]** をクリックします。
8. **[選択]** をクリックしてターゲットオブジェクトを選択します。既存のターゲットオブジェクトを選択するか、実行時に新しいターゲットオブジェクトを作成し、オブジェクト名を指定することができます。

   次の図は、**[ターゲットオブジェクト]** ボックスを示しています。



9. 必要に応じて、ターゲットの詳細プロパティを指定します。

ターゲットの作成に関するルールとガイドライン

[ターゲットの作成] プロパティを使用する場合は、次のルールとガイドラインを考慮してください。

- ターゲット名に英数字を含めることはできません。ファイル名では、ピリオド（.）、アンダースコア（_）、アットマーク（@）、ドル記号（$）、パーセント記号（%）のみを特殊文字として使用できます。
- **[ターゲットの作成]** を使用して Avro、ORC、または Parquet ファイルを作成し、ターゲットディレクトリにコロン（:）を含むファイル名がある場合、マッピングは失敗します。
- 既存のターゲット名を指定した場合、警告メッセージは表示されません。しかし、Secure Agent により既存のターゲットが同じファイル名で上書きされます。
- **[ターゲットの作成]** オプションを使用して Avro、ORC、または Parquet ファイルを書き込む場合、NULL データ型は指定できません。
- ソースで JSON ファイルの文字列カラムの精度を設定し、**[ターゲットの作成]** を選択すると、文字列カラムのデフォルトの精度が保持されます。

- ファイルまたはディレクトリのソースタイプを選択し、**［実行時に新規作成］**を選択して、マッピングを実行すると、マッピングが成功した場合でも、Tomcat ログに次の例外が表示されます。
  Internal error.無効なパス要素[Partition]が検出されたため、エラーが発生しました。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。
- フォルダパスとファイル名を指定し、**［実行時に新規作成］**を選択してマッピングを実行すると、マッピングが成功した場合でも Tomcat ログに次の例外が表示されます。
  java.lang.RuntimeException: Exception occured during the mapgen using EXACT_PATH approach: Only bucket name can be changed in the connection.Folder path change is not supported.

  ファイル名のみを指定し、**［実行時に新規作成］**を選択して、マッピングを実行すると、マッピングが成功した場合でも、Tomcat ログに次の例外が表示されます。
  java.lang.RuntimeException: Exception occured during the mapgen using EXACT_PATH approach: String index out of range: -1
- フォルダパスとファイル名を指定し、詳細モードのマッピングを実行して、実行時に作成されたターゲットにデータを書き込むと、マッピングが成功した場合でも Tomcat ログに次の例外が表示されます。
  [Exception occured during the mapgen using EXACT_PATH approach: The following object <target_object_name> is not found in the <bucket_name>]

  このメッセージは無視してください。例外は誤解を招く恐れがあります。
- 実行時に作成したフラットファイルにデータを書き込んだ場合は、ターゲットフラットファイルの最後に空白行が含まれます。

ターゲットオブジェクトのパスのルールおよびガイドライン

［ターゲットの作成］プロパティでパスを指定する場合は、次のルールとガイドラインを考慮してください。

- パスを指定する場合、Secure Agent はこのプロパティで指定したパスおよび**［フォルダパス］**接続プロパティで指定したバケット内にターゲットオブジェクトを作成します。Secure Agent は次の形式でターゲットオブジェクトを作成します。<bucket_name>/<path_name>/<target_object_name>。
- Secure Agent はバケットのみを使用し、**［フォルダパス］**接続プロパティで指定したパスは無視します。例えば、パスを folder1/folder2、ターゲットオブジェクト名を Records と指定します。接続プロパティの**［フォルダパス］**で<bucket_name>/folder3 と指定します。Secure Agent は次の場所にターゲットオブジェクトを作成します。<bucket_name>/folder1/folder2/Records。
- パスを指定していない場合、Secure Agent は、次の形式で**［フォルダパス］**接続プロパティで指定したバケット内にターゲットオブジェクト名を作成します。<bucket_name>/<target_object_name>。
  例えば、パスを指定せず、ターゲットオブジェクト名に Records を指定すると、Secure Agent は、次の形式で**［フォルダパス］**接続プロパティで指定したバケット内にターゲットオブジェクトを作成します。<bucket_name>/Records。
- パスにバケット名は指定しないでください。
  - マッピングの場合、パスにバケット名を指定すると、バケット名はフォルダパス内のフォルダと見なされます。例えば、パスを<bucket_name>/<path_name>のように指定した場合、<bucket_name>はフォルダと見なされます。
  - 詳細モードのマッピングの場合、パスにバケット名を指定すると、バケット名は無視されます。

Amazon S3 V2 ターゲットファイルのパラメータ化

Amazon S3 V2 ターゲットオブジェクトのファイル名とターゲットフォルダの場所をパラメータ化して、実行時にファイル名とフォルダの場所を渡すことができます。フォルダが存在しない場合は、Secure Agent によっ

てフォルダ構造が動的に作成されます。Amazon S3 V2 ターゲットファイルのパラメータ化は、マッピングにのみ適用されます。

タイムスタンプを使用したパラメータ化

タイムスタンプ情報をファイル名に追加して、ファイルがいつ作成されたかを示すことができます。フラット形式タイプのファイルを書き込むマッピングを作成する場合は、タイムスタンプを使用したパラメータ化を使用できます。

ターゲットファイルのファイル名を指定するとき、マッピングタスクがタイムスタンプ情報をファイル名に追加するために使用する Apache STRFTIME 関数の形式に基づいて特殊文字を含めます。**[特殊文字の処理]** オプションを有効にして、ファイル名に含まれる%[mod]という形式の特殊文字を処理する必要があります。マッピングで STRFTIME 関数の形式を使用できます。

[特殊文字の処理] を有効にすると、Secure Agent は **[ターゲットの作成]** の入力パラメータと出力パラメータを無視します。

次の表に、マッピングまたはマッピングタスクで使用される一般的な STRFTIME 関数の形式を示します。

特殊文字	説明
%d	2 桁の 10 進数で表される日（01～31）。
%m	2 桁の 10 進数で表される月（01～12）。
%y	2 桁の 10 進数で表される、世紀を含まない年（00～99）。
%Y	世紀を含む年（2015 など）。
%T	24 時間表記の時刻（%H:%:M:%S に相当）。
%H	24 時間表記の時間（00～24）。
%l	12 時間表記の時間（01～12）。
%M	10 進数で表される分（00～59）。
%S	10 進数で表される秒（00～60）。
%p	AM または PM。

パラメータファイルを使用したパラメータ化

パラメータファイルを使用して Amazon S3 V2 ターゲットファイルをパラメータ化できます。フラット形式タイプのファイルを書き込むマッピングを作成する場合は、パラメータファイルを使用できます。

パラメータファイルを使用して Amazon S3 V2 ターゲットファイルをパラメータ化するには、次の手順を実行します。

1. Amazon S3 V2 ターゲットオブジェクトを作成します。
2. **[ターゲットの作成]** オプションで、**[ターゲットファイル名]** の値を$p1、**[ターゲットオブジェクトパス]** の値を$p2 に指定します。
3. ターゲットオブジェクト名とターゲットオブジェクトパスに追加したパラメータを、パラメータファイルで定義します。

