ユーザーガイド

AWS データ転送ターミナル

AWS データ転送ターミナル: ユーザーガイド

Table of Contents

データ転送ターミナルとは

AWS データ転送ターミナルは、データストレージデバイスを持ち込み、AWS クラウドサービスとの間で高速データ転送を行うことができるネットワーク対応の物理拠点です。遠隔地で取得したデータをアップロードすることで、より簡単にアクセスできるようにします。

AWS マネジメントコンソールからいずれかの物理的なデータ転送ターミナル施設の予約を行い、予定の時刻に施設を訪れて、ユーザー自身のデバイスを使用してデータを AWS クラウドサービスにアップロードします。スケジュールした予約が完了し、退出したあとは、施設は再びセキュリティが確保され、次のスケジュールされた予約に向けて準備が整えられます。

> **Note**
>
> AWS データ転送ターミナルは、現時点では AWS エンタープライズのお客様のみが利用できます。

データ転送ターミナルにアクセスするには:

- AWS データ転送ターミナルコンソール: https://console.aws.amazon.com/datatransferterminal
- データ転送ターミナル施設: コンソールで予約が行われると、データ転送ターミナル施設の場所が提供されます。データ転送の詳細については、「データ転送を行う」を参照してください。

機能

AWSデータ転送ターミナルを使用すると、リモートロケーションから AWS クラウドサービスにデータを簡単に取り込むことができます。リモートデータアップロードのニーズに対するデータ転送ターミナルの利点の一部を次に示します。

安全、プライベート、そして排他的

各データ転送ターミナル施設は、高速ネットワーク接続を介してデータストレージデバイスと AWS サービス間で大規模なデータ転送を行うための安全かつプライベートな場所です。

専用予約コンソール

承認された担当者を転送チームに追加し、AWS データ転送ターミナルコンソールを使用してデータ転送ターミナル予約をスケジュールします。

光ファイバーネットワーク接続

各データ転送ターミナル施設には、高速データアップロードと冗長性を確保するために 2 つの 100 ギガビット (Gbps) 光ファイバー (LR4) 接続が備わっています。

データストレージデバイスの制御

Snowball デバイスを出荷し、データが AWS クラウドサービスにアップロードされるのを待つ必要はありません。データ転送プロセス全体を通じて物理データストレージデバイスを制御し、データを必要な場所により速く移動できます。

主要なコンセプト

AWS データ転送ターミナルを使用するには、プロセス所有者がデータ転送ターミナル施設にアクセスするためのデータ転送スペシャリストの予約をスケジュールする必要があります。データ転送ターミナルの用語の詳細については、以下のセクションを参照してください。

トピック

転送チーム

転送チームとは、AWS アカウント所有者によって決められた担当者のグループであり、組織に代わってデータ転送を行う担当者を選択できます。転送チームの設定には、転送チームに名前を付け、チームの担当者を指定することが含まれます。1 回の予約には、4 人以下のデータ転送スペシャリストのグループをお勧めします。

詳細については、「データ転送ターミナルの予約をスケジュールする」を参照してください。

担当者

担当者とは、予約を作成および管理できる個人、またはデータ転送ターミナル施設に移動して使用できる個人を指します。担当者は、プロセス所有者、データ転送スペシャリスト、またはその両方の場合があります。

プロセス所有者

- プロセス所有者は、AWS アカウント所有者で、AWS データ転送ターミナルアカウントから担当者を追加、編集、削除できます。

データ転送スペシャリスト

- データ転送スペシャリストは、データ転送ターミナル施設でデータアップロードトランザクションを行うことができる個人です。これらの担当者は、プロセス所有者によって承認され、AWS データ転送ターミナルアカウントに追加されている必要があります。データ転送ターミナル施設にアクセスする場合、政府発行の ID が必要です。

施設

データ転送ターミナル施設とは、1 つ以上のサービスプロバイダーが共同所有および管理するデータハブです。各施設では、データ転送ターミナルのデータ転送スペシャリストは、データ転送ターミナルスイートにアクセスするために、予約レコードと一致する政府発行の身分証明書を提供する必要があります。

スケジューリングに関する考慮事項

データ転送ターミナルコンソールでは、1~6 時間までの予約を、1 週間のどの曜日でも 1 年を通じて行うことができます。個々の予約は連続してスケジュールでき、予約の間隔は最低 1 時間です。すべての予約は、少なくとも 24 時間前に行う必要があります。

データ転送に必要な時間は、アップロードのパフォーマンス速度によって異なります。データ転送ターミナルの予約を計画およびスケジュールする際は、アップロードのパフォーマンスに影響する以下の要因を考慮してください。

機器

- 一部の機器には、アップロードのパフォーマンスに影響を与える可能性のある設定が含まれている場合があります。推奨されるアップロードのパフォーマンス速度については、機器の仕様を参照してください。

ネットワーク条件

- ネットワークトラフィックが多い時間はデータのアップロード速度に影響するため、データ転送セッションの時間を選択する際は考慮する必要があります。オフピーク時間またはネットワークアクティビティが少ない時間帯にデータ転送セッションを計画することで、アップロード速度が向上する場合があります。

データ転送サイズ

- データ転送ターミナルのネットワーク接続は、大規模なデータ転送用に設計されています。ただし、転送されるデータのサイズは、セッションにかかる時間に影響します。

ユースケース

AWS エンタープライズのお客様は誰でも データ転送ターミナルシステムにアクセスできますが、特定のユースケースシナリオでは、より大きなメリットが得られる場合があります。

Autonomous Driving and Advanced Driver Assistant Systems (AD/ADAS): Automotive Original Equipment Manufacturers (OEM) とサプライヤは、北米、欧州、および ASEAN 内の多数の大都市圏でデータを運用および収集している自律型車両のフリートから大規模なデータセットを生成します。データ転送ターミナルでは、これらのフリート車両によって収集されたデータを AWS クラウドサービスにアップロードし、AD/ADAS モデルのトレーニングに使用できます。

メディアとエンターテインメント: スタジオやその他のコンテンツクリエーターは、遠隔地でデジタルの映像・音声 (AV) ファイルを生成することがよくあります。これらの AV ファイルは、地理的に分散した制作チームと編集チームが並行してリアルタイムでワークフローを開始できるように、適時にクラウドにアップロードすることが重要です。データ転送ターミナルを使用してリモートでデータをアップロードすることで、製作タイムラインを短縮し、製作コストを削減できます。

地図作成、写真測量、3D 画像: マッピングや画像アプリケーションを扱う組織は、遠隔地でデータを収集し、分析またはトレーニングのためにそれらのビジュアルファイルを AWS クラウドにアップロードする必要があります。データ転送ターミナルは、これらの大規模なデータセットを収集および分析する時間を最小限に抑え、ドライバーや農業従事者、この情報のその他の利用者のために地理空間データを最新の状態に保つのに役立ちます。

関連サービス

以下の AWS サービスは、データ転送ターミナルの使用時に最適なエクスペリエンスを提供します。

AWS のサービス	説明
AWS Snowball Edge	AWS データ転送ターミナルは、AWS クラウドへの高速アップロードのための場所を提供し、データへのアクセスの待機時間を最小限に抑えることで、Snowball 製品を補完します。

AWS のサービス	説明
Amazon S3 ()	独自のデバイスをデータ転送ターミナルに持ち込み、Amazon S3 サービスにデータを迅速かつ安全にアップロードします。

データ転送ターミナルを使用するための技術要件

データ転送ターミナルで予約をスケジュールする前に、ネットワークに接続するために必要な機器と設定があることを確認する必要があります。最適なネットワーク接続とエクスペリエンスについては、次のガイドラインを参照してください。

機器

モニター、キーボード、マウス、コンピュータ、ラップトップなどの接続用のポータブルデバイスを、スケジュールされた予約のためにデータ転送ターミナル施設に持ち込む必要があります。

お使いのハードウェアは光ファイバー (L4) 接続に対応している必要があります

> **Note**
>
> データセキュリティのベストプラクティスとして、データ転送ターミナルに持ち込むストレージデバイスでデータが暗号化および保護されていること、およびデータ転送ターミナル施設の使用中にデータ暗号化ポリシーを適用していることを確認します。詳細については、「AWS データ転送ターミナルのセキュリティ」を参照してください。

ネットワークの要件

アップロードするデバイス、サーバー、またはアプライアンス (ラップトップ) がネットワークに接続できるよう準備し、DHCP がサポートされていることを確認します。最適なデータアップロードを行えるようにするには、以下が必要です。

- データ転送ターミナル施設で提供されるファイバーケーブル接続用の NIC および LC コネクタと互換性のある 100G QSFP28 LR4 (100GBASE-LR4) 光 QSFP トランシーバー。
- IP アドレスの自動設定 DHCP は有効になっています。DNS サーバーは DHCP によって自動的に割り当てられます。
- 最新のソフトウェアおよび NIC ドライバー。

パフォーマンスの最適化

AWS データ転送ターミナルの使用中にスループットを最大化するには、次の推奨事項を考慮してください。

- 推奨ハードウェア:
  - 100 Gbps のネットワークインターフェイスカード
  - 16 コア CPU
  - 128 GB RAM
  - 複数の NVMe SSD ドライブを RAID アレイに構成したもの
- AWS コマンドラインインターフェイスまたは AWS SDK を使用したアップロードには、AWS 共通ランタイム (AWS CRT) ライブラリを使用します。

  以下のパラメータを設定して Amazon S3 転送設定を最適化します。これらの値は、AWS 設定ファイルの最上位 `s3` キー、デフォルトロケーション `~/.aws/config` で設定します。

```
[default]
s3 =
    preferred_transfer_client = crt
    target_bandwidth = 100Gb/s
    max_concurrent_requests = 20
    multipart_chunksize = 16MB
```

  すべての Amazon S3 設定値は、最上位 `s3` キーの下にインデントおよびネストされていることに注意してください。

  - オプション: `aws configure set` コマンドを使用して、上記の値をプログラムで設定できます。例えば、デフォルトプロファイルに上記の値を設定するには、代わりに次のコマンドを実行できます。

```
aws configure set default.s3.preferred_transfer_client crt
aws configure set default.s3.target_bandwidth 100Gb/s
aws configure set default.s3.max_concurrent_requests 20
aws configure set default.s3.multipart_chunksize 16MB
```

- デフォルト以外のプロファイルにこれらの値をプログラムで設定するには、`--profile` フラグを指定します。例えば、`test-profile` という名前のプロファイルの設定を設定するには、以下の例のようなコマンドを実行します。

```
aws configure set s3.max_concurrent_requests 20 --profile test-profile
```

- デバイスで BBR (Linux) を有効にすると、スループットが向上します。

```
sysctl -w net.core.default_qdisc=fq
```

```
sysctl -w net.ipv4.tcp_congestion_control=bbr
```

詳細情報

ネットワーク接続とパフォーマンスを最適化するための AWS コマンドライン Amazon S3 設定の詳細については、次のリソースを参照してください。

- AWS CLI コマンドリファレンスのAWS CLI Amazon S3 設定
- パフォーマンスの高い Amazon S3 クライアントを使用する: Amazon S3 Amazon AppStream SDK for Java の AWS CRT ベースのクライアント
- AWSナレッジセンターの「AWS を使用して大きなファイルを Amazon S3 にアップロードするときにパフォーマンスを最適化する方法を教えてください。」

開始方法

データ転送ターミナル施設の 1 つを予約して、AWS クラウドサービスへのリモートデータ転送を開始します。まず、データ転送ターミナル施設と AWS エンタープライズアカウントでサポートされている機器が必要です。

