Amazon Simple Storage Service

入門ガイド

Amazon Simple Storage Service: 入門ガイド

Table of Contents

Amazon Simple Storage Service の開始方法

Amazon Simple Storage Service (Amazon S3) は、インターネット用のストレージです。Amazon S3 を使用すると、いつでもWeb上の任意の場所から、任意の量のデータを格納および取得できます。シンプルかつ直感力あるウェブインターフェイスの AWS Management Console を用いて、これらのタスクを実行することができます。

Amazon S3 は、オブジェクトとしてデータをバケットに保管します。オブジェクトは、ファイルと、そのファイルを記述する任意のメタデータです。Amazon S3 にファイルを保存するには、バケットにファイルをアップロードします。ファイルをオブジェクトとしてアップロードする際に、オブジェクトと任意のメタデータにアクセス権限を設定することができます。

バケットは、オブジェクトのコンテナです。1 つまたは複数のバケットを持つことができます。バケットごとにアクセスを制御し、バケット内のオブジェクトを作成、削除、リスト化できるユーザーを決定できます。また、Amazon S3 がバケットとそのコンテンツを保存する地理的リージョンを選択し、バケットとそのオブジェクトのアクセスログを表示することもできます。

このガイドでは、Amazon S3 を紹介し、AWS マネジメントコンソールを使用して以下のタスクを完了する方法について説明します。

Amazon S3 の機能、料金、よくある質問については、Amazon S3 製品ページを参照してください。

Amazon S3 のセットアップ

AWS にサインアップすると、Amazon S3 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。料金が発生するのは、実際に使用したサービスの分のみです。

Amazon S3 では、お支払いは実際に使用した分のみです。Amazon S3 の機能と料金の詳細については、「Amazon S3」を参照してください。Amazon S3 の新規のお客様は、Amazon S3 を無料で使い始めることができます。詳細については、「AWS 無料利用枠」を参照してください。

Amazon S3 の使用を開始するには、以下のステップに従います。

トピック

AWS にサインアップ

AWS アカウントをお持ちでない場合は、以下の手順に従ってアカウントを作成してください。

サインアップして AWS アカウントを作成するには

1. https://portal.aws.amazon.com/billing/signup を開きます。
2. オンラインの手順に従います。

   サインアップ手順の一環として、通話呼び出しを受け取り、電話のキーパッドを用いて確認コードを入力することが求められます。

AWS のサインアップ処理が完了すると、ユーザーに確認メールが送信されます。https://aws.amazon.com/ の [My Account (アカウント)] をクリックして、いつでもアカウントの現在のアクティビティを表示し、アカウントを管理することができます。

IAM ユーザーを作成する

アマゾン ウェブ サービス (AWS) アカウントを初めて作成する場合は、1 つのサインイン アイデンティティを使用します。このアイデンティティで、アカウントのすべての AWS のサービスとリソースにアクセスできます。このアイデンティティは、AWS アカウントのルートユーザーと呼ばれます。サインインするときに、アカウントの作成に使用した E メールアドレスとパスワードを入力します。

> Important
>
> 強くお勧めしているのは、日常的なタスクには、それが管理者タスクであっても、root ユーザーを使用しないことです。代わりに、最初の IAM ユーザーを作成するためにのみ、ルートユーザーを使用するというベストプラクティスに従います。その後、ルートユーザーの認証情報を安全な場所に保管し、それらを使用して少数のアカウントおよびサービス管理タスクのみを実行しま

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については、「ルートユーザー認証情報が必要なタスク」を参照してください。

AWS にサインアップしたけれど使用する IAM ユーザーをまだ作成していない場合は、次の手順に従います。

自分用の管理者ユーザーを作成し、そのユーザーを管理者グループに追加するには (コンソール)

1. [Root user (ルートユーザー)] を選択し、AWS アカウントのメールアドレスを入力して、アカウント所有者として IAM コンソールにサインインします。次のページでパスワードを入力します。