以下に例を示します。

```
$p1=filename
$p2=path
```

4. パラメータファイルを次の場所に配置します。

   `<Informatica Cloud Secure Agent\apps\Data_Integration_Server\data\userparameters>`

5. マッピングタスクの［**スケジュール**］タブでパラメータファイル名を指定します。
6. マッピングタスクを保存して実行します。

詳細モードのマッピングのルールとガイドライン

詳細モードのマッピングを作成する場合は、次のガイドラインを考慮してください。

- 詳細モードのマッピングを実行するときに、次の形式のフォルダがターゲットで作成され、そのフォルダ内に複数のターゲットファイルが生成されます: `<target_foldername>.<file_extension>`。
- 詳細モードのマッピングでデータを Amazon S3 ファイルに書き込むときに、ファイルがフォルダに置き換えられ、フォルダ内にターゲットファイルが生成されます。同じ Amazon S3 ファイルを参照する別の詳細モードのマッピングを作成すると、ファイルが見つからず、次のエラーメッセージが発生してマッピングが失敗します。

  `Operation failed: Index: 0, Size: 0.`
- ファイルから読み取るように読み取り操作を設定する場合は、ファイル名の先頭の文字を_または.以外にする必要があります。
- ルックアップトランスフォーメーションを設定して複数一致時にエラーを報告するように［エラーを報告］オプションを選択した場合、不一致カラムのデータはエラーメッセージが表示されずにターゲットに書き込まれます。
- JSON ファイルからデータを読み取る際、行のいずれかに不適切な Boolean 値が含まれていた場合、すべての行が拒否され、NULL 値がターゲットに書き込まれます。
- Unicode 文字を含む JSON ファイルからデータを読み取ると、データの不整合が発生する場合があります。
- Amazon S3 V2 コネクタがサポートしていないデータ型を選択すると、マッピングが失敗するか、すべての行が拒否される可能性があります。
- メタデータ解決用の JSON サンプルデータファイルの一部として`"{"Elements":[]}"`などの空の配列要素がある場合、JSON パーサーは次のエラーで失敗します。

  `[SDK_APP_COM_20000] error [Array must contain at least 1 element for projection].`

  メタデータ解決のための空の配列なしで、スキーマ全体をサンプルデータ行として入力します。［スキーマファイルからインポートする］オプションを使用して、このファイルをアップロードできます。
- メタデータ解決用の JSON サンプルデータファイルの一部として`"{"Elements":[]}"`などの空の構造体要素がある場合、JSON パーサーは次のエラーで失敗します。

  `Struct must contain at least one key :: fields`

  メタデータ解決のための空の構造体なしで、スキーマ全体をサンプルデータ行として提供します。［スキーマファイルからインポートする］オプションを使用して、このファイルをアップロードできます。
- JSON パーサーは、配列の最初の値を使用して、配列要素のデータ型を解釈します。例えば、最初の値が整数で、その後に長い値が含まれている場合、メタデータは整数として解決されます。実行時に、長整数型の値が DTM バッファに収まらないため、行全体がドロップされます。

  メタデータの解決に必要なデータ型またはサブフィールドを含む最初の配列または構造体要素を含むサンプルデータ行として、スキーマ全体を入力します。［スキーマファイルからインポートする］オプションを使用して、このファイルをアップロードできます。

- JSON ファイルからのメタデータの解釈に使用される最初の行サイズには 2MB の制限があります。データファイルの最初の行が 2MB より大きい場合、JSON パーサーは失敗します。

  構造体要素と配列要素から追加のタグを削除して、サンプルデータの行サイズを減らします。JSON パーサーは、構造体要素と配列要素内の最初の要素のみを必要とします。最初の要素でメタデータの解決に必要なデータ型またはサブフィールドを指定します。［スキーマファイルからインポートする］オプションを使用して、このファイルをアップロードできます。
- ステージングディレクトリのソースとターゲットの詳細プロパティは適用されません。ただし、詳細設定の Amazon S3 のステージングディレクトリを指定する必要があります。詳細については、「*Administrator*」を参照してください。
- 修飾子モードを［最小］に設定してエスケープ文字を使用すると、ターゲットでは文字はエスケープされず、引用符で囲まれます。修飾子モードを［すべて］に設定します。
- 修飾子モードを［すべて］に設定し、修飾子の値を指定しない場合、\0（NUL）が修飾子と見なされます。
- フラットソースファイルをパラメータ化すると、FileName フィールドがソースフィールドに表示されます。回避策として、ターゲットの受信フィールドにルールを追加し、FileName フィールドを除外します。

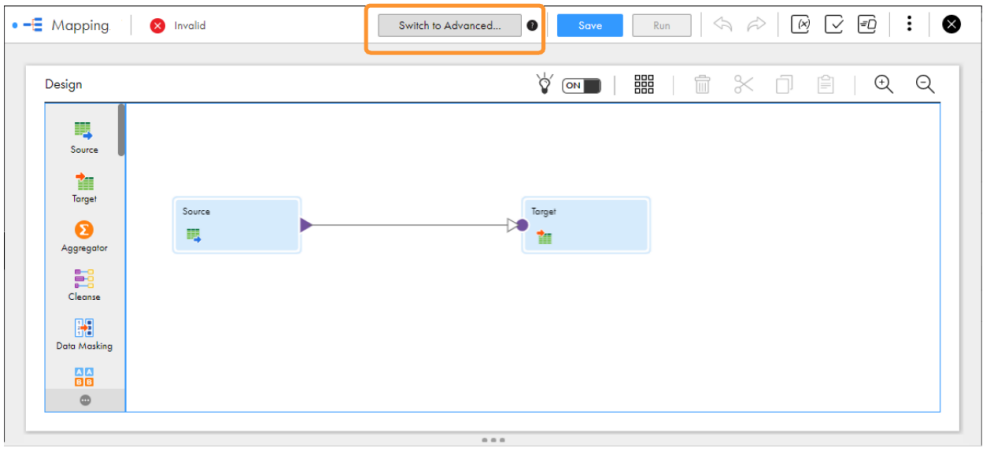
詳細モードのマッピングの例

運用中の学生データベースで数百万件のレコードを保持している大規模なコミュニティカレッジで働いているとします。カレッジでは、世界中の 45 か所のキャンパスと 700 か所の拠点に 10,000 人以上の教職員がいます。非常に大規模な IT インフラストラクチャを保有していて、毎日インターネットからおよそ 15 TB の情報がダウンロードされています。

パフォーマンスと拡張性の問題を回避し、高額なコストが発生しないようにするために、このカレッジではデータ全体をオペレーショナルデータストアから Amazon S3 に短期間で移行するよう計画しています。Amazon S3 からすべての注文レコードを読み取って Amazon Redshift ターゲットに書き込む場合のパフォーマンスを向上させるために、詳細モードで実行されるマッピングを作成します。