データ転送ターミナルの予約をスケジュールする前に、このガイドの「データ転送ターミナルを使用するための技術要件」セクションを確認して、データ転送に最適な設定が適用された機器があることを確認してください。すべてのデータストレージデバイスとネットワーク接続機器が、スイートで利用可能な光ファイバーネットワーク接続と互換性があるわけではありません。

AWS にサインアップすると、データ転送ターミナルを含む AWS のすべてのサービスに対して AWS アカウントが自動的にサインアップされます。請求されるのは、使用したサービスの料金のみです。

データ転送ターミナルを設定するには、以下のセクションの手順を使用します。

AWS にサインアップしてデータ転送ターミナルをセットアップする際に、オプションで AWS マネジメントコンソールの表示言語を変更できます。詳細については、「AWS マネジメントコンソール入門ガイド」の「AWS マネジメントコンソールの言語の変更」を参照してください。

AWS アカウントを入手したら、データ転送ターミナルにアクセスできます。AWS データ転送ターミナルのセットアップと使用の詳細については、「データ転送ターミナルの予約をスケジュールする」を参照してください。

AWS アカウントへのサインアップ

AWS の使用を開始するには、AWS アカウントが必要です。AWS アカウントの作成については、「AWS アカウント管理リファレンスガイド」の「AWS アカウントの始め方」を参照してください。

データ転送ターミナルの予約をスケジュールする

AWS データ転送ターミナルの使用を開始するには、AWS アカウントを作成し、https://console.aws.amazon.com/datatransferterminal のデータ転送ターミナルコンソールにログインする必要があります。データ転送ターミナルコンソールにログインすると、既存の予約を表示したり、新しい予約を作成したりできます。予約をスケジュールするには、以下を実行する必要があります。

1. 転送チームを作成します。予約を作成し、データ転送ターミナル施設にアクセスしてデータ転送を行うには、指定されたユーザーのグループを作成する必要があります。このトピックの詳細については、「転送チームを作成する」を参照してください。
2. チームがセットアップされたら、チームに担当者を追加する必要があります。転送チームへの担当者の追加の詳細については、「担当者を追加する」を参照してください。
3. プロセス所有者は、アカウントのチームとのデータ転送をスケジュールできます。予約のスケジュール方法の詳細については、「予約の詳細を指定する」を参照してください。
4. リクエストを送信する前に、予約の詳細が正しいことを確認してください。送信後、少なくとも 24 時間は予約リクエストを変更できません。詳細については、「予約を確認して確定する」を参照してください。

予約が処理および確認されると、転送チームはスケジュールされた時刻にデータ転送ターミナル施設にアクセスできます。詳細については、「データ転送ターミナル施設でデータ転送を行う」を参照してください。

転送チームを作成する

データ転送ターミナル施設にアクセスするには、AWS マネジメントコンソールで予約をスケジュールする必要があります。AWS アカウントにログインしてデータ転送ターミナルコンソールにアクセスし、次の手順を実行して予約をスケジュールします。

1. データ転送ターミナルのホームページから、[今すぐ始める] ボタンを選択します。
2. アカウントに転送チームがまだ設定されていない場合、[予約の作成] ボタンは無効になります。開始するには、転送チームを作成して名前を付ける必要があります。
   a. [転送チームの作成] ボタンを選択します。
   b. チームに名前を付けます。
      - 名前は 2 文字以上 64 文字以下で、文字または数字で始まる必要があります。
      - 文字、数字、ピリオド、ダッシュのみを使用してください。特殊文字は認識されません。

- 機密の識別情報を含めないでください。

c. 転送チームの説明を作成します。

- 特定の期間、キャンペーン、またはプロジェクトに対するチームの目的を説明するなど、チームを識別するのに役立つ説明を入力します。

d. [転送チームの作成] ボタンを選択します。

転送チームページに戻ると、新しく作成したチームが「転送チーム」セクションの下に表示されます。

データ転送ターミナルアカウントの転送チームの更新

新しい Transfer チームを設定するには、このガイドの「データ転送ターミナルの予約をスケジュールする」セクションを参照してください。

転送チームを変更または削除するには、以下を実行します。

1. 「転送チーム」ページで、変更する転送チームを選択します。
2. 転送チームの名前と説明を変更するには、[編集] ボタンを選択します。
3. 担当者を追加または削除するには、[担当者] タブを選択し、このよくある質問の「アカウントから担当者を変更、追加、または削除する方法」セクションで説明されているステップを完了します。
4. 選択した転送チームの予約を追加またはキャンセルするには、このよくある質問の「データ転送ターミナルアカウントの担当者の更新」セクションを参照してください。

担当者を追加する

プロセス所有者とデータ転送スペシャリストを転送チームに追加して、データ転送を設定し、データ転送ターミナル施設にアクセスします。転送チームに担当者を追加するには、以下を実行します。

1. 「転送チーム」ページで、「転送チーム」セクションに記載されているものから目的の転送チームカードを選択します。転送チームの概要ページが表示されます。
2. [担当者] タブを選択し、[担当者を登録する] ボタンを使用して、転送チームに担当者を追加します。
3. 「担当者の登録」ページで、転送チームに追加する人に関する必要な情報をフィールドに入力します。

a. 担当者エイリアス: 個人を識別するための一意のエイリアスを作成します。

- エイリアスは、個人のアイデンティティを保護しながら担当者を識別するために使用されます。
- 最大 64 文字で、文字、数字、ダッシュを含めることができます。
- 特殊文字は使用できません。

b. 名: 政府発行の身分証明書に記載されている人物の名を入力します。

c. 姓: 政府発行の身分証明書に記載されている人物の姓を入力します。

d. E メールアドレス: 予約情報とデータ転送ターミナル施設へのアクセス手順を受け取るため、有効な E メールアドレスを記入します。

4. [担当者の登録] ボタンを選択して、転送チームへの人物の追加を完了します。

データ転送ターミナルアカウントの担当者の更新

データ転送ターミナルコンソールでアカウントの既存の担当者を変更することは、現在サポートされていません。 AWSデータ転送ターミナルプロセスの所有者は、現時点では担当者を追加または削除することしかできません。

データ転送ターミナルアカウントから担当者を削除するには、次の手順を実行します。

1. 「転送チーム」ページで、削除する担当者に関連付けられた転送チームを選択します。
2. 選択した転送チームの概要ページで、[担当者] タブを選択します。
3. 削除するエイリアスの横にあるラジオボタンをクリックします。プロファイルを削除するときにのみ、ユーザーのエイリアスを表示できます。
4. [削除] ボタンを選択します。選択した担当者に対し、この操作が意図されたものであることを確認する警告が表示されます。[削除] ボタンをクリックして続行します。コンソールの上部に、担当者が正常に削除されたことを確認するバナーが表示されます。

予約の詳細を指定する

次の手順では、AWS マネジメントコンソールでデータ転送ターミナルの予約をスケジュールする方法について説明します。データ転送ターミナル施設の使用については、「データ転送を行う」を参照してください。

1. [今後の予約] タブの [予約の作成] ボタンを選択します。

2. 「予約の詳細を指定」ページのフィールドに入力します。

   a. 転送チームの選択: デフォルトとして選択された転送チームが最初に表示されます。別のチームを選択する場合は、ドロップダウン矢印をクリックして、利用可能な転送チームのリストから選択します。

   b. プロセス所有者: 予約の管理を担当する担当者エイリアスを選択します。

      - 予約に使用できるプロセス所有者は 1 人のみで、AWS アカウントで承認された担当者である必要があります。

        プロセス所有者は、データ転送アクティビティを実行するデータ転送スペシャリストの 1 人として含めることができます。

   c. データ転送スペシャリスト: データ転送ターミナル施設へのアクセスを許可する担当者を選択して、データ転送アクティビティを完了します。必要に応じて、複数の担当者を選択できます。

      - ベストプラクティスは、転送チームを 4 人以下のデータ転送スペシャリストに制限することです。

   d. データ転送ターミナル情報: データ転送セッションについて、データ転送ターミナル施設、希望する日付、詳細な時刻を指定します。

      i. データ転送ターミナル施設: ドロップダウン矢印をクリックして、データ転送ターミナル施設を選択します。

      > **Note**
      >
      > 予約時に提供されるのは施設の説明のみです。追加の位置情報は、予約確認メールに記載されます。

      ii. データ転送ターミナルの日時: [予約の日付と時刻を検索] フィールドをクリックしてカレンダーを表示し、予約をスケジュールします。

      - 予約は最低でも 24 時間前までに行う必要があり、また 6 か月を超える先の予約はできません。予約時間は最大 6 時間です。必要に応じて、夜間作業の場合を考慮し、1 つの予約が複数日にまたがることも可能です。
      - 時間は 24 時間制で表示され、1 時間単位でのみ予約できます。
      - 連続して予約するには、各データ転送セッションの間に少なくとも 1 時間の間隔を空けて個別の予約を作成する必要があります。
      - 詳細については、「スケジューリングに関する考慮事項」を参照してください。

3. 予約の詳細が正しいことを確認し、[作成] ボタンを選択して続行します。これにより確認ページに移動し、予約の概要が表示されます。

予約を確認して確定する

予約の詳細を指定したら、[次へ] ボタンを選択して、引き続き概要ページを表示します。「確認と作成」ページで、データ転送ターミナルの予約リクエストの詳細を確認します。

- リクエストに問題がなければ、[作成] ボタンを選択します。
- 予約を変更する必要がある場合は、[戻る] ボタンを選択します。

予約リクエストが送信されると、プロセス所有者はリクエストが受信され、処理中であることを確認する E メールを受信します。リクエストが承認されると、別の E メールで予約確認と、データ転送ターミナル施設の検索およびアクセスに関する手順が送られます。データ転送ターミナル施設のアクセスについては、「データ転送を行う」を参照してください。

予約の変更

データ転送ターミナルの予約リクエストに変更を加えるには、24 時間の処理期間が必要です。

処理期間の後、予約を表示、編集、または削除するには、コンソールの転送チームページに移動します。

1. チームのカードで目的の予約を見つけて選択します。
2. [アクション] メニューをクリックし、目的のアクションを選択します。
   - 表示: 表示オプションを選択すると、日付、時刻、場所、割り当てられた担当者など、予約の詳細を表示できます。
   - 編集: 日付、時刻、場所、割り当てられた担当者など、予約の詳細を変更できます。変更は、希望する予約日の 24 時間前までに行う必要があります。改訂は即時に承認および適用されるわけではないことにご注意ください。プロセス所有者は、更新されたリクエストの確認を受け取ります。
   - 削除: 削除オプションを使用すると、予約をキャンセルできます。キャンセルリクエストは、予約予定日の 24 時間前までに行う必要があります。リクエストが承認されると、プロセス所有者はキャンセルされた予約の確認を受け取ります。

データ転送ターミナル施設でデータ転送を行う

データ転送ターミナルは、AWS ネットワークへの安全なアクセスを提供する安全な共同所有の場所です。データ転送ターミナル施設にアクセスするには、場所の説明とアクセス手順が記載された確認メールを受信していることを確認してください。データ転送ターミナル施設へのアクセスと使用の詳細については、以下のトピックを参照してください。

トピック

持ち込むもの

データ転送スペシャリストは、ラップトップコンピュータ、フラッシュドライブ、ソリッドステートドライブ (SSD)、AWS Snowball Edge など、データ転送の実行に必要なアイテムを持ち込む必要があります。データ転送ターミナル施設のファイバーネットワークケーブルを使用するように機器が最適化されていることを確認してください。最適な機器と設定の詳細については、「データ転送ターミナルを使用するための技術要件」を参照してください。