   Note

   以下の IAM の **`Administrator`** ユーザーの使用に関するベストプラクティスに従って、ルートユーザーの認証情報は安全な場所に保管しておくことを強くお勧めします。ルートユーザーとしてのサインインは、いくつかのアカウントとサービスの管理タスクの実行にのみ使用してください。
2. ナビゲーションペインで [Users]、[Add user] の順に選択します。
3. [ユーザー名] に「**`Administrator`**」と入力します。
4. [AWS Management Console access (AWS マネジメントコンソールへのアクセス)] の横にあるチェックボックスをオンにします。[Custom password (カスタムパスワード)] を選択し、その後テキストボックスに新しいパスワードを入力します。
5. (オプション) デフォルトでは、AWS は新しいユーザーの初回のサインイン時に新しいパスワードの作成を要求します。必要に応じて [User must create a new password at next sign-in (ユーザーは次回のサインイン時に新しいパスワードを作成する必要がある)] のチェックボックスをオフにして、新しいユーザーがサインインしてからパスワードをリセットできるようにできます。
6. [Next: Permissions (次へ: アクセス許可)] を選択します。
7. [Set permissions (アクセス許可の設定)] で、[Add user to group (ユーザーをグループに追加)] を選択します。
8. [Create group] を選択します。
9. [グループの作成] ダイアログボックスで、[グループ名] に「**`Administrators`**」と入力します。
10. [Filter policies (フィルタポリシー)] を選択し、[AWS managed -job function (AWS 管理ジョブ機能)] を選択して、表の内容をフィルタリングします。
11. ポリシーリストで、[AdministratorAccess] のチェックボックスをオンにします。次に、[Create group] を選択します。

    Note

    `AdministratorAccess` アクセス許可を使用して AWS の請求およびコスト管理コンソールにアクセスするには、IAM ユーザーと IAM ロールの請求情報へのアクセスを有効にする必要があります。これを行うには、請求コンソールへのアクセスの委任に関するチュートリアルのステップ 1 の手順に従ってください。
12. グループのリストに戻り、新しいグループのチェックボックスをオンにします。必要に応じて [Refresh] を選択し、リスト内のグループを表示します。
13. [次へ: タグ] を選択します。
14. (オプション) タグをキー - 値のペアとしてアタッチして、メタデータをユーザーに追加します。IAM でのタグの使用の詳細については、IAM ユーザーガイドの「IAM ユーザーとロールのタグ付け」を参照してください。
15. [Next: Review] を選択して、新しいユーザーに追加するグループメンバーシップのリストを表示します。続行する準備ができたら、[Create user] を選択します。

このプロセスを繰り返して新しいグループとユーザーを作成して、AWS アカウントのリソースへのアクセス許可をユーザーに付与できます。ポリシーを使用して特定の AWS のリソースへのユーザーのアクセス

許可を制限する方法については、「AWS リソースのアクセス管理」と「IAM 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。

IAM ユーザーとしてのサインイン

IAM ユーザーを作成したら、IAM ユーザー名とパスワードを使用して AWS にサインインできます。

IAM ユーザーとしてサインインする前に、IAM コンソールで IAM ユーザーのサインインのリンクを確認できます。IAM ダッシュボードの [IAM users sign-in link (IAM ユーザーのサインインのリンク)] の下に、AWS アカウントのサインインのリンクが表示されます。サインインのリンクの URL には、ダッシュ (-) を除いた AWS アカウント ID が含まれています。

サインインのリンクの URL に AWS アカウント ID を含めたくない場合は、アカウントのエイリアスを作成します。詳細については、IAM ユーザーガイドの「AWS アカウントのエイリアスの作成、削除および一覧表示」を参照してください。

AWS ユーザーとしてサインインするには

1. AWS マネジメントコンソールからサインアウトします。
2. サインインリンクを入力します。

   サインインのリンクには、AWS アカウント ID (ダッシュを除く) または AWS アカウントのエイリアスが含まれています。

   ```
   https://aws_account_id_or_alias.signin.aws.amazon.com/console
   ```
3. 作成した IAM ユーザー名とパスワードを入力します。

   サインインすると、ナビゲーションバーに「your_user_name @ your_aws_account_id」が表示されます。

バケットの作成

AWS へのサインアップが済んだので、AWS マネジメントコンソールを使用してバケットを作成する準備が整いました。Amazon S3 のすべてのオブジェクトは、バケットに保管されます。Amazon S3 にデータを保管する前に、バケットを作成する必要があります。