1. データ統合で、**［新規］** > **［マッピング］** > **［マッピング］** をクリックします。
2. Mapping Designer で、**［詳細に切り替え］** をクリックします。

   次の図は、Mapping Designer の **［詳細に切り替え］** ボタンを示しています。



3. **［詳細に切り替え］**ダイアログボックスで、**［詳細に切り替え］**をクリックします。

   Mapping Designer でマッピングキャンバスが更新され、詳細モードで使用できるトランスフォーメーションと関数が表示されます。

4. マッピングの名前、場所、説明を入力します。
5. ソーストランスフォーメーションの全般プロパティで、名前と説明を指定します。
6. **［ソース］**タブで、次の手順を実行して、ソースからデータを読み込むためのソース詳細を入力します。
   a. **［接続］**フィールドで、必要なソース接続を選択します。
   b. **［ソースタイプ］**フィールドで、ソースのタイプを選択します。
   c. **［オブジェクト］**フィールドで、必要なオブジェクトを選択します。
   d. **［詳細プロパティ］**セクションで、適切な値を入力します。
7. **［フィールド］**タブで、ソースフィールドをターゲットフィールドにマッピングします。
8. ターゲットトランスフォーメーションの全般プロパティで、名前と説明を指定します。
9. **［ターゲット］**タブで、次の手順を実行して、Amazon S3 ターゲットにデータを書き込むためのターゲット詳細を入力します。
   a. **［接続］**フィールドで、Amazon S3 V2 ターゲット接続を選択します。
   b. **［ターゲットタイプ］**フィールドで、ターゲットのタイプを選択します。
   c. **［オブジェクト］**フィールドで、必要なオブジェクトを選択します。
   d. **［操作］**フィールドで、必要な操作を選択します。
   e. **［詳細プロパティ］**セクションで、詳細プロパティに適切な値を指定します。
10. ソースおよびターゲットをマッピングします。
11. **［保存］** > **［実行］**をクリックして、マッピングを検証します。

    ［監視］で、タスクの実行後にログのステータスを監視できます。

第 5 章

マッピングの移行

ある環境で接続とマッピングを設定した後で、別の環境に移行してマッピングを実行することができます。詳細モードで設定されたマッピングを移行することもできます。

移行後は、Administrator サービスから接続プロパティを変更できますが、マッピングを変更する必要はありません。データ統合は、以前の環境で設定されたランタイム属性を使用して、新しい環境でマッピングを正常に実行します。

開発組織（組織 1）でマッピングを開発し、次にプロダクション組織（組織 2）でマッピングを移行して実行するシナリオについて考えてみます。移行後に、組織 2 で同一または異なる接続エンドポイントあるいはオブジェクトパスを使用することが必要になる場合があります。要件に応じて、移行を計画する前に、この節のガイドラインを考慮してください。

移行されたマッピングへの同じオブジェクトパスの使用

組織 2 に移行されたマッピングで組織 1 と同じオブジェクトパスを使用する場合は、組織 2 の Amazon S3 アカウントで同じフォルダパスとファイル名を使用する必要があります。

例えば、組織 1 に使用されるアカウント 1 と組織 2 に使用されるアカウント 2 という 2 つの異なるアカウントがある場合、フォルダパスとファイル名は、次のように両方のアカウントで同じである必要があります。

アカウント 1: folder1/filename1

アカウント 2: folder1/filename1

このシナリオでは、詳細プロパティのフォルダパスとファイル名をオーバーライドする必要はありません。

同じオブジェクトパスに関するルールとガイドライン

移行されたマッピングに同じオブジェクトパスを使用する場合は、次のルールとガイドラインを考慮してください。

- 接続のフォルダパスにバケット名を指定する場合は、フォルダパスにバケット名のみを指定できます。例えば、`bucket1/folder1` のようにバケット名とフォルダ名を指定することはできません。ない場合、マッピングはエラーで失敗します。
- フォルダパスにバケット名が含まれるマッピングを移行すると、バケット名のみが変更されます。例えば、マッピングにソースオブジェクト `bucket1/folder1/source1` がある場合、接続にフォルダパス `bucket2` を持つ組織 2 にこのソースオブジェクトをインポートすると、データは `bucket2/folder1/source1` から読み取られます。

- 詳細モードのマッピングの場合、組織 1 の接続でフォルダパスを bucket1/folder1 として指定し、フォルダパス bucket2 を持つ組織 2 にマッピングを移行すると、マッピングはフォルダ bucket2/bucket1/folder1 にデータを書き込みます。
  マッピングは、データをフォルダ bucket2/folder1 に書き込みます。

移行されたマッピングへの別のオブジェクトパスの使用

マッピングを移行した後に、別のオブジェクトパスを使用して、新しい環境からマッピングを実行できます。

このシナリオでは、マッピングを移行する前に、オブジェクトメタデータ、ランタイム属性、または接続属性を変更して、移行された環境にオブジェクトパスを反映させることができます。新しい環境でマッピングを編集または更新する必要はありません。

原則として、詳細プロパティ、接続、またはオブジェクトプロパティでフォルダパスとファイル名を指定すると、データ統合は次の優先順位で属性を使用します。

1. **ランタイムの詳細属性**。マッピングのソース、ターゲット、またはルックアップトランスフォーメーションのフォルダパスやファイル名などの詳細プロパティ。
2. **接続属性**。接続プロパティのフォルダパス属性。
3. **オブジェクトメタデータ**。マッピングのソース、ターゲット、またはルックアップトランスフォーメーションで選択されたオブジェクト。

移行オプション

移行を行うときは、次のオプションのいずれかを選択して、オブジェクトパスを更新できます。

オプション 1: 接続プロパティを更新して、新しいオブジェクトを参照する

マッピングを組織 2 にインポートすると、**[接続の確認]** セクションで既存の接続を変更して、組織 2 の指定されたフォルダパスおよびファイル名にアクセス可能な接続にマッピングできます。

オプション 2: 詳細プロパティからプロパティをオーバーライドする

移行の前に、組織 1 のマッピングの詳細プロパティで、組織 2 のオブジェクトに必要なフォルダパスおよびファイル名を指定します。

移行後にマッピングを実行すると、Secure Agent は設定された詳細パラメータを使用して、指定されたオブジェクトを組織 1 からインポートされたマッピングでオーバーライドします。

オプション 3: マッピングのプロパティをパラメータ化する

移行前に、フォルダパスやファイル名などの詳細属性をパラメータ化するという選択ができます。マッピングでは、入力パラメータ、入出力パラメータ、およびパラメータファイルを設定できます。マッピングを移行した後は、マッピングを編集または更新しないでください。フォルダパスやファイル名などの詳細属性に入出力パラメータを使用した場合は、パラメータファイルからこれらのパラメータを更新できます。