お客様は、お客様および付随するデータ転送スペシャリストがデータ転送ターミナル施設に持ち込む機器やアイテムのインストール、使用、および削除について責任を負います。作業室に持ち込まれたものは、退出時にすべて持ち出す必要があります。 AWSデータ転送ターミナルは、忘れ物や紛失物については責任を負いません。

データ転送ターミナル施設の住所

データ転送ターミナル施設の住所は提供されません。代わりに、予約で指定されたプロセス所有者とデータ転送スペシャリストは、データ転送ターミナル施設の検索可能なパブリックネームが記載された E メールを受け取ります。 AWSデータ転送ターミナルでは、インターネット上のパブリックネームを検索してデータ転送ターミナルの施設を見つけることができるように、AWS Direct Connect と同じ場所識別システムを使用します。この情報が記載された E メールがない場合は、転送チームに含まれていることと、E メール情報が正しいことを AWS データ転送ターミナルのアカウントマネージャーに確認してください。

建物へのアクセス

データ転送ターミナル施設にアクセスするには、各データ転送スペシャリストが身分証明書または政府発行の ID を提供する必要があります。建物に入ると、セキュリティによってデータ転送ターミナルの作業室に案内されます。

データ転送ターミナルの作業室で想定される機器。

各データ転送ターミナル施設に設置されているのは、2 本の光ファイバーケーブル、テーブルまたはデスク、椅子のみであるはずです。室内にその他の機器や物品がある場合は、ただちにサポートに報告してください。

ネットワーク接続の問題のトラブルシューティング

AWS データ転送ターミナルの使用中に、インターネットに接続できない、接続速度が遅いなどのネットワーク接続に関する問題が発生した場合は、次のトラブルシューティングのヒントを検討してください。

トピック

機器接続の問題

データ転送ターミナルスイートで物理的な接続を確立できない場合は、次の点を考慮してください。

- 各データ転送ターミナル施設には、シングルモードの LC ファイバーケーブルが 2 本あります。これらのケーブルの一方または両方が見当たらない場合は、すぐに AWS サポートにお問い合わせください。
- 1 つの光ファイバーケーブルが機能しない場合は、まずケーブルを巻き直してみてください。それでも最初のケーブルで接続できない場合は、もう一方のケーブルを使用してみてください。

それでもケーブルを使用して接続できない場合は、すぐに AWS サポートにお問い合わせください。

接続性のトラブルシューティング

機器に接続できるが、ネットワークに接続できない場合は、次のトラブルシューティングの手順を試してください。

- 機器の設定が指定されたネットワーク要件を満たしていることを確認します。詳細については、「データ転送ターミナルを使用するための技術要件」を参照してください。
- 他の光ファイバーケーブルに切り替えて接続します。
- 光ファイバーケーブルを接続したまま、デバイスを再起動します。
- デバイスで基本的なネットワーク診断を実行して、以下を確認します。
  - DHCP が有効になっている

- 接続されたネットワークインターフェイスに IP アドレスが割り当てられている
- DNS サーバーが設定されている
- システムクロックは NTP と同期されている

それでも接続できない場合は、AWS サポートに連絡して、デバイスで実行されているオペレーティングシステム (OS) に応じて次の出力結果を提供してください。

Linux/UNIX

- ターミナルまたはコマンドラインインターフェイス (CLI) で IP アドレスとルーティング情報を取得します。IP アドレスがネットワークインターフェイスに割り当てられ、デフォルトゲートウェイアドレスを持つデフォルトルートがルートテーブルに追加されていることを確認します。

```
ip address show
ip route show
```

  - または、iproute2 がデバイスにインストールされておらず、ip コマンドが使用できない場合は、次のコマンドを使用します。

```
ifconfig
netstat -rn
```

- DNS サーバー情報を収集します。nameserver キーワードで始まる 2 つの IP アドレスが表示されます。

```
cat /etc/resolv.conf
```

- 基本的な接続テストの出力結果を収集します。default_gateway_address を、割り当てられたデフォルトゲートウェイの IP アドレスに置き換えます。

```
ping -c 5 <default_gateway_address>
ping -c 5 s3.amazonaws.com
traceroute s3.amazonaws.com
```

- HTTPS 接続テストの出力結果を収集します。次のコマンドを実行すると、Amazon S3 からの HTTP 200 OK レスポンスが表示されます。

```
curl -i https://s3.amazonaws.com/ping
```

Server

- コマンドプロンプトで IP アドレス、ルーティング、DNS サーバー情報を取得します。IP アドレスがネットワークインターフェイスに割り当てられ、2 つの DNS サーバーが割り当てられ、デフォルトゲートウェイアドレスを持つデフォルトルートがルートテーブルに追加されていることを確認します。

```
ipconfig /all
route print
```

- コマンドプロンプトで基本的な接続テストの出力結果を収集します。default_gateway_address を、割り当てられたデフォルトゲートウェイの IP アドレスに置き換えます。

```
ping <default_gateway_address>
ping s3.amazonaws.com
tracert s3.amazonaws.com
```

- PowerShell で HTTPS 接続テストの出力結果を収集します。次のコマンドを実行すると、HTTP 200 OK レスポンスが表示されます。

```
Invoke-WebRequest -Uri "https://s3.amazonaws.com/ping"
```

ネットワークスループット

ネットワーク内の実際のデータ転送速度を測定するネットワークスループットは、さまざまな要因の影響を受ける可能性があります。以下は、データ転送速度に影響する可能性があります。

- ハードウェア: デバイスのハードウェアコンポーネントにより、データのアップロード時に接続速度が低下する可能性があります。デバイスで使用される CPU とディスクがパフォーマンス制限に達している可能性があります。RAID アレイで NVMe SSD を使用することを検討してください。パフォーマンスを向上させ、CPU 使用率を下げるには、必ず AWS CRT ライブラリを使用してください。
- 暗号化オーバーヘッド: HTTPS などの安全な送信では、暗号化オーバーヘッドにより処理時間が長くなります。
- レイテンシー: レイテンシーとは、データパケットが送信元から送信先に移動するのにかかる時間を指します。別の地理的リージョンの Amazon S3 バケットにアップロードすると、高いレイテン

シーが観察され、データ転送の遅延やスループットの低下につながる可能性があります。可能な限り同じリージョン内でデータ転送を行うことが、ベストプラクティスとされています。

- パケット損失: 紛失したパケットは再送信が必要となり、データ転送が遅くなります。

AWS データ転送ターミナルのセキュリティ

AWS データ転送ターミナルは、AWS クラウドとの間でデータ転送を行うための安全な環境を提供します。他の物理ネットワークファイバー接続と同様に、データ転送ターミナル接続はデフォルトの暗号化を提供しません。したがって、データ転送の安全性を確保するために、データ暗号化のベストプラクティスを適用する責任はユーザーにあります。

AWS でのクラウドセキュリティは最優先事項です。AWS のユーザーは、セキュリティを最も重視する組織の要件を満たすように構築されたデータセンターとネットワークアーキテクチャを利用できます。

セキュリティは、AWS とお客様との間での責任共有です。責任共有モデルでは、この責任がクラウドのセキュリティおよびクラウド内のセキュリティとして説明されています。

- クラウドのセキュリティ - 「AWS」は、「AWS」クラウドで「AWS」のサービスを実行するインフラストラクチャを保護する責任を負います。また、「AWS」は、使用するサービスを安全に提供します。サードパーティーの監査人は、AWS コンプライアンスプログラム の一環として、セキュリティの有効性を定期的にテストおよび検証します。AWS データ転送ターミナルに適用されるコンプライアンスプログラムについては、「コンプライアンスプログラムによる AWS 対象範囲内のサービス」を参照してください。
- クラウド内のセキュリティ - ユーザーの責任は、使用する AWS のサービスに応じて異なります。また、ユーザーは、データの機密性、会社の要件、適用される法律や規制など、その他の要因についても責任を負います。

このドキュメントは、データ転送ターミナルの使用時に責任共有モデルがどのように適用されるかを理解するために役立ちます。以下のトピックでは、データ転送ターミナルサービスの使用中にデータを保護する方法について説明します。また、データ転送ターミナルリソースのモニタリングや保護に役立つ他の AWS のサービスの使用方法についても説明します。

トピック

AWS データ転送ターミナルでのデータ保護

AWS データ転送ターミナルでのデータ保護に AWS の責任共有モデルがどのように適用されるかについて説明します。このモデルで説明したように、AWS は、すべての AWS クラウドを実行するグローバルインフラストラクチャを保護する責任を負います。ユーザーは、このインフラストラクチャでホストされるコンテンツに対する管理を維持する責任があります。また、使用する AWS のサービスのセキュリティ設定と管理タスクにも責任があります。データプライバシーの詳細については、「データプライバシーに関するよくある質問」を参照してください。欧州でのデータ保護の詳細については、AWS セキュリティブログの「AWS 責任共有モデルと GDPR ブログ記事を参照してください。

データ保護の目的で、AWS アカウントの認証情報を保護し、個々のユーザーアカウントを AWS IAM Identity Center または AWS Identity and Access Management (IAM) で設定することをお勧めします。この方法により、それぞれのジョブを遂行するために必要な権限のみが各ユーザーに付与されます。また、次の方法でデータを保護することもお勧めします:

- 各アカウントで多要素認証 (MFA) を使用します。
- SSL/TLS を使用して AWS リソースと通信します。TLS 1.2 は必須ですが、TLS 1.3 を推奨します。
- AWS CloudTrail を使用して API とユーザーアクティビティログを設定します。CloudTrail 証跡を使用して AWS アクティビティをキャプチャする方法については、「AWS ユーザーガイド」の「CloudTrail 証跡の使用」を参照してください。
- AWS 暗号化ソリューションを AWS のサービス内のすべてのデフォルトのセキュリティ管理と一緒に使用します。
- Amazon Macie などの高度な管理されたセキュリティサービスを使用します。これらは、Amazon S3 に保存されている機密データの検出と保護を支援します。
- コマンドラインインターフェイスまたは API を使用して AWS にアクセスする際に FIPS 140-3 検証済みの暗号化モジュールが必要な場合は、FIPS エンドポイントを使用します。利用可能な FIPS エンドポイントの詳細については、「連邦情報処理規格 (FIPS) 140-3」を参照してください。

お客様の E メールアドレスなどの極秘または機密情報を、タグ、または [名前] フィールドなどの自由形式のテキストフィールドに含めないことを強くお勧めします。コンソール、API、AWS CLI、または AWS SDK サービスと転送ターミナル、または他の AWS サービスを併用する場合も同様です。タグ、または名前に使用される自由記述のテキストフィールドに入力したデータは、請求または診断ログに使用される場合があります。外部サーバーに URL を提供する場合、そのサーバーへのリクエストを検証できるように、認証情報を URL に含めないことを強くお勧めします。

データ暗号化

AWS データ転送ターミナルは、セルフマネージドストレージシステムと AWS ストレージサービス間でデータを安全に転送するための高速ネットワーク接続へのアクセスを提供します。転送中のストレージデータの暗号化方法は、デバイス上で有効になっているポリシーと、データが転送されるサービスによって異なります。データの管理と転送中の暗号化は、データ転送ターミナルを使用する個人の責任です。