> Note
>
> バケットの作成は課金対象にはなりません。バケット内にオブジェクトを保存した場合、およびバケット宛てまたはバケットからオブジェクトを転送した場合にのみ課金されます。このガイドの例に従って操作して発生する使用料はごくわずかです (1 USD 未満)。ストレージ料金の詳細については、「Amazon S3 の料金」を参照してください。

AWS コマンドラインインターフェイスを使用してバケットを作成するには、AWS CLI コマンドリファレンスの「create-bucket」を参照してください。

バケットを作成するには

1. AWS マネジメントコンソールにサインインして Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
2. [バケットを作成する] を選択します。

   [バケットを作成する] ページが開きます。
3. [バケット名] に、バケットの DNS に準拠する名前を入力します。

   バケット名には次の条件があります。

   - すべての Amazon S3 で一意にする。
   - 3～63 文字で指定する。
   - 大文字を含めないでください。
   - 先頭の文字には小文字の英文字または数字を使用する。

   バケットを作成したら、その名前を変更することはできません。バケットの名前付けについて詳しくは、 Amazon Simple Storage Service デベロッパー開発者ガイドの「バケット命名規則」を参照してください。

   > Important
   >
   > バケット名にアカウント番号などの機密情報を含めないでください。バケット名は、バケット内のオブジェクトを参照する URL に表示されます。
4. [Region (リージョン)] で、バケットを配置する AWS リージョンを選択します。

   レイテンシーとコストを最小化するため、さらに規制条件に対応するために、最寄りのリージョンを選択します。明示的に別のリージョンに移動する場合を除き、特定のリージョンに保管されたオブジェクトは、そのリージョンから移動されることはありません。Amazon S3 AWS リージョンのリストについては、AWS 全般のリファレンスの「AWS サービスエンドポイント」を参照してください。
5. [Bucket settings for Block Public Access (ブロックパブリックアクセスのバケット設定)] で、値をデフォルトのままにします。

   デフォルトでは、Amazon S3 は、バケットへのすべてのパブリックアクセスをブロックします。パブリックアクセスブロックの設定はすべて有効のままにしておくことをお勧めします。パブリックアクセスのブロックの詳細については、Amazon Simple Storage Service 開発者ガイドの「Amazon S3 パブリックアクセスブロックの使用」を参照してください。

6. [バケットを作成する] を選択します。

Amazon S3 にバケットが作成されました。

オブジェクトをバケットに追加するには、「バケットへのオブジェクトのアップロード (p. 7)」を参照してください。

バケットへのオブジェクトのアップロード

バケットを作成したので、バケットにオブジェクトをアップロードする準備が整いました。オブジェクトは、テキストファイル、写真、ビデオなど、どのような種類のファイルでも可能です。

オブジェクトをバケットにアップロードするには

1. [Buckets (バケット)] リストで、オブジェクトのアップロード先のバケットの名前を選択します。
2. バケットの [Objects (オブジェクト)] タブで、[Upload (アップロード)] を選択します。
3. [Files and Folders (ファイルとフォルダ)] で、[Add files (ファイルを追加)] を選択します。
4. アップロードするファイルを選択し、続いて [Open (オープン)] を選択します。
5. [Upload] を選択します。

オブジェクトがバケットに正常にアップロードされました。

オブジェクトを表示するには、「オブジェクトのダウンロード (p. 8)」を参照してください。

オブジェクトのダウンロード

バケットにオブジェクトをアップロードしたので、オブジェクトとローカルコンピュータにダウンロードしたオブジェクトについての情報を表示できます。

バケットからオブジェクトをダウンロードする方法

1. [バケット] リストで、作成したバケットの名前を選択します。
2. [Objects (オブジェクト)] リストで、アップロードしたオブジェクトの名前を選択します。

   オブジェクトの概要が表示されます。
3. [概要] タブで、オブジェクトに関する情報を確認します。
4. オブジェクトをコンピュータにダウンロードするには、[ダウンロード] を選択します。