マッピング内のオブジェクトではなく、詳細プロパティのみをパラメータ化する

詳細プロパティのみをパラメータ化し、実行時にそれらのプロパティを使用する場合は、マッピングのオブジェクトプロパティでプレースホルダオブジェクトを選択してから、詳細プロパティからこのプレースホルダオブジェクトへのオーバーライドを指定します。プレースホルダオブジェクトに、オーバーライドとして指定した対応するテーブルと同じメタデータが含まれていることを確認してください。マッピングを実行すると、詳細プロパティで指定した値でプレースホルダオブジェクトがオーバーライドされます。

オブジェクトと詳細プロパティをパラメータ化する

Amazon S3 オブジェクトタイプと詳細フィールドをパラメータ化したままにする場合は、パラメータの追加時に入力パラメータウィンドウで［**実行時にパラメータのオーバーライドを許可**］オプションが選択されていない状態で、必要なオブジェクトをタスクレベルで選択します。タスクを実行すると、詳細プロパティで指定した値が優先されます。

パラメータ化ルール

オブジェクトと詳細プロパティをパラメータ化する場合は、次のルールを考慮してください。

- パラメータ化は、［**ターゲットの作成**］オプションを使用するマッピングには適用されません。
- パラメータ化は、移行のユース ケースにおける詳細モードのマッピングには適用されません。
- ［**実行時にパラメータのオーバーライドを許可する**］チェックボックスを有効にして、接続またはオブジェクトをパラメータ化することはできません。

ルールおよびガイドライン

移行されたマッピングに同じオブジェクトパスまたは異なるオブジェクトパスを使用する場合は、次のルールとガイドラインを考慮してください。

- 次の表に、トランスフォーメーション、オブジェクトタイプ、および新しい環境に移行したときに保持されるマッピングの詳細プロパティのフィールドを示します。

トランスフォーメーション	オブジェクトタイプ	詳細フィールド
ソース	単一オブジェクト	フォルダパスとファイル名
ルックアップ	単一オブジェクト	
ターゲット	単一オブジェクト	

- マッピングを組織 1 から組織 2 に移行した後は、マッピングを編集しないでください。
- 組織 2 の既存のターゲットオブジェクトについては、詳細プロパティでフォルダパスとファイル名を指定する必要があります。オブジェクトが組織 2 に存在しない場合、または接続が組織 1 で使用したオブジェクトにアクセスできない場合、403 エラーが発生してマッピングは失敗します。
- 詳細プロパティで有効なフォルダとファイル名が指定されていることを確認してください。有効なフォルダとファイル名が指定されていない場合、マッピングは失敗します。
- ターゲットオブジェクトで FileName フィールドを使用しており、フォルダパスとファイル名をオーバーライドして、マッピングを組織 2 に移行すると、403 エラーが発生してマッピングは失敗します。この問題は、組織 2 の接続が、組織 1 で使用したバケット、オブジェクト、およびフォルダのパスにアクセスできない場合に発生します。
- フォルダパスの詳細プロパティでワイルドカード文字を指定する場合、名前パターンに一致するすべてのフォルダには、同じメタデータと形式オプションを持つファイルが含まれている必要があります。
- サブディレクトリからファイルを再帰的に読み取る場合、オーバーライドするフォルダパスの詳細プロパティには、ディレクトリ内のファイルが含まれている必要があります。
  例えば、フォルダパスを<bucket1>/<dir1>のように指定した場合、ファイルがディレクトリ<dir1>:<bucket1>/<dir1>/<file1>に存在することを確認します。

  フォルダパスの詳細プロパティにサブディレクトリ内のみのファイルが含まれ、ディレクトリにファイルが含まれていない場合、マッピングは失敗します。

- 実行時にデータオブジェクトスキーマを動的に更新することはできません。スキーマ変更処理はサポートされないため、ソース、ターゲット、またはルックアップトランスフォーメーションで選択されたテーブルおよび対応する詳細フィールドのオーバーライドに対して同じメタデータを使用する必要があります。
- 新しい環境に移行するマッピングでは、Informatica 暗号化を除くすべての暗号化タイプを設定できます。
- ソースタイプを［ディレクトリ］として選択した場合、マッピングを正常に実行するには、.tmp などの自動生成されたトランザクションファイルをすべて削除します。_SUCCESS および.CRC ファイルは無視されます。
- バケット名を指定せずに、詳細プロパティでスラッシュ（/）から始まる/<folder_name>という形式のフォルダパスを指定した場合、接続プロパティで指定したフォルダパスがこのフォルダパスに追加されます。

  例えば、詳細プロパティでフォルダパスを/<dir2>と指定し、接続プロパティでフォルダパスを<my_bucket1>/<dir1>と指定すると、このフォルダパスは、接続プロパティで指定したフォルダパスに<my_bucket1>/<dir1>/<dir2>という形式で追加されます。

  接続プロパティでフォルダパスを<my_bucket1>/<dir1>と指定し、詳細プロパティでフォルダパスを<my_bucket2>/<dir2>と指定すると、Secure Agent はフォルダパス<my_bucket2>/<dir2>にファイルを書き込みます。
- 詳細モードのマッピングの詳細プロパティで、有効なオーバーライドフォルダパスを指定していることを確認してください。オーバーライドフォルダパスのパターンが実際のフォルダパスと一致しない場合、マッピングは失敗します。

第 6 章

Amazon S3 V2 コネクタへのアップグレード

Amazon S3 V1 接続を使用して Amazon S3 にアクセスしている場合は、新しい Amazon S3 V2 コネクタにアップグレードできます。Amazon S3 接続を使用する既存のマッピングおよびマッピングタスクのソースまたはターゲット接続タイプを Amazon S3 V2 接続に置き換えることができます。

接続タイプのアップグレード

既存のマッピングで接続を置き換えると、以前に選択したオブジェクトは保持されません。Amazon S3 オブジェクトを再インポートする必要があります。2 つのコネクタ間で共通のフィールドに設定されたソース、ターゲット、およびルックアップの詳細プロパティは、新しいコネクタに保持されます。また、古いコネクタからの設定済みのフィールドマッピングを保持するためのオプションもあります。