保管中の暗号化

AWS データ転送ターミナルは、保管中のデータをすべて暗号化します。

データ転送ターミナルは、予約に必要なデータのみをキャプチャします。これには、予約に参加する個人および予約をスケジュールするために指定された個人の姓名や E メールアドレスが含まれます。このデータ収集の目的は、予約の詳細を確認し、データ転送を実行するために部屋へのアクセスを確保することです。このトランザクション情報は 35 日以上はバックアップされませんが、AWS アカウント情報は 10 年間保持されます。

転送中の暗号化

AWS データ転送ターミナルは、転送中のデータを暗号化しません。コンソールからデータ転送ターミナル API エンドポイントを操作し、転送チームのセットアップ、担当者の追加、予約のスケジュールを行う際は、データが転送中に暗号化されます。AWS 責任共有モデルの一環として、データ転送ターミナルを介して AWS サービスへの接続方法を選択できます。TLS 1.2 や 1.3 などの強力な転送中暗号化を使用して、AWS サービスに接続することを強くお勧めします。

例えば、以下のバケットポリシーに示すように、Amazon S3 バケットポリシーの aws:SecureTransport 条件を使用して、HTTPS (TLS) 経由で暗号化された接続のみを使用します。

Amazon S3 など、他の AWS サービスを使用した転送中のデータ暗号化の詳細については、「Amazon S3 ユーザーガイド」の「サーバー側の暗号化によるデータの保護」を参照してください。

キー管理

AWS データ転送ターミナルは、カスタマーマネージドキーを直接サポートしていません。データ転送ターミナルを予約する際は、あなたが接続する AWS サービスで利用可能なカスタマーマネージド

キーのサポートを使用してください。カスタマーマネージドキーの詳細と保管中のデータの暗号化方法については、「AWS Key Management Service デベロッパーガイド」の [AWS KMS キー] セクションを参照してください。

ネットワーク間トラフィックのプライバシー

データ転送ターミナルコンソールへのアクセスは、公開されたサービス API を通じて行います。データ転送ターミナルリソースは、仮想プライベートクラウド (VPC) とは独立しています。

データ転送ターミナルのアイデンティティとアクセス管理

AWS Identity and Access Management (IAM) は、管理者が AWS リソースへのアクセスを安全に制御するのに役立つ AWS のサービスです。IAM 管理者は、誰が 認証 (サインイン) され、データ転送ターミナルリソースを使用する権限 (許可) を受けるかを制御します。IAM は、AWS のサービスで追加料金は発生しません。

トピック

- オーディエンス
- アイデンティティによる認証
- ポリシーを使用したアクセス権の管理
- データ転送ターミナルと IAM の連携方法

オーディエンス

AWS Identity and Access Management (IAM) の使用方法は、データ転送ターミナルで行う作業に応じて異なります。

サービスユーザー – 業務を行うためにデータ転送ターミナルサービスを使用する場合は、管理者から必要な認証情報と許可が提供されます。さらに多くのデータ転送ターミナル機能を使用して作業を行う場合は、追加のアクセス許可が必要になることがあります。アクセスの管理方法を理解すると、管理者に適切なアクセス許可をリクエストするのに役に立ちます。データ転送ターミナルの機能にアクセスできない場合は、「AWS データ転送ターミナルのアイデンティティとアクセスのトラブルシューティング」を参照してください。

サービス管理者 – 社内のデータ転送ターミナルリソースを担当している場合は、通常、データ転送ターミナルへのフルアクセスがあります。サービスユーザーがアクセスするデータ転送ターミナル機

能やリソースを決めるのは管理者の仕事です。その後、IAM 管理者にリクエストを送信して、サービスユーザーの権限を変更する必要があります。このページの情報を点検して、IAM の基本概念を理解してください。会社でデータ転送ターミナルと IAM を併用する方法の詳細については、「データ転送ターミナルと IAM の連携方法」を参照してください。

IAM 管理者 – 管理者は、データ転送ターミナルへのアクセスを管理するポリシーの作成方法の詳細について確認する場合があります。IAM で使用できるデータ転送ターミナルのアイデンティティベースポリシーの例については、「AWS データ転送ターミナルのアイデンティティベースのポリシーの例」を参照してください。

アイデンティティによる認証

認証とは、アイデンティティ認証情報を使用して AWS にサインインする方法です。ユーザーは、AWS アカウントのルートユーザーもしくは IAM ユーザーとして、または IAM ロールを引き受けることによって、認証を受ける (AWS にサインインする) 必要があります。

ID ソースから提供された認証情報を使用して、フェデレーティッドアイデンティティとして AWS にサインインできます。AWSフェデレーティッドアイデンティティの例としては、IAM アイデンティティセンター (IAM アイデンティティセンター) ユーザー、貴社のシングルサインオン認証、Google または Facebook の認証情報などがあります。フェデレーティッド ID としてサインインする場合、IAM ロールを使用して、前もって管理者により ID フェデレーションが設定されています。フェデレーションを使用して AWSにアクセスする場合、間接的にロールを引き受けることになります。

ユーザーのタイプに応じて、AWS マネジメントコンソールまたは AWS アクセスポータルにサインインできます。AWS へのサインインの詳細については、「AWS サインインユーザーガイド」の「AWS アカウントにサインインする方法」を参照してください。

プログラムを使用して AWS にアクセスする場合、AWSは Software Development Kit (SDK) とコマンドラインインターフェイス (CLI) を提供し、認証情報を使用してリクエストに暗号で署名します。AWS ツールを使用しない場合は、リクエストに自分で署名する必要があります。リクエストに自分で署名する推奨方法の使用については、「IAM ユーザーガイド」の「API リクエストに対する AWS Signature Version 4」を参照してください。

使用する認証方法を問わず、追加セキュリティ情報の提供をリクエストされる場合もあります。例えば、AWS は、アカウントのセキュリティを強化するために多要素認証 (MFA) を使用することをお勧めします。詳細については、「AWS IAM Identity Center ユーザーガイド」の「多要素認証」および「IAM ユーザーガイド」の「IAM の AWS 多要素認証」を参照してください。

AWS アカウントのルートユーザー

AWS アカウントを作成する場合は、このアカウントのすべての AWS サービスとリソースに対して完全なアクセス権を持つ 1 つのサインインアイデンティティから始めます。このアイデンティティは AWS アカウントルートユーザーと呼ばれ、アカウントの作成に使用したメールアドレスとパスワードでのサインインによりアクセスされます。日常的なタスクには、ルートユーザーを使用しないことを強くお勧めします。ルートユーザー資格情報は保護し、ルートユーザーでしか実行できないタスクを実行するときに使用します。ルートユーザーとしてサインインする必要があるタスクの完全なリストについては、「IAM ユーザーガイド」の「ルートユーザー資格情報が必要なタスク」を参照してください。

フェデレーテッドアイデンティティ

ベストプラクティスとして、管理者アクセスを必要とするユーザーを含む人間のユーザーに対し、ID プロバイダーとのフェデレーションを使用して、一時的な認証情報の使用により、AWS サービスにアクセスすることを要求します。

フェデレーション ID は、エンタープライズユーザーディレクトリ、ウェブ ID プロバイダー、AWS Directory Service、Identity Center ディレクトリのユーザー、または ID ソースから提供された認証情報を使用して AWS のサービスにアクセスするユーザーです。フェデレーティッド ID が AWS アカウントにアクセスすると、ロールを引き受け、そのロールによって一時的な認証情報が提供されます。

アクセスを一元管理する場合は、AWS IAM Identity Center を使用することをお勧めします。IAM Identity Center でユーザーとグループを作成するか、すべての AWS アカウントとアプリケーションで使用するために、独自の ID ソースで一連のユーザーとグループに接続して同期することもできます。IAM Identity Center の詳細については、「AWS IAM Identity Center ユーザーガイド」の「IAM Identity Center とは何ですか?」を参照してください。

IAM ユーザーとグループ

IAM ユーザーは、単一のユーザーまたはアプリケーションに対する特定の許可を持つ AWS アカウント内のアイデンティティです。可能であれば、パスワードやアクセスキーなどの長期的な認証情報を保有する IAM ユーザーを作成する代わりに、一時的な認証情報を使用することをお勧めします。ただし、IAM ユーザーでの長期的な認証情報が必要な特定のユースケースがある場合は、アクセスキーをローテーションすることをお勧めします。詳細については、「IAM ユーザーガイド」の「長期的な認証情報を必要とするユースケースのためにアクセスキーを定期的にローテーションする」を参照してください。

IAM グループは、IAM ユーザーの集団を指定するアイデンティティです。グループとしてサインインすることはできません。グループを使用して、複数のユーザーに対して一度に権限を指定できます。多数のユーザーグループがある場合、グループを使用することで権限の管理が簡単になります。例えば、IAMAdmins という名前のグループを設定して、そのグループに IAM リソースを管理する許可を与えることができます。

ユーザーは、ロールとは異なります。ユーザーは 1 人の人または 1 つのアプリケーションに一意に関連付けられますが、ロールはそれを必要とする任意の人が引き受けるようになっています。ユーザーには永続的な長期の認証情報がありますが、ロールでは一時認証情報が提供されます。詳細については、「IAM ユーザーガイド」の「IAM ユーザーに関するユースケース」を参照してください。

IAM ロール

IAM ロールは、特定のアクセス許可を持つ、AWS アカウント内のアイデンティティです。これは IAM ユーザーに似ていますが、特定のユーザーに関連付けられていません。AWS マネジメントコンソールで IAM ロールを一時的に引き受けるには、ユーザーから IAM ロール に切り替える (コンソール) ことができます。ロールを引き受けるには、AWS CLI または AWS API オペレーションを呼び出すか、カスタム URL を使用します。ロールを使用する方法の詳細については、「IAM ユーザーガイド」の「ロールを引き受けるための各種方法」を参照してください。

IAM ロールと一時的な認証情報は、次の状況で役立ちます:

- フェデレーションユーザーアクセス – フェデレーティッド ID に許可を割り当てるには、ロールを作成してそのロールの許可を定義します。フェデレーテッド ID が認証されると、その ID はロールに関連付けられ、ロールで定義されている許可が付与されます。フェデレーションのロールについては、IAM ユーザーガイド の サードパーティー ID プロバイダー (フェデレーション) 用のロールを作成する を参照してください。IAM Identity Center を使用する場合は、許可セットを設定します。アイデンティティが認証後にアクセスできるものを制御するため、IAM Identity Center は、権限セットを IAM のロールに関連付けます。アクセス許可セットの詳細については、「AWS IAM Identity Center ユーザーガイド」の「アクセス許可セット」を参照してください。
- 一時的な IAM ユーザー権限 - IAM ユーザーまたはロールは、特定のタスクに対して複数の異なる権限を一時的に IAM ロールで引き受けることができます。
- クロスアカウントアクセス - IAM ロールを使用して、自分のアカウントのリソースにアクセスすることを、別のアカウントの人物 (信頼済みプリンシパル) に許可できます。ロールは、クロスアカウントアクセスを許可する主な方法です。ただし、一部の AWS のサービスでは、(ロールをプロキシとして使用する代わりに) リソースにポリシーを直接アタッチできます。クロスアカウントアクセスにおけるロールとリソースベースのポリシーの違いについては、「IAM ユーザーガイド」の「IAM でのクロスアカウントのリソースへのアクセス」を参照してください。