オブジェクトが正常にダウンロードされました。

Amazon S3 内でオブジェクトをコピーして貼り付ける方法については、「フォルダへのオブジェクトのコピー (p. 9)」を参照してください。

フォルダへのオブジェクトのコピー

バケットにオブジェクトを追加し、そのオブジェクトをダウンロードできました。このチュートリアルでは、フォルダを作成し、そこにオブジェクトをコピーします。

オブジェクトをフォルダにコピーするには

1. [バケット] リストで、バケット名を選択します。
2. [フォルダの作成] を選択して、新しいフォルダを設定します。
   a. フォルダ名 (`favorite-pics` など) を入力します。
   b. フォルダの暗号化設定で、[なし] を選択します。
   c. [Save] を選択します。
3. コピーするオブジェクトを含む Amazon S3 バケットまたはフォルダに移動します。
4. コピーするオブジェクトの名前の左にあるチェックボックスをオンにします。
5. [Actions (アクション)] を選択し、表示されるオプションのリストから [Copy (コピー)] を選択します。

   または、右上のオプションから [Copy (コピー)] を選択します。
6. コピー先フォルダを選択します。
   a. [Browse S3 (S3 の参照)] を選択します。
   b. フォルダ名の左にあるオプションボタンを選択します。

      フォルダ内に移動し、コピー先としてサブフォルダを選択するには、フォルダ名を選択します。
   c. [コピー先の選択] を選択します。

   コピー先フォルダへのパスが [コピー先] ボックスに表示されます。[コピー先] には、s3://*bucket-name*/*folder-name*/ などコピー先のパスを入力してもかまいません。
7. 右下の [コピー] を選択します。

   Amazon S3 は、オブジェクトをコピー先フォルダに移動します。

Amazon S3 でオブジェクトとバケットを削除するには、「オブジェクトとバケットの削除 (p. 10)」を参照してください。

オブジェクトとバケットの削除

オブジェクトまたはバケットが不要になった場合は、それ以上の料金が発生しないように、オブジェクトまたはバケットを削除することをお勧めします。この開始方法のウォークスルーを演習として完了し、バケットまたはオブジェクトを使用する予定がない場合は、料金が発生しないようにバケットを削除することをお勧めします。バケットを削除する前に、バケットを空にするか、バケット内のオブジェクトを削除する必要があります。オブジェクトとバケットを削除すると、それらは使用できなくなります。

引き続き同じバケット名を使用する場合は、オブジェクトを削除するか、バケットを空にすることをお勧めしますが、バケットは削除しないでください。バケットを削除すると、その名前は再利用できるようになります。ただし、バケットを再利用する前に、別のアカウントで同じ名前のバケットが作成される可能性があります。

トピック

バケットを空にする

バケットを削除する場合は、まずバケットを空にする必要があります。これにより、バケット内のすべてのオブジェクトが削除されます。

バケットを空にするには

1. [Buckets (バケット)] リストで、空にするバケットを選択し、[Empty (空にする)] を選択します。
2. バケットを空にして、バケット内のすべてのオブジェクトを削除することを確認するには、[Empty bucket (バケットを空にする)] にバケットの名前を入力します。

   Important

   バケットを空にすると、元に戻すことはできません。バケットを空にするアクションの実行中にバケットに追加されたオブジェクトは削除されます。
3. バケットを空にしてバケット内のすべてのオブジェクトを削除するには、[Empty (空にする)] を選択します。

   [Empty bucket: Status (バケットを空にする: ステータス)] ページが開き、失敗したオブジェクトの削除と成功したオブジェクトの削除の概要を確認できます。
4. バケットリストに戻るには、[Exit (終了)] を選択します。

オブジェクトの削除

バケットからすべてのオブジェクトを空にせずに、削除するオブジェクトを選択する場合は、オブジェクトを削除できます。

1. [Buckets (バケット)] リストで、オブジェクトを削除するバケットの名前を選択します。
2. 削除するオブジェクトの名前の左にあるチェックボックスをオンにします。
3. [アクション] を選択し、表示されるオプションのリストから [削除] を選択します。

または、右上のオプションから [削除] を選択します。

4. これらのオブジェクトを削除するかどうかを確認するメッセージが表示されたら、**delete** と入力します。
5. 右下の [オブジェクトの削除] を選択すると、指定したオブジェクトが Amazon S3 によって削