古いコネクタの設定済みの値を使用して、マッピングを正常に実行できます。さらに、拡張された Amazon S3 V2 コネクタが提供する機能を設定できます。

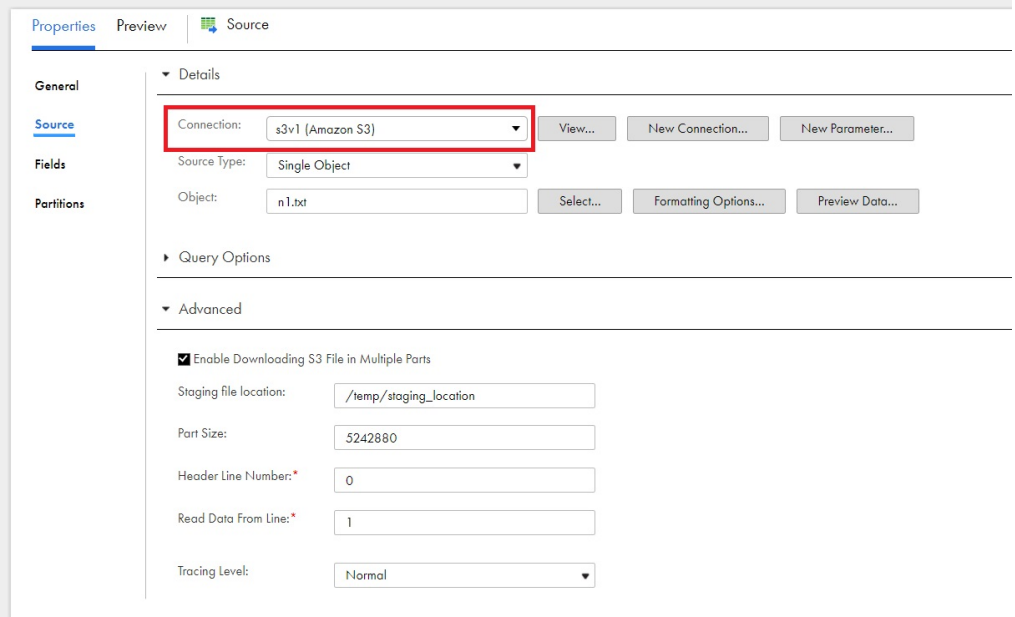
注: マッピングで Amazon S3 V1 接続を使用して Amazon S3 との間でデータの読み取りまたは書き込みを行う場合は、Amazon S3 V2 接続を使用して、拡張コネクタが提供する機能を利用することをお勧めします。Amazon S3 V2 コネクタのライセンスを取得するには、グローバルカスタマサポートにお問い合わせください。

接続切り替えの例

Amazon S3 V1 接続を使用する既存の Amazon S3 マッピングを Amazon S3 V2 接続にアップグレードする必要があるとします。

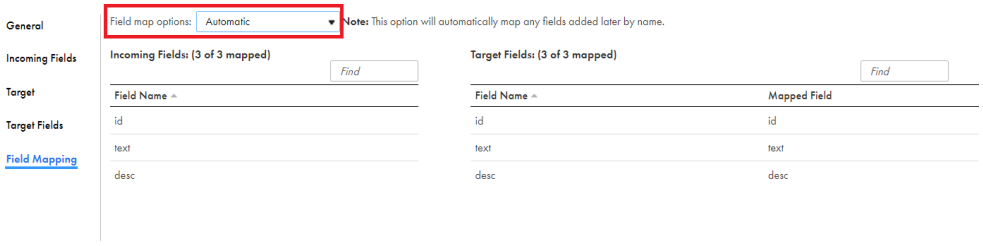
1. Amazon S3 V2 にアップグレードする既存の Amazon S3 V1 マッピングを開きます。

   次の図に、Amazon S3 V1 接続を使用する、ソーストランスフォーメーションで設定された詳細プロパティを含んだ既存のマッピングを示します。



2. 接続を切り替えたときにフィールドマッピングからのマッピングされたフィールドを保持するには、**[フィールドマッピング]** タブで、Amazon S3 V1 マッピングの次の **[フィールドマップオプション]** メニューから選択を行います。

   - 切り替え後に、自動的にマッピングされたフィールドを保持するには、**[自動]** を選択します。

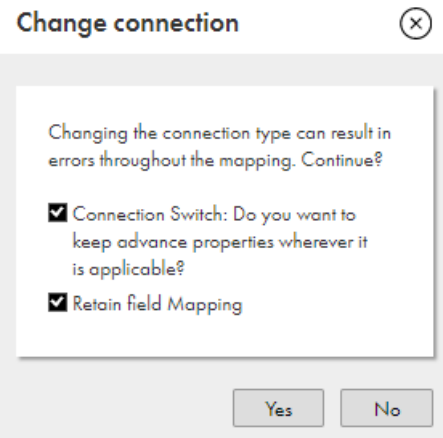


   - 切り替え後に、保持されたフィールドを手動でマッピングするには、**[手動]** を選択します。

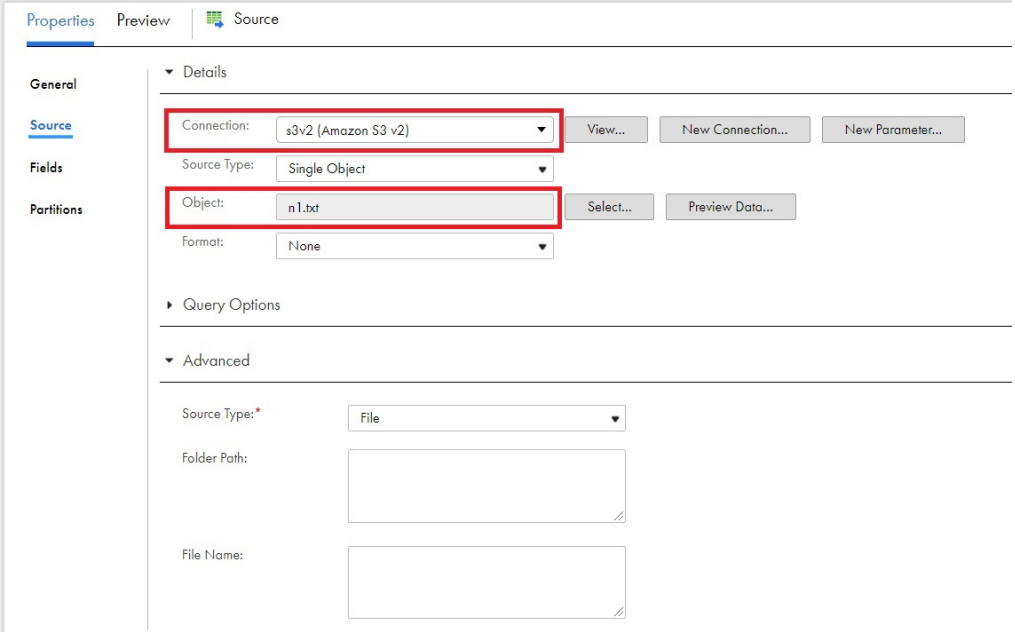
     注: 手動を選択した場合は、接続を切り替えた後に、保持されたフィールドを以前のマッピングを使用して自動的にマッピングするオプションがあります。

3. 接続を切り替えるには、**[接続]** フィールドで、接続を Amazon S3 V1 から Amazon S3 V2 に変更します。
4. **[接続の変更]** ダイアログボックスで次のプロパティを選択し、**[はい]** をクリックします。
   - **接続の切り替え**。選択した接続に切り替えます。
   - **フィールドマッピングの保持**。Amazon S3 V1 からの設定済みのフィールドマッピングを保持します。

次の図に、選択する必要のあるオプションを示します。

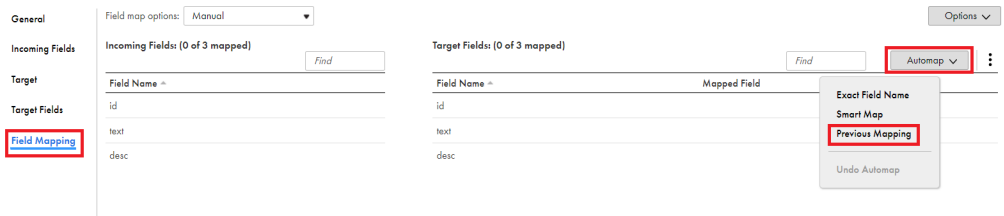


5. マッピングでは、Amazon S3 V1 と同じオブジェクトパスを使用します。次の図に、Amazon S3 V1 と同じオブジェクトパスを使用して切り替えた接続を示します。