- クロスサービスアクセス – 一部の AWS のサービスは、AWS の他のサービスの機能を使用します。例えば、サービスで呼び出しを行うと、通常そのサービスによって Amazon EC2 でアプリケーションが実行されたり、Amazon S3 にオブジェクトが保存されたりします。サービスは、呼び出し元のプリンシパルの許可、サービスロール、サービスリンクロールを使用してこれを行う場合があります。
  - 転送アクセスセッション (FAS) – IAM ユーザーまたはロールを使用して AWS でアクションを実行するユーザーは、プリンシパルと見なされます。一部のサービスを使用する際に、アクションを実行することで、別のサービスの別のアクションがトリガーされることがあります。FAS は、AWS サービスを呼び出すプリンシパルの権限を、AWS サービスのリクエストと合わせて使用し、ダウンストリームのサービスに対してリクエストを行います。FAS リクエストは、サービスが、完了するために他の AWS サービスまたはリソースとのやりとりを必要とするリクエストを受け取ったときにのみ行われます。この場合、両方のアクションを実行するためのアクセス許可が必要です。FAS リクエストを行う際のポリシーの詳細については、「転送アクセスセッション」を参照してください。
  - サービスロール - サービスがユーザーに代わってアクションを実行するために引き受ける IAM ロールです。IAM 管理者は、IAM 内からサービスロールを作成、変更、削除できます。詳細については、「IAM ユーザーガイド」の「AWS のサービスにアクセス許可を委任するロールの作成」を参照してください。
  - サービスリンクロール – サービスリンクロールは、AWS のサービスにリンクされているサービスロールの一種です。サービスがロールを引き受け、ユーザーに代わってアクションを実行できるようになります。サービスにリンクされたロールは、AWS アカウント内に表示され、サービスによって所有されます。IAM 管理者は、サービスリンクロールのアクセス許可を表示できますが、編集することはできません。
- Amazon EC2 で実行されているアプリケーション – EC2 インスタンスで実行され、AWS CLI または AWS API リクエストを作成しているアプリケーションの一時的な認証情報を管理するには、IAM ロールを使用します。これは、EC2 インスタンス内でのアクセスキーの保存に推奨されます。AWS ロールを EC2 インスタンスに割り当て、そのすべてのアプリケーションで使用できるようにするには、インスタンスに添付されたインスタンスプロファイルを作成します。インスタンスプロファイルにはロールが含まれ、EC2 インスタンスで実行されるプログラムは一時的な認証情報を取得できます。詳細については、「IAM ユーザーガイド」の「Amazon EC2 インスタンスで実行されるアプリケーションに IAM ロールを使用して許可を付与する」を参照してください。

ポリシーを使用したアクセス権の管理

AWS でアクセスを制御するには、ポリシーを作成して AWS ID またはリソースにアタッチします。ポリシーは AWS のオブジェクトであり、アイデンティティやリソースに関連付けて、これらのアクセス許可を定義します。AWS は、プリンシパル (ユーザー、ルートユーザー、またはロールセッション) がリクエストを行うと、これらのポリシーを評価します。ポリシーでの権限により、リクエストが許可されるか拒否されるかが決まります。大半のポリシーは JSON ドキュメントとして AWS に保存されます。JSON ポリシードキュメントの構造と内容の詳細については、「IAM ユーザーガイド」の「JSON ポリシー概要」を参照してください。

管理者は AWS JSON ポリシーを使用して、だれが何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

デフォルトでは、ユーザーやロールに権限はありません。IAM 管理者は、リソースで必要なアクションを実行するための権限をユーザーに付与する IAM ポリシーを作成できます。その後、管理者はロールに IAM ポリシーを追加し、ユーザーはロール引き継ぐことができます。

IAM ポリシーは、オペレーションの実行方法を問わず、アクションの許可を定義します。例えば、`iam:GetRole` アクションを許可するポリシーがあるとします。このポリシーがあるユーザーは、AWS マネジメントコンソール、AWS CLI、または AWS API からロールの情報を取得できます。

アイデンティティベースポリシー

アイデンティティベースのポリシーは、IAM ユーザーグループ、ユーザーのグループ、ロールなど、アイデンティティにアタッチできる JSON 許可ポリシードキュメントです。これらのポリシーは、ユーザーとロールが実行できるアクション、リソース、および条件をコントロールします。アイデンティティベースポリシーの作成方法については、「IAM ユーザーガイド」の「カスタマー管理ポリシーでカスタム IAM アクセス許可を定義する」を参照してください。

アイデンティティベースのポリシーは、さらにインラインポリシーまたはマネージドポリシーに分類できます。インラインポリシーは、単一のユーザー、グループ、またはロールに直接埋め込まれています。管理ポリシーは、AWS アカウント内の複数のユーザー、グループ、およびロールにアタッチできるスタンドアロンポリシーです。マネージドポリシーには、AWS マネージドポリシーとカスタマーマネージドポリシーがあります。マネージドポリシーまたはインラインポリシーのいずれかを選択する方法については、「IAM ユーザーガイド」の「管理ポリシーとインラインポリシーのいずれかを選択する」を参照してください。

リソースベースのポリシー

リソースベースのポリシーは、リソースに添付する JSON ポリシードキュメントです。リソースベースのポリシーには例として、IAM ロールの信頼ポリシーや Amazon S3 バケットポリシーがあげられます。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスをコントロールできます。ポリシーがアタッチされているリソースの場合、指定されたプリンシパルがそのリソースに対して実行できるアクションと条件は、ポリシーによって定義されます。リソースベースのポリシーで、[specify a principal] (プリンシパルを指定する) 必要があります。プリンシパルには、アカウント、ユーザー、ロール、フェデレーティッドユーザー、または AWS のサービスを含めることができます。

リソースベースのポリシーは、そのサービス内にあるインラインポリシーです。リソースベースのポリシーでは、IAM からの AWS マネージド型ポリシーを使用することはできません。

アクセスコントロールリスト (ACL)

アクセスコントロールリスト (ACL) は、どのプリンシパル (アカウントメンバー、ユーザー、またはロール) がリソースにアクセスするためのアクセス許可を持つかを制御します。ACL はリソースベースのポリシーに似ていますが、JSON ポリシードキュメント形式は使用しません。

Amazon S3、AWS WAF、および Amazon VPC は、ACL をサポートするサービスの例です。ACL の詳細については、Amazon Simple Storage Service デベロッパーガイド の アクセスコントロールリスト (ACL) の概要 を参照してください。

その他のポリシータイプ

AWS では、他の一般的ではないポリシータイプをサポートしています。これらのポリシータイプでは、より一般的なポリシータイプで付与された最大の権限を設定できます。

- アクセス許可の境界 - アクセス許可の境界は、アイデンティティベースポリシーによって IAM エンティティ (IAM ユーザーまたはロール) に付与できる権限の上限を設定する高度な機能です。エンティティにアクセス許可の境界を設定できます。結果として得られるアクセス許可は、エンティティのアイデンティティベースポリシーとそのアクセス許可の境界の共通部分になります。`Principal` フィールドでユーザーまたはロールを指定するリソースベースのポリシーでは、アクセス許可の境界は制限されません。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。アクセス許可の境界の詳細については、「IAM ユーザーガイド」の「IAM エンティティのアクセス許可の境界」を参照してください。
- サービスコントロールポリシー (SCP) – SCP とは、AWS Organizations 内の組織または組織単位 (OU) に対し、アクセス許可の上限を指定するための JSON ポリシーです。AWSOrganizations

は、ビジネスが所有する複数の AWS アカウントを、グループ化および一元管理するためのサービスです。組織内のすべての機能を有効にすると、サービスコントロールポリシー (SCP) を一部またはすべてのアカウントに適用できます。SCP はメンバーアカウントのエンティティに対するアクセス許可を制限します (各 AWS アカウントルートユーザーなど)。Organizations と SCP の詳細については、「AWS Organizations ユーザーガイド」の「サービスコントロールポリシー」を参照してください。

- リソースコントロールポリシー (RCP) – RCP は、所有する各リソースにアタッチされた IAM ポリシーを更新することなく、アカウント内のリソースに利用可能な最大数のアクセス許可を設定するために使用できる JSON ポリシーです。RCP は、メンバーアカウントのリソースの許可を制限し、組織に属するかどうかにかかわらず、AWS アカウントルートユーザーを含む ID のための有効な許可に影響を及ぼす可能性があります。RCP をサポートする AWS のリストを含む Organizations と RCP の詳細については、「AWS ユーザーガイド」の「リソースコントロールポリシー (RCP)」を参照してください。
- セッションポリシー - セッションポリシーは、ロールまたはフェデレーションユーザーの一時的なセッションをプログラムで作成する際にパラメータとして渡す高度なポリシーです。結果として得られるセッションの許可は、ユーザーまたはロールのアイデンティティベースポリシーとセッションポリシーの共通部分です。また、リソースベースのポリシーから権限が派生する場合もあります。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。詳細については、「IAM ユーザーガイド」の「セッションポリシー」を参照してください。

複数のポリシータイプ

1 つのリクエストに複数のタイプのポリシーが適用されると、結果として作成されるアクセス許可を理解するのがさらに難しくなります。複数のポリシータイプが関連するとき、リクエストを許可するかどうかを AWS が決定する方法の詳細については、IAM ユーザーガイド の ポリシーの評価ロジック を参照してください。

データ転送ターミナルと IAM の連携方法

IAM を使用して データ転送ターミナルへのアクセスを管理する前に、データ転送ターミナル で使用できる IAM 機能について理解しておく必要があります。

IAM の特徴量	データ転送ターミナルのサポート
アイデンティティベースのポリシー	あり
リソースベースのポリシー	なし

IAM の特徴量	データ転送ターミナルのサポート
ポリシーアクション	あり
ポリシーリソース	あり
ポリシー条件キー	あり
ACL	なし
ABAC (ポリシー内のタグ)	いいえ
一時的な認証情報	あり
プリンシパル権限	いいえ
サービスロール	いいえ
サービスリンクロール	不可

データ転送ターミナルおよびその他の AWS サービスと大部分の IAM 機能の連携についての概要は、「IAM ユーザーガイド」の「IAM と連携する AWS のサービス」を参照してください。

データ転送ターミナルのアイデンティティベースのポリシー

ID ベースのポリシーのサポート: あり

アイデンティティベースポリシーは、IAM ユーザー、ユーザーグループ、ロールなど、アイデンティティにアタッチできる JSON 許可ポリシードキュメントです。これらのポリシーは、ユーザーとロールが実行できるアクション、リソース、および条件をコントロールします。アイデンティティベースポリシーの作成方法については、「IAM ユーザーガイド」の「カスタマー管理ポリシーでカスタム IAM アクセス許可を定義する」を参照してください。

IAM アイデンティティベースのポリシーでは、許可または拒否するアクションとリソース、およびアクションを許可または拒否する条件を指定できます。プリンシパルはアタッチされているユーザーまたはロールに適用されるため、アイデンティティベースのポリシーでは指定できません。JSON ポリシーで使用できるすべての要素について学ぶには、「IAM ユーザーガイド」の「IAM JSON ポリシーの要素のリファレンス」を参照してください。

データ転送ターミナルのアイデンティティベースのポリシーの例

データ転送ターミナルのアイデンティティベースポリシーの例を確認するには、「AWS データ転送ターミナルのアイデンティティベースのポリシーの例」を参照してください。

データ転送ターミナル内のリソースベースのポリシー

リソースベースのポリシーのサポート: なし

リソースベースのポリシーは、リソースに添付する JSON ポリシードキュメントです。リソースベースのポリシーには例として、IAM ロールの信頼ポリシーや Amazon S3 バケットポリシーがあげられます。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスをコントロールできます。ポリシーがアタッチされているリソースの場合、指定されたプリンシパルがそのリソースに対して実行できるアクションと条件は、ポリシーによって定義されます。リソースベースのポリシーで、[specify a principal] (プリンシパルを指定する) 必要があります。プリンシパルには、アカウント、ユーザー、ロール、フェデレーティッドユーザー、または AWS のサービスを含めることができます。

クロスアカウントアクセスを有効にするには、全体のアカウント、または別のアカウントの IAM エンティティを、リソースベースのポリシーのプリンシパルとして指定します。リソースベースのポリシーにクロスアカウントのプリンシパルを追加しても、信頼関係は半分しか確立されない点に注意してください。プリンシパルとリソースが異なる AWS アカウントにある場合、信頼されたアカウントの IAM 管理者は、リソースにアクセスするための許可をプリンシパルエンティティ (ユーザーまたはロール) に付与する必要もあります。IAM 管理者は、ID ベースのポリシーをエンティティにアタッチすることで許可を付与します。ただし、リソースベースのポリシーで、同じアカウントのプリンシパルへのアクセス権が付与されている場合は、アイデンティティベースのポリシーをさらに付与する必要はありません。詳細については、「IAM ユーザーガイド」の「IAM でのクロスアカウントリソースアクセス」を参照してください。

データ転送ターミナルのポリシーアクション

ポリシーアクションのサポート: あり

管理者は AWS JSON ポリシーを使用して、だれが何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

JSON ポリシーの `Action` 要素にはポリシー内のアクセスを許可または拒否するために使用できるアクションが記述されます。ポリシーアクションの名前は通常、関連する AWS API オペレーションと同じです。一致する API オペレーションのないアクセス許可のみのアクションなど、いくつかの

例外があります。また、ポリシーに複数のアクションが必要なオペレーションもあります。これらの追加アクションは依存アクションと呼ばれます。

このアクションは関連付けられたオペレーションを実行するためのアクセス許可を付与するポリシーで使用されます。

データ転送ターミナルアクションのリストを確認するには、「サービス認可リファレンス」の「AWS データ転送ターミナルで定義されるアクション」を参照してください。

データ転送ターミナルのポリシーアクションは、アクションの前に次のプレフィックスを使用します。

```
datatransferterminal
```

単一のステートメントで複数のアクションを指定するには、アクションをカンマで区切ります。

```
"Action": [
      "datatransferterminal:action1",
      "datatransferterminal:action2"
         ]
```

データ転送ターミナルのアイデンティティベースポリシーの例を確認するには、「AWS データ転送ターミナルのアイデンティティベースのポリシーの例」を参照してください。

データ転送ターミナルのポリシーリソース

ポリシーリソースのサポート: あり

管理者は AWS JSON ポリシーを使用して、だれが何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

Resource JSON ポリシー要素はアクションが適用されるオブジェクトを指定します。ステートメントにはResource または NotResource 要素を含める必要があります。ベストプラクティスとして、Amazon リソースネーム (ARN) を使用してリソースを指定します。これはリソースレベルの許可と呼ばれる特定のリソースタイプをサポートするアクションに対して実行できます。

オペレーションのリスト化など、リソースレベルの許可をサポートしないアクションの場合はステートメントがすべてのリソースに適用されることを表示するワイルドカード (*) を使用します。

```
"Resource": "*"
```

データ転送ターミナルリソースのタイプとその ARN のリストを確認するには、「サービス認可リファレンス」の「AWS データ転送ターミナルで定義されるリソース」を参照してください。どのアクションで各リソースの ARN を指定できるかについては、「AWS データ転送ターミナルで定義されるアクション」を参照してください。

データ転送ターミナルのアイデンティティベースポリシーの例を確認するには、「AWS データ転送ターミナルのアイデンティティベースのポリシーの例」を参照してください。

データ転送ターミナルのポリシー条件キー

サービス固有のポリシー条件キーのサポート: あり

管理者は AWS JSON ポリシーを使用して、だれが何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

`Condition` 要素 (または `Condition` *`block`*) lets you specify conditions in which a statement is in effect. The `Condition` 要素はオプションです。イコールや未満などの条件演算子を使用して条件式を作成して、ポリシーの条件とリクエスト内の値を一致させることができます。

1 つのステートメントに複数の `Condition` 要素を指定する場合、または 1 つの `Condition` 要素に複数のキーを指定する場合、AWS では `AND` 論理演算子を使用してそれらを評価します。単一の条件キーに複数の値を指定する場合、AWS では `OR` 論理演算子を使用して条件を評価します。ステートメントのアクセス許可が付与される前に、すべての条件が満たされる必要があります。

条件を指定する際にプレースホルダー変数も使用できます。例えば IAM ユーザーに、IAM ユーザー名がタグ付けされている場合のみリソースにアクセスできる権限を付与することができます。詳細については、「IAM ユーザーガイド」の「IAM ポリシーの要素: 変数およびタグ」を参照してください。

AWS はグローバル条件キーとサービス固有の条件キーをサポートしています。すべての AWS グローバル条件キーを確認するには、IAM ユーザーガイドのAWS グローバル条件コンテキストキーを参照してください。

データ転送ターミナルの条件キーのリストを確認するには、「サービス認可リファレンス」の「AWS データ転送ターミナルの条件キー」を参照してください。条件キーを使用できるアクションとリソースについては、「AWS データ転送ターミナルで定義されるアクション」を参照してください。

データ転送ターミナルのアイデンティティベースポリシーの例を確認するには、「AWS データ転送ターミナルのアイデンティティベースのポリシーの例」を参照してください。

データ転送ターミナルの ACL

ACL のサポート: なし

アクセスコントロールリスト (ACL) は、どのプリンシパル (アカウントメンバー、ユーザー、またはロール) がリソースにアクセスするためのアクセス許可を持つかを制御します。ACL はリソースベースのポリシーに似ていますが、JSON ポリシードキュメント形式は使用しません。

データ転送ターミナルでの ABAC

ABAC (ポリシー内のタグ) のサポート: なし

属性ベースのアクセス制御 (ABAC) は、属性に基づいてアクセス許可を定義する認可戦略です。AWS では、属性はタグと呼ばれます。タグは、IAM エンティティ (ユーザーまたはロール)、および多数の AWS リソースにアタッチできます。エンティティとリソースのタグ付けは、ABAC の最初の手順です。次に、プリンシパルのタグが、アクセスを試行するリソースのタグと一致したときにオペレーションを許可するよう、ABAC ポリシーを設計します。

ABAC は、急成長する環境や、ポリシー管理が煩雑になる状況で役に立ちます。

タグに基づいてアクセスを制御するには、`aws:ResourceTag/[replaceable]key-name ``, , or aws:TagKeys condition keys.` を使用するポリシーの条件要素のタグ情報を指定します。サービスがすべてのリソースタイプで 3 つの条件キーすべてをサポートしている場合、値はサービスに対して Yes です。サービスが一部のリソースタイプに対してのみ 3 つの条件キーのすべてをサポートする場合、値は「部分的」になります。ABAC の詳細については、「IAM ユーザーガイド」の「ABAC 認可でアクセス許可を定義する」を参照してください。ABAC をセットアップする手順を説明するチュートリアルについては、「IAM ユーザーガイド」の「属性ベースのアクセスコントロール (ABAC) を使用する」を参照してください。

データ転送ターミナルでの一時的な認証情報の使用

一時的な認証情報のサポート: あり

AWS サービスには、一時的な認証情報を使用してサインインしても機能しないものがあります。一時的な認証情報を利用できる AWS のサービスを含めた詳細情報については、「IAM ユーザーガイド」の「IAM と連携する AWS サービス」を参照してください。

ユーザー名とパスワード以外の方法で AWS マネジメントコンソールにサインインする場合は、一時認証情報を使用していることになります。例えば、会社の Single Sign-On (SSO) リンクを使用して

AWS にアクセスすると、そのプロセスは自動的に一時的な認証情報を作成します。また、ユーザーとしてコンソールにサインインしてからロールを切り替える場合も、一時的な認証情報が自動的に作成されます。ロールの切り替えに関する詳細については、「IAM ユーザーガイド」の「ユーザーから IAM ロールに切り替える (コンソール)」を参照してください。

一時的な認証情報は、AWS CLI または AWS API を使用して手動で作成できます。作成後、一時認証情報を使用して AWS にアクセスできるようになります。AWSは、長期的なアクセスキーを使用する代わりに、一時認証情報を動的に生成することをお勧めします。詳細については、「IAM の一時的セキュリティ認証情報」を参照してください。

データ転送ターミナルのクロスサービスプリンシパルアクセス許可

転送アクセスセッション (FAS) のサポート: なし

IAM ユーザーまたはロールを使用して AWS でアクションを実行するユーザーは、プリンシパルとみなされます。一部のサービスを使用する際に、アクションを実行することで、別のサービスの別のアクションがトリガーされることがあります。FAS は、AWS サービスを呼び出すプリンシパルの権限を、AWS サービスのリクエストと合わせて使用し、ダウンストリームのサービスに対してリクエストを行います。FAS リクエストは、サービスが、完了するために他の AWS サービスまたはリソースとのやりとりを必要とするリクエストを受け取ったときにのみ行われます。この場合、両方のアクションを実行するためのアクセス許可が必要です。FAS リクエストを行う際のポリシーの詳細については、「転送アクセスセッション」を参照してください。

データ転送ターミナルのサービスロール

サービスロールのサポート: なし

サービスロールとは、サービスがユーザーに代わってアクションを実行するために引き受ける IAM ロールです。IAM 管理者は、IAM 内からサービスロールを作成、変更、削除できます。詳細については、「IAM ユーザーガイド」の「AWS のサービスにアクセス許可を委任するロールの作成」を参照してください。

> **Warning**
>
> サービスロールの権限を変更すると、データ転送ターミナルの機能が停止する可能性があります。データ転送ターミナルが指示する場合以外は、サービスロールを編集しないでください。

データ転送ターミナルのサービスにリンクされたロール

サービスにリンクされたロールのサポート: なし

サービスにリンクされたロールは、AWS のサービスにリンクされているサービスロールの一種です。サービスがロールを引き受け、ユーザーに代わってアクションを実行できるようになります。サービスにリンクされたロールは、AWS アカウント内に表示され、サービスによって所有されます。IAM 管理者は、サービスにリンクされたロールのアクセス許可を表示できますが、編集することはできません。

サービスにリンクされたロールの作成または管理の詳細については、「IAM と提携する AWS のサービス」を参照してください。表の「サービスリンクロール」列に Yes と記載されたサービスを見つけます。サービスにリンクされたロールに関するドキュメントをサービスで表示するには、[はい] リンクを選択します。

AWS データ転送ターミナルのアイデンティティベースのポリシーの例

デフォルトでは、ユーザーおよびロールにはデータ転送ターミナルリソースを作成または変更するアクセス許可がありません。また、AWS マネジメントコンソール、AWS コマンドラインインターフェイス (AWS CLI)、または AWS API を使用してタスクを実行することもできません。IAM 管理者は、リソースで必要なアクションを実行するための権限をユーザーに付与する IAM ポリシーを作成できます。その後、管理者はロールに IAM ポリシーを追加し、ユーザーはロールを引き継ぐことができます。

これらサンプルの JSON ポリシードキュメントを使用して、IAM アイデンティティベースのポリシーを作成する方法については、「IAM ユーザーガイド」の「IAM ポリシーを作成する (コンソール)」を参照してください。