Amazon S3 V1 マッピングから設定されたソースの詳細プロパティが、ソーストランスフォーメーションに反映されています。

6. Amazon S3 V1 マッピングの［**フィールドマッピング**］タブで［**手動**］を選択し、Amazon S3 V2 のフィールドマッピングを反映するには、［**フィールドマッピング**］タブで［**自動マップ**］を選択し、［**以前のマッピング**］を選択します。



注: Amazon S3 V1 で［**自動**］を選択した場合、このタスクを実行する必要はありません。

7. ［**保存**］をクリックします。

切り替え後に保持される詳細プロパティ

Amazon S3 接続を使用する既存のマッピングまたはマッピングタスクのソースまたはターゲット接続タイプを Amazon S3 V2 接続に置き換える場合に、設定済みの詳細プロパティを保持するためのオプションがあります。

次の表に、Amazon S3 V2 マッピングに保持される Amazon S3 V1 の設定済みのソース、ルックアップ、およびターゲットの詳細プロパティを示します。

プロパティ	Amazon S3 V2 **に保持される** Amazon S3 V1 **のプロパティ**
ソースとルックアップ	- パーツサイズ - ステージングディレクトリ
ターゲット	- パーツサイズ - 一時領域ディレクトリ - TransferManager スレッドプールサイズ - オブジェクトタグ - パーティションファイルのマージ - フォルダパス - 圧縮形式

第 7 章

データ型リファレンス

データ統合では、Amazon S3 を使用したマッピングおよびマッピングタスクで次のデータ型が使用されます。

Amazon S3 **のネイティブデータ型**

Amazon S3 のデータ型は、フィールドのメタデータを編集するときに、ソースおよびターゲットトランスフォーメーションの［フィールド］タブに表示されます。

トランスフォーメーションデータ型

トランスフォーメーションで表示されるデータ型のセットです。ANSI SQL-92 汎用データ型に基づく内部データ型で、プラットフォーム間でデータを移動するとき Secure Agent によって使用されます。トランスフォーメーションデータ型は、マッピング内のすべてのトランスフォーメーションに表示されます。

データ統合は、ソースデータを読み取るときに、ネイティブデータ型を対応するトランスフォーメーションデータ型に変換してから、データのトランスフォームを実行します。データ統合は、ターゲットに書き込むときに、トランスフォーメーションデータ型を対応するネイティブデータ型に変換します。

フラットファイルデータ型とトランスフォーメーションデータ型

次の表に、Secure Agent がサポートしている Amazon S3 データ型と、対応するトランスフォーメーションデータ型の一覧を示します。

Amazon S3 **のデータ型**	**トランスフォーメーションデータ型**	**説明**
NUMBER	Decimal	精度 1〜28 桁、スケール 0〜28 桁
STRING	String	1〜104,857,600 文字
NSTRING	Text	1〜104,857,600 文字

注: NUMBER データ型と NSTRING データ型は、**［スキーマファイルからインポートする］**オプションを使用してフラットファイルをインポートする場合にのみサポートされます。

Avro Amazon S3 ファイルデータ型とトランスフォーメーションデータ型

Avro Amazon S3 のファイルデータ型は、Secure Agent がプラットフォーム間でデータを移動するために使用するトランスフォーメーションデータ型にマップされます。

次の表に、Secure Agent がサポートしている Avro Amazon S3 ファイルのデータ型と、対応するトランスフォーメーションデータ型の一覧を示します。

Avro Amazon S3 **ファイルデータ型**	**トランスフォーメーションデータ型**	**範囲と内容**
配列	配列	文字数に制限はありません
Boolean	Integer	TRUE（1）または FALSE（0）
Date	日付/時刻	0001 年 1 月 1 日～9999 年 12 月 31 日。
Decimal	Decimal	マッピングの場合: 精度 18 桁および 28 桁。0 から 28 までのスケール。 18 桁または 28 桁未満の精度を指定した場合、18 桁または 28 桁が精度と見なされます。 詳細モードのマッピングの場合、精度は 18、28、および 38 桁となります。0 から 38 までのスケール。
Double	Double	精度 15
Float	Double	精度 15
Int	Integer	-2,147,483,648～2,147,483,647 精度 10、位取り 0
Long	Bigint	-9,223,372,036,854,775,808 to 9,223,372,036,854,775,807 精度 19、位取り 0
マップ	マップ	文字数に制限はありません
Null	Integer	-2,147,483,648～2,147,483,647 精度 10、位取り 0
Record	Struct	文字数に制限はありません

Avro Amazon S3 ファイルデータ型	トランスフォーメーションデータ型	範囲と内容
String	String	-1〜104,857,600 文字
Union	["primitive_type|complex_type", "null"]または["null", "primitive_type|complex_type"]の共有体で表される対応するデータ型。	プリミティブデータ型または複合データ型に依存します。

次の表に、Avro ファイル形式のタイムスタンプデータ型のサポート状況を示します。

タイムスタンプデータ型	マッピング	詳細モードのマッピング
Timestamp_micros	○	はい
Timestamp_millis	はい	いいえ
Time_millis	はい	いいえ
Time_micros	はい	いいえ

Avro データ型のルールとガイドライン

Avro Amazon S3 ファイルデータ型とトランスフォーメーションデータ型を使用する場合は、次のルールとガイドラインを考慮してください。

- マッピングを実行して Amazon S3 ターゲットにデータを書き込む場合、Avro データ型の固定された型を使用することはできません。
- ソースファイルで正しい精度とスケールを指定します。指定しない場合、ソースデータをターゲットに書き込む際に小数点の位置が変わります。
- ソースファイルには、1900-01-01T00:00:00Z 以降のタイムスタンプ値が必要です。ない場合、マッピングはエラーで失敗します。
- **［ターゲットの作成］**オプションを使用しており、アップストリームトランスフォーメーションで Avro データ型の精度を変更した場合、精度は適用されません。
  精度に関する問題を解決するには、デフォルトの精度でターゲットオブジェクトを作成してから、精度を編集します。

Date、Decimal、および Timestamp 型の有効化

Avro データ型に Date、Decimal、および Timestamp 型を使用するには、マッピングを実行する前に次の手順を実行します。

1. Administrator で、**［ランタイム環境］**タブにリストされている Secure Agent を選択します。
2. **［編集］**をクリックします。
3. **［システム構成の詳細］**セクションで、サービスとして **［データ統合サービス］**を選択します。
4. **INFA_DEBUG** プロパティを編集し、*-DEnableNewAvroDataTypes=true* と入力します。