定義されるアクションとリソースタイプ (リソースタイプごとの ARN の形式など) の詳細については、「サービス認可リファレンス」の「アクション」を参照してください。

トピック

- ポリシーに関するベストプラクティス
- データ転送ターミナルコンソールの使用
- 自分の権限の表示をユーザーに許可する

ポリシーに関するベストプラクティス

アイデンティティベースのポリシーは、ユーザーのアカウント内で誰かがデータ転送ターミナルリソースを作成、アクセス、または削除できるどうかを決定します。これらのアクションを実行すると、AWS アカウントに追加料金が発生する可能性があります。アイデンティティベースポリシーを作成したり編集したりする際には、以下のガイドラインと推奨事項に従ってください:

- AWS マネージドポリシーを使用して開始し、最小特権の許可に移行する – ユーザーとワークロードへの許可の付与を開始するには、多くの一般的なユースケースのために許可を付与する AWS マネージドポリシーを使用します。これらは AWS アカウントで使用できます。ユースケースに固有の AWS カスタマー管理ポリシーを定義して、アクセス許可を絞り込むことをお勧めします。詳細については、IAM ユーザーガイド の AWS マネージドポリシー または ジョブ機能の AWS マネージドポリシー を参照してください。
- 最小特権を適用する – IAM ポリシーでアクセス許可を設定する場合は、タスクの実行に必要な許可のみを付与します。これを行うには、特定の条件下で特定のリソースに対して実行できるアクションを定義します。これは、最小特権アクセス許可とも呼ばれています。IAM を使用して許可を適用する方法の詳細については、IAM ユーザーガイド の IAM でのポリシーとアクセス許可 を参照してください。
- IAM ポリシーで条件を使用してアクセスをさらに制限する - ポリシーに条件を追加して、アクションやリソースへのアクセスを制限できます。たとえば、ポリシー条件を記述して、すべてのリクエストを SSL を使用して送信するように指定できます。また、AWS CloudFormation などの特定の AWS サービスを介して使用する場合、条件を使用してサービスアクションへのアクセスを許可することもできます。詳細については、IAM ユーザーガイド」の「IAM JSON ポリシー要素: 条件」を参照してください。
- IAM アクセスアナライザー を使用して IAM ポリシーを検証し、安全で機能的な権限を確保する - IAM アクセスアナライザー は、新規および既存のポリシーを検証して、ポリシーが IAM ポリシー言語 (JSON) および IAM のベストプラクティスに準拠するようにします。IAM アクセスアナライザーは 100 を超えるポリシーチェックと実用的な推奨事項を提供し、安全で機能的なポリシーの作成をサポートします。詳細については、IAM ユーザーガイド の IAM Access Analyzer でポリシーを検証する を参照してください。
- 多要素認証 (MFA) を要求する – AWS アカウントで IAM ユーザーまたはルートユーザーを要求するシナリオがある場合は、セキュリティを強化するために MFA をオンにします。API オペレーションが呼び出されるときに MFA を必須にするには、ポリシーに MFA 条件を追加します。詳細については、IAM ユーザーガイド の MFA を使用した安全な API アクセス を参照してください。

IAM でのベストプラクティスの詳細については、IAM ユーザーガイド の IAM でのセキュリティのベストプラクティス を参照してください。

データ転送ターミナルコンソールの使用

AWS データ転送ターミナルコンソールにアクセスするには、許可の最小限のセットが必要です。これらの許可では、AWS アカウントでのデータ転送ターミナルリソースに関する詳細のリスト化と表示が許可されている必要があります。最小限必要な許可よりも制限が厳しいアイデンティティベースのポリシーを作成すると、そのポリシーを持つエンティティ (ユーザーまたはロール) に対してコンソールが意図したとおりに機能しません。

AWS CLI または AWS API のみを呼び出すユーザーには、コンソールの最小アクセス許可を付与する必要はありません。代わりに、実行しようとしている API オペレーションに一致するアクションのみへのアクセスを許可します。

ユーザーとロールが引き続きデータ転送ターミナルコンソールを使用できるようにするには、エンティティにデータ転送ターミナル *ConsoleAccess* または *ReadOnly* AWS 管理ポリシーもアタッチします。詳細については、「IAM ユーザーガイド」の「ユーザーへのアクセス許可の追加」を参照してください。

自分の権限の表示をユーザーに許可する

この例では、ユーザーアイデンティティにアタッチされたインラインおよびマネージドポリシーの表示を IAM ユーザーに許可するポリシーの作成方法を示します。このポリシーには、コンソールで、または AWS CLI もしくは AWS API を使用してプログラム的に、このアクションを完了するための許可が含まれています。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
```

```
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS データ転送ターミナルのアイデンティティとアクセスのトラブルシューティング

次の情報は、データ転送ターミナルと IAM の使用に伴って発生する可能性がある一般的な問題の診断や修復に役立ちます。

トピック

- データ転送ターミナルでアクションを実行する権限がありません
- AWS アカウントの外部のユーザーにデータ転送ターミナルリソースへのアクセスを許可したい

データ転送ターミナルでアクションを実行する権限がありません

AWS データ転送ターミナルコンソールで予約を表示またはスケジュールできない場合は、必要なアクセス許可がない可能性があります。アカウント管理者に連絡して、アクセスと適切なアクセス許可を付与する IAM ID ポリシーを設定してください。

AWS アカウントの外部のユーザーにデータ転送ターミナルリソースへのアクセスを許可したい

他のアカウントのユーザーや組織外の人が、リソースにアクセスするために使用できるロールを作成できます。ロールの引き受けを委託するユーザーを指定できます。リソースベースのポリシーまたはアクセスコントロールリスト (ACL) をサポートするサービスの場合、それらのポリシーを使用して、リソースへのアクセスを付与できます。

詳細については、以下を参照してください。

- データ転送ターミナルがこれらの機能をサポートしているかどうかについては、「データ転送ターミナルと IAM の連携方法」を参照してください。
- 所有している AWS アカウント全体のリソースへのアクセス権を提供する方法については、IAM ユーザーガイドの所有している別の AWS アカウントへのアクセス権を IAM ユーザーに提供を参照してください。
- リソースへのアクセスをサードパーティーの AWS アカウントに提供する方法については、IAM ユーザーガイドの「サードパーティーが所有する AWS アカウントへのアクセスの提供」を参照してください。
- ID フェデレーションを介してアクセスを提供する方法については、IAM ユーザーガイド の 外部で認証されたユーザー (ID フェデレーション) へのアクセスの許可 を参照してください。
- クロスアカウントアクセスにおけるロールとリソースベースのポリシーの使用方法の違いについては、IAM ユーザーガイド の IAM でのクロスアカウントのリソースへのアクセス を参照してください。

データ転送ターミナル API リファレンス: アクションとリソース

AWS Identity and Access Management (IAM) ポリシーを作成する際、このページは、AWS データ転送ターミナル API オペレーション、実行するアクセス許可を付与する対象アクション、およびアクセス許可を付与できる AWS リソースの関係を理解するのに役立ちます。

一般的に、データ転送ターミナルのアクセス許可をポリシーに追加する方法は次のとおりです。

- `Action` エレメントにアクションを指定します。`datatransferterminal:` 値にはプレフィックスと API オペレーション名が含まれます。例えば、`datatransferterminal:CreateTask`。
- `Resource` エレメントのアクションに関連する AWS リソースを指定します。

データ転送ターミナルポリシーで AWS 条件キーを使用することもできます。すべての AWS キーのリストについては、「IAM ユーザーガイド」の「利用可能なキー」を参照してください。

データ転送ターミナル API オペレーションと対応するアクション

CreateTransferTeam

- アクション:`datatransferterminal:CreateTransferTeam`

  リソース: None

GetTransferTeam

- アクション:datatransferterminal:GetTransferTeam

  リソース: arn:aws::$[replaceable]Partition:datatransferterminal:
  $[replaceable]Region:$[replaceable]Account:transfer-team/
  $[replaceable]TransferTeamId````

UpdateTransferTeam

- アクション:datatransferterminal:UpdateTransferTeam

  リソース: arn:aws::$[replaceable]Partition:datatransferterminal:
  $[replaceable]Region:$[replaceable]Account:transfer-team/
  $[replaceable]TransferTeamId````

DeleteTransferTeam

- アクション:datatransferterminal:DeleteTransferTeam

  リソース: arn:aws::$[replaceable]Partition:datatransferterminal:
  $[replaceable]Region:$[replaceable]Account:transfer-team/
  $[replaceable]TransferTeamId````

ListTransferTeams

- アクション:datatransferterminal:ListTransferTeams

  リソース: None

RegisterPerson

- アクション:datatransferterminal:RegisterPerson

  リソース: arn:aws::$[replaceable]Partition:datatransferterminal:
  $[replaceable]Region:$[replaceable]Account:transfer-team/
  $[replaceable]TransferTeamId````

GetPerson

- アクション:datatransferterminal:GetPerson

  リソース: arn:aws::$[replaceable]Partition:datatransferterminal:
  $[replaceable]Region:$[replaceable]Account:transfer-team/
  $[replaceable]TransferTeamId/person/$[replaceable]PersonId````

  依存アクション: datatransferterminal:GetTransferTeam

依存リソース: arn:aws::$[replaceable]Partition:datatransferterminal:
$[replaceable]Region:$[replaceable]Account:transfer-team/
$[replaceable]TransferTeamId````

DeregisterPerson

- アクション:datatransferterminal:DeregisterPerson

  リソース: arn:aws::$[replaceable]Partition:datatransferterminal:
  $[replaceable]Region:$[replaceable]Account:transfer-team/
  $[replaceable]TransferTeamId/person/$[replaceable]PersonId````

  依存アクション: datatransferterminal:GetTransferTeam

  依存リソース: arn:aws::$[replaceable]Partition:datatransferterminal:
  $[replaceable]Region:$[replaceable]Account:transfer-team/
  $[replaceable]TransferTeamId````

ListPersons

- アクション:datatransferterminal:ListPersons

  リソース: arn:aws::$[replaceable]Partition:datatransferterminal:
  $[replaceable]Region:$[replaceable]Account:transfer-team/
  $[replaceable]TransferTeamId````

CreateReservation

- アクション:datatransferterminal:CreateReservation

  リソース: arn:aws::$[replaceable]Partition:datatransferterminal:
  $[replaceable]Region:$[replaceable]Account:transfer-team/
  $[replaceable]TransferTeamId````

  依存アクション: datatransferterminal:GetTransferTeam

  依存リソース: arn:aws::$[replaceable]Partition:datatransferterminal:
  $[replaceable]Region:$[replaceable]Account:transfer-team/
  $[replaceable]TransferTeamId````

  依存アクション: datatransferterminal:GetPerson

依存リソース: arn:aws::$[replaceable]Partition:datatransferterminal:
$[replaceable]Region:$[replaceable]Account:transfer-team/
$[replaceable]TransferTeamId/person/$[replaceable]PersonId````

依存アクション: datatransferterminal:GetFacility

依存リソース: arn:aws::
$[replaceable]Partition:datatransferterminal:::facility/
$[replaceable]FacilityId````

GetReservation

- アクション:datatransferterminal:GetReservation

  リソース: arn:aws::$[replaceable]Partition:datatransferterminal:
  $[replaceable]Region:$[replaceable]Account:transfer-team/
  $[replaceable]TransferTeamId/reservation/$[replaceable]ReservationId````

  依存アクション: datatransferterminal:GetTransferTeam

  依存リソース: arn:aws::$[replaceable]Partition:datatransferterminal:
  $[replaceable]Region:$[replaceable]Account:transfer-team/
  $[replaceable]TransferTeamId````

UpdateReservation

- アクション:datatransferterminal:UpdateReservation

  リソース: arn:aws::$[replaceable]Partition:datatransferterminal:
  $[replaceable]Region:$[replaceable]Account:transfer-team/
  $[replaceable]TransferTeamId/reservation/$[replaceable]ReservationId````

  依存アクション: datatransferterminal:GetTransferTeam

  依存リソース: arn:aws::$[replaceable]Partition:datatransferterminal:
  $[replaceable]Region:$[replaceable]Account:transfer-team/
  $[replaceable]TransferTeamId````

  依存アクション: datatransferterminal:GetPerson

依存リソース: arn:aws::$[replaceable]Partition:datatransferterminal:
$[replaceable]Region:$[replaceable]Account:transfer-team/
$[replaceable]TransferTeamId/person/$[replaceable]PersonId````

DeleteReservation

- アクション:datatransferterminal:DeleteReservation

  リソース: arn:aws::$[replaceable]Partition:datatransferterminal:
  $[replaceable]Region:$[replaceable]Account:transfer-team/
  $[replaceable]TransferTeamId/person/$[replaceable]PersonId````

  依存アクション: datatransferterminal:GetTransferTeam

  依存リソース: arn:aws::$[replaceable]Partition:datatransferterminal:
  $[replaceable]Region:$[replaceable]Account:transfer-team/
  $[replaceable]TransferTeamId````

ListReservations

- アクション:datatransferterminal:ListReservations

  リソース: arn:aws::$[replaceable]Partition:datatransferterminal:
  $[replaceable]Region:$[replaceable]Account:transfer-team/
  $[replaceable]TransferTeamId````

ListFacilities

- アクション:datatransferterminal:ListFacilities

  リソース: None

GetFacility

- アクション:datatransferterminal:GetFacility

  リソース: arn:aws::$[replaceable]Partition:datatransferterminal:::facility/
  $[replaceable]FacilityId````

GetFacilityAvailability

- アクション:datatransferterminal:GetFacilityAvailability

  リソース: arn:aws::$[replaceable]Partition:datatransferterminal:::facility/
  $[replaceable]FacilityId/availability

依存アクション: `datatransferterminal:GetFacility`

依存リソース: `arn:aws::$[replaceable]Partition:datatransferterminal:::facility/$[replaceable]FacilityId/availability`

AWS データ転送ターミナルのコンプライアンス検証

AWS のサービスが特定のコンプライアンスプログラムの対象であるかどうかを確認するには、「コンプライアンスプログラムによる対象範囲内の AWS サービス」をご覧いただき、関心のあるコンプライアンスプログラムを選択してください。一般的な情報については、「AWS コンプライアンスプログラム」を参照してください。

サードパーティーの監査報告書は、AWS アーティファクトを使用してダウンロードすることができます。詳細については、「Downloading reports in AWS Artifact」を参照してください。

AWS のサービスの使用時におけるユーザーのコンプライアンス責任は、データの機密性、企業のコンプライアンス目的、適用法と規制に応じて異なります。AWS は、コンプライアンスに役立つ以下のリソースを提供しています。

- セキュリティのコンプライアンスとガバナンス – これらのソリューション実装ガイドでは、アーキテクチャ上の考慮事項について説明し、セキュリティとコンプライアンスの機能をデプロイする手順を示します。
- HIPAA 対応サービスのリファレンス – HIPAA 対応サービスの一覧が提供されています。すべての AWS のサービスが HIPAA 対象であるわけではありません。
- AWS コンプライアンスのリソース - このワークブックとガイドのコレクションは、お客様の業界や所在地に適用される場合があります。
- https://d1-awsstatic-com-whitepapers-compliance-AWS-Customer-Compliance-Guides-pdf[AWS Customer Compliance Guides] – コンプライアンスの観点から見た責任共有モデルを理解できます。このガイドは、AWS のサービスを保護するためのベストプラクティスを要約したものであり、複数のフレームワーク (米国標準技術研究所 (NIST)、ペイメントカード業界セキュリティ標準評議会 (PCI)、国際標準化機構 (ISO) など) にわたるセキュリティ統制へのガイダンスがまとめられています。
- AWS Config デベロッパーガイドの「ルールでのリソースの評価」 – AWS Config サービスは、リソースの設定が内部規定、業界のガイドライン、規制にどの程度適合しているかを評価します。

- AWS セキュリティハブ – この AWS サービスは、AWS 内のセキュリティ状態に関する包括的なビューを提供します。Security Hub では、セキュリティコントロールを使用して AWS リソースを評価し、セキュリティ業界標準とベストプラクティスに対するコンプライアンスをチェックします。サポートされているサービスとコントロールの一覧については、Security Hub のコントロールリファレンスを参照してください。
- Amazon GuardDuty – この AWS サービスは、環境をモニタリングして、疑わしいアクティビティや悪意のあるアクティビティがないか調べることで、AWS アカウント、ワークロード、コンテナ、データに対する潜在的な脅威を検出します。GuardDuty を使用すると、特定のコンプライアンスフレームワークで義務付けられている侵入検出要件を満たすことで、PCI DSS などのさまざまなコンプライアンス要件に対応できます。
- AWS Audit Manager – この AWS サービスでは、AWS の使用状況を継続的に監査し、リスクの管理方法と、規制や業界標準へのコンプライアンスの管理方法を簡素化できます。

AWS データ転送ターミナルのレジリエンス

AWS のグローバルインフラストラクチャは、AWS リージョンとアベイラビリティーゾーンを中心として構築されています。AWSリージョンには、低レイテンシー、高いスループット、そして高度の冗長ネットワークで接続されている複数の物理的に独立および隔離されたアベイラビリティーゾーンがあります。アベイラビリティーゾーンでは、ゾーン間で中断することなく自動的にフェイルオーバーするアプリケーションとデータベースを設計および運用することができます。アベイラビリティーゾーンは、従来の単一または複数のデータセンターインフラストラクチャよりも可用性、耐障害性、および拡張性が優れています。

AWS リージョンとアベイラビリティーゾーンの詳細については、「AWS グローバルインフラストラクチャ」を参照してください。

AWS データ転送ターミナルは、世界各地で利用できます。インターネットからアクセスできる任意の AWS リージョンに接続できます。

データ転送ターミナルでのログ記録とモニタリング

AWS データ転送ターミナルは、データ転送ターミナルのユーザー、ロール、または AWS サービスによって実行されたアクションを記録するサービスである AWS CloudTrail と統合されています。CloudTrail は、データ転送ターミナルへのすべての API コールをイベントとしてキャプチャします。キャプチャされる呼び出しには、データ転送ターミナルコンソールからの呼び出しと、データ転送ターミナル API オペレーションへのコード呼び出しが含まれます。証跡を作成する場合は、データ転送ターミナルのイベントなど、Amazon S3 バケットへの CloudTrail イベントの継続的な配信を

有効にすることができます。追跡を設定しない場合でも、CloudTrail コンソールのイベント履歴で最新のイベントを表示できます。CloudTrail で収集された情報を使用して、データ転送ターミナルに対するリクエスト、リクエスト元の IP アドレス、リクエスト者、リクエスト日時などの詳細を確認できます。

CloudTrail に関する詳細は、AWS CloudTrail ユーザーガイドを参照してください。

CloudTrail のデータ転送ターミナル情報

AWS アカウントを作成すると、そのアカウントに対して CloudTrail が有効になります。データ転送ターミナルでアクティビティが発生すると、そのアクティビティは [イベント履歴] の他の AWS サービスイベントとともに CloudTrail イベントに記録されます。最近のイベントは、AWS アカウントで表示、検索、ダウンロードできます。詳細については、「CloudTrail イベント履歴でのイベントの表示」を参照してください。

データ転送ターミナルのイベントなど、AWS アカウントのイベントの継続的な記録を行うには、証跡を作成します。証跡により、ログファイルを CloudTrail で Amazon S3 バケットに配信できます。デフォルトでは、コンソールで証跡を作成すると、すべての AWS リージョンに証跡が適用されます。証跡は、AWS パーティションのすべてのリージョンからのイベントを記録し、指定した Amazon S3 バケットにログファイルを配信します。さらに、CloudTrail ログで収集したイベントデータをより詳細に分析し、それに基づいて対応するため、他の AWS サービスを構成できます。詳細については、次を参照してください:

- 追跡を作成するための概要
- CloudTrail がサポートされているサービスと統合
- 「CloudTrail の Amazon SNS 通知の設定」
- 複数のリージョンから CloudTrail ログファイルを受け取るおよび複数のアカウントから CloudTrail ログファイルを受け取る

すべてのデータ転送ターミナルアクションは CloudTrail によってログに記録され、このガイドの「データ転送ターミナル API リファレンス: アクションとリソース」セクションに記載されています。

各イベントまたはログエントリには、リクエストの生成者に関する情報が含まれます。アイデンティティ情報は、以下を判別するのに役立ちます。

- リクエストが、ルートまたは AWS Identity and Access Management (IAM) ユーザーの認証情報のどちらを使用して送信されたか。

- リクエストがロールまたはフェデレーションユーザーのテンポラリなセキュリティ認証情報を使用して行われたかどうか。
- リクエストが別の AWS サービスによって行われたかどうか。

詳細については、「CloudTrail userIdentity エレメント」を参照してください。

データ転送ターミナルのログファイルエントリを理解する

「トレイル」は、指定した Amazon S3 バケットにイベントをログファイルとして配信するように設定できます。CloudTrail のログファイルは、単一か複数のログエントリを含みます。イベントは、任意の出典からの単一のリクエストを表し、リクエストされたアクション、アクションの日時、リクエストパラメータなどに関する情報が含まれます。CloudTrail ログファイルは、公開 API コールの順序付けられたスタックトレースではないため、特定の順序では表示されません。

AWS データ転送ターミナルのインフラストラクチャセキュリティ

マネージドサービスである AWS データ転送ターミナルは、{https---d0-awsstatic-com-whitepapers-Security-AWS-Security-Whitepaper-pdf}[Amazon Web Services: Overview of Security Processes] ホワイトペーパーに記載されている AWS グローバルネットワークセキュリティ手順で保護されています。

ネットワーク経由でデータ転送ターミナルにアクセスするには、AWS 発行の API コールを使用します。クライアントで Transport Layer Security (TLS) 1.0 以降がサポートされている必要があります。TLS 1.2 以降が推奨されています。また、DHE (Ephemeral Diffie-Hellman) や ECDHE (Elliptic Curve Ephemeral Diffie-Hellman) などの Perfect Forward Secrecy (PFS) を使用した暗号スイートもクライアントでサポートされている必要があります。これらのモードは Java 7 以降など、ほとんどの最新システムでサポートされています。

また、リクエストにはアクセスキー ID と、IAM プリンシパルに関連付けられているシークレットアクセスキーを使用して署名する必要があります。または、AWS Security Token Service (AWS STS) で一時的なセキュリティ認証情報を生成して、リクエストに署名することもできます。

データ転送ターミナルユーザーガイドのドキュメント履歴

次の表は、このガイドのドキュメント履歴をまとめたものです。

変更	説明	日付
レイアウトの更新	ドキュメントレイアウトの更新と、表現および内容の軽微な修正。	2025 年 1 月 1 日
初版発行	元のドキュメントのリリース日。	2024 年 12 月 1 日