   注: 複数のフラグを入力するには、フラグをスペースで区切ります。
5. **［保存］**をクリックします。
6. Secure Agent を再起動します。

Avro データ型に Date、Decimal、および Timestamp 型を使用するには、詳細モードのマッピングを実行する前に次の手順を実行します。

1. Administrator で、**［詳細クラスタ］**を選択します。
2. 既存の設定に移動するか、新しい設定を作成します。
3. **［詳細設定］**セクションで、**［カスタムプロティ］**に移動します。
4. *-DEnableNewAvroDataTypes=true* と入力します。
5. **［保存］**をクリックします。

JSON Amazon S3 ファイルデータ型とトランスフォーメーションデータ型

JSON Amazon S3 ファイルデータ型は、Secure Agent がプラットフォーム間でデータを移動するために使用するトランスフォーメーションデータ型にマッピングされます。JSON ファイルデータ型は、詳細モードのマッピングでのみ使用できます。

次の表に、Secure Agent がサポートしている JSON Amazon S3 ファイルデータ型と、対応するトランスフォーメーションデータ型の一覧を示します。

JSON Amazon S3 **ファイルデータ型**	**トランスフォーメーションデータ型**	**範囲と内容**
配列	配列	文字数に制限はありません
Double	Double	精度 15
Integer	Integer	-2,147,483,648～2,147,483,647 精度 10、位取り 0
Object	Struct	文字数に制限はありません
String	String	-1～104,857,600 文字

ORC Amazon S3 ファイルデータ型とトランスフォーメーションデータ型

ORC Amazon S3 ファイルデータ型は、Secure Agent がプラットフォーム間でデータを移動するために使用するトランスフォーメーションデータ型にマッピングされます。

次の表に、Secure Agent がサポートしている ORC Amazon S3 ファイルデータ型と、対応するトランスフォーメーションデータ型の一覧を示します。

ORC Amazon S3 ファイルデータ型	トランスフォーメーションデータ型	範囲と内容
BigInt	BigInt	-9223372036854775808～9,223,372,036,854,775,807
Boolean	Integer	TRUE（1）または FALSE（0）
Char	String	1～104,857,600 文字
Date	Date/Time	西暦 1753 年 1 月 1 日～西暦 4712 年 12 月 31 日 （精度はマイクロ秒まで）
Double	ダブル	精度 15 桁
Float	ダブル	精度 15 桁
Integer	Integer	-2,147,483,648～2,147,483,647
SmallInt	Integer	-32,768～32,767
String	String	1～104,857,600 文字
タイムスタンプ	Date/Time	1～19 文字 精度 19～26、位取り 0～6
TinyInt	Integer	-128～127
Varchar	String	1～104,857,600 文字

Parquet Amazon S3 のファイルデータ型とトランスフォーメーションデータ型

Parquet Amazon S3 のファイルデータ型は、Secure Agent がプラットフォーム間でデータを移動するために使用するトランスフォーメーションデータ型にマップされます。

次の表に、Secure Agent がサポートしている Parquet Amazon S3 ファイルのデータ型と、対応するトランスフォーメーションデータ型の一覧を示します。

Parquet Amazon S3 **ファイルデータ型**	**トランスフォーメーションデータ型**	**範囲と内容**
Boolean	Integer	TRUE（1）または FALSE（0）
Date	日付/時刻	0001 年 1 月 1 日 - 9999 年 12 月 31 日
Decimal	Decimal	マッピングの場合: 精度 18 桁および 28 桁。0 から 28 までのスケール。 18 桁または 28 桁未満の精度を指定した場合、18 桁または 28 桁が精度と見なされます。 詳細モードのマッピングの場合、精度は 18、28、および 38 桁となります。0 から 38 までのスケール。
Double	Double	精度 15
Float	Double	精度 15
Int32	Integer	-2,147,483,648～+2,147,483,647
Int64	Bigint	-9,223,372,036,854,775,808～+9,223,372,036,854,775,807 8 バイト符号付き整数
Int96	Binary	12 バイト符号付き整数
マップ	マップ	文字数に制限はありません。
Struct	Struct	文字数に制限はありません。
String	String	-1～104,857,600 文字
Time	Date/Time	1 日のうちの時間。精度はマイクロ秒まで。

Parquet Amazon S3 ファイルデータ型	トランスフォーメーションデータ型	範囲と内容
タイムスタンプ	Date/Time	0001 年 1 月 1 日 00:00:00 - 9999 年 12 月 31 日、23:59:59.997997。精度はマイクロ秒まで。
group(LIST)	Array	文字数に制限はありません。

注: ソースファイルで正しい精度とスケールを指定します。指定しない場合、ソースデータをターゲットに書き込む際に小数点の位置が変わります。

Parquet ファイルの読み取りまたは書き込みを行うために指定する Parquet スキーマは小文字である必要があります。Parquet は大文字と小文字を区別するスキーマではありません。

Parquet の Timestamp データ型のサポート

次の表に、Parquet ファイル形式のタイムスタンプデータ型のサポート状況を示します。

タイムスタンプデータ型	マッピング	詳細モードのマッピング
Timestamp_micros	はい	いいえ
Timestamp_millis	はい	いいえ
Time_millis	はい	いいえ
Time_micros	はい	いいえ
int96	○	はい
Date	○	はい

Secure Agent でサポートされていない Parquet のデータ型は以下のとおりです。

- Timestamp_nanos
- Time_nanos
- Timestamp_tz

第 8 章

トラブルシューティング

Amazon S3 V2 コネクタでのエラーのトラブルシューティングには、以下のセクションを使用します。

Amazon S3 V2 コネクタのトラブルシューティング

Java ヒープサイズの設定

このセクションでは、Secure Agent の JVM オプションが多数のファイルを読み取るように設定されていない場合に発生する可能性があるエラーについて説明します。

マッピングタスクを実行して多数のレコードを書き込むと、「ERROR java.lang.OutOfMemoryError: GC overhead limit exceeded.**（エラー** java.lang.OutOfMemoryError: GC **オーバーヘッド制限を超過しました。）」というエラーが発生します。**

この問題を解決するには、以下のタスクを実行して Secure Agent の JVM オプションを設定し、Java ヒープサイズのメモリを増やします。

1. **［Administrator］** > **［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、利用可能な Secure Agent のリストからメモリを増加する Secure Agent を選択します。
3. 右上隅の**［編集］**をクリックします。
4. **［システム構成の詳細］**セクションで、データ統合サーバーの**［タイプ］**に**［DTM］**を選択します。
5. **［JVMOption1］**を**［-Xms2048m］**に編集します。

   注: 処理するデータに基づいて最大ヒープサイズと最小ヒープサイズを指定します。
6. Secure Agent を手動で再起動します。

サイズが 1.4 GB **以上のファイルを書き込むマッピングを実行して、暗号化タイプに**［Informatica Encryption］**を選択している場合、「**[ERROR] java.lang.OutOfMemoryError: Java heap space**（**[**エラー**] java.lang.OutOfMemoryError: Java **ヒープ領域）」が発生します。**

この問題を解決するには、以下のタスクを実行して Secure Agent の JVM オプションを設定し、Java ヒープサイズのメモリを増やします。

1. **［Administrator］** > **［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、利用可能な Secure Agent のリストからメモリを増加する Secure Agent を選択します。
3. 右上隅の**［編集］**をクリックします。
4. **［システム構成の詳細］**セクションで、データ統合サーバーの**［タイプ］**に**［DTM］**を選択します。

5. ［**JVMOption1**］を［**-Xmx8046m**］に編集します。
6. Secure Agent を手動で再起動します。

FFParserRetainNullString カスタムプロパティ

NULL という名前の文字列を含む csv ファイルから読み取る場合、タスクはターゲットにデータを書き込みません。この問題を解決するには、次のタスクを実行し、カスタムプロパティ FFParserRetainNullString を設定します。

1. ［**Administrator**］ > ［**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 を選択します。
3. 右上隅の［**編集**］をクリックします。
4. ［**カスタム構成の詳細**］セクションで、データ統合サーバーの［**タイプ**］に［**Tomcat JRE**］を選択します。
5. ［**名前**］を［**FFParserRetainNullString**］と入力し、［**値**］を［**true**］と入力します。
6. ［**保存**］をクリックします。

RedirectToSessionLog カスタムプロパティ

ソースまたはターゲットの Amazon S3 V2 ファイルを選択し、Parquet ファイル形式オプションを設定すると、多数のログファイルが生成される場合があります。この問題を解決してログを無効にするには、次のタスクを実行し、カスタムプロパティ RedirectToSessionLog を設定します。

1. ［**Administrator**］ > ［**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 を選択します。
3. 右上隅の［**編集**］をクリックします。
4. ［**カスタム構成の詳細**］セクションで、データ統合サーバーの［**タイプ**］に［**DTM**］を選択します。
5. ［**名前**］を［**RedirectToSessionLog**］と入力し、［**値**］を［**なし**］と入力します。
6. ［**保存**］をクリックします。

JSON ファイルの空の構造データ

JSON ファイルに空の構造データを含むフィールドがある場合、Secure Agent はそのフィールドを無視し、メタデータの読み取り中に残りのフィールドを読み取ります。

例えば、JSON ファイルの最初の行にデータ{"id":123,"address":{}}がある場合、address フィールドは無視され、［**フィールド**］タブには表示されません。JSON ファイルで連続する行の address フィールドに値がある場合、［**サンプリングするデータ要素**］プロパティを使用してこのフィールドを取得できます。

Amazon S3 バケットが存在しないか、ユーザーにバケットにアクセスする権限がありません。

Secure Agent をホストするマシンの時刻を変更しないでください。Secure Agent の時刻は、タイムゾーンに従って正確である必要があります。正確でない場合、マッピングは例外で失敗します。

トラブルシューティング FAQ

Informatica Cloud Data Integration Amazon S3 V2 **コネクタの** FAQ（**よくある質問**）

Amazon S3 V2 コネクタの FAQ（よくある質問）については、https://docs.informatica.com/integration-cloud/cloud-data-integration-connectors/h2l/1207-frequently-asked-questions-for-amazon-s3-v2-connector/abstract.html を参照してください。。

Amazon S3 V2 **コネクタの** AWS IAM **認証はどのように設定しますか**?

AWS IAM 認証の設定の詳細については、https://docs.informatica.com/integration-cloud/cloud-data-integration-connectors/h2l/1199-configuring-iam-authentication-for-amazon-s3-and-amazon-s3-/abstract.html を参照してください。。

マッピングのターゲットプロパティで［ターゲットの作成］オプションを使用して形式オプションを設定しない場合に発生する次のエラーを解決する方法:「com.informatica.powercenter.sdk.SDKException:Error during binary data write: java.lang.String cannot be cast to [B」

この問題の詳細については、https://kb.informatica.com/solution/23/Pages/69/568954.aspx?myk=568954 を参照してください。

Amazon S3 V2 **コネクタを使用して** JSON **ファイルを読み取るにはどうすればよいですか。**

Amazon S3 V2 コネクタを使用して JSON ファイルを読み取る方法については、https://docs.informatica.com/integration-cloud/cloud-data-integration-connectors/h2l/1271-reading-a-json-file-using-an-amazon-s3-v2-connector/abstract.html を参照してください。。

詳細モードのマッピングを実行して、複数レベルの JSON **ファイルを読み書きできますか**?

はい。詳細モードのマッピングからの複数レベル JSON ファイルの読み取りまたは書き込みの詳細については、https://kb.informatica.com/faq/7/Pages/23/574694.aspx?myk=574694 を参照してください。

索引

A

Amazon S3
　ターゲットの指定 58
Amazon S3 V2
　複数ファイルの処理 29
　サポートされているアセット 8
　ソース 26
　ソーストランスフォーメーション 47
　ターゲット 34
　ディレクトリソース 28
　マッピングでのソース 47
　ルックアップ 54
　形式オプション 54
　接続プロパティ 17
Amazon S3 V2 コネクタ
　概要 8
　管理 9, 10
Amazon S3 V2 ソース
　クライアントサイド暗号化 27
Amazon S3 V2 ターゲット
　マッピング 50
Amazon S3 V2 接続
　概要 17
Amazon S3 コネクタ
　概要 9
Amazon S3 とトランスフォーメーション
　データ型 72

C

Cloud Application Integration コミュニティ
　URL 6
Cloud 開発者コミュニティ
　URL 6

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

J

Java ヒープサイズ
　設定 79
JSON Amazon S3 ファイルデータ型
　トランスフォーメーションデータ型 75

L

Linux
　プロキシの設定 24

O

ORC ファイルのデータ型
　トランスフォーメーションデータ型 76

W

Web サイト 6
Windows
　プロキシの設定 23

あ

アップグレード通知 7

お

オブジェクトタグ
　ルールおよびガイドライン 43

し

システムステータス 7

す

ステータス
　Informatica Intelligent Cloud Services 7

そ

ソース
　ファイル名フィールド 33
　マッピングでの Amazon S3 V2 47
ソーストランスフォーメーション
　Amazon S3 V2 のプロパティ 47

た

ターゲット
　ファイル名フィールド 41
ターゲットの作成
　ターゲットファイルのパラメータ化 60

ターゲットの作成 *(続く)*
タイムスタンプの追加 60

て

データ圧縮
ソースとターゲット 43
データ暗号化
Informatica Encryption 28
ソース 27
ターゲット 34
データ型リファレンス
概要 72

と

トラブルシューティング
Amazon S3 V2 コネクタ 80

は

パーティション化
Amazon S3 V2 ソース 33
Amazon S3 V2 ターゲット 36
パラメータファイルを使用したパラメータ化 60

ふ

ファイルの増分ロード
概要 31
プロキシ設定
JVMOption 23
Linux での設定 24
Windows での設定 23

ま

マッピング
Amazon S3 V2 ソースのプロパティ 47
マッピングの作成
ルールとガイドライン 61

め

メンテナンスの停止 7

る

ルールおよびガイドライン
形式オプションの設定 57

わ

ワイルドカード文字
概要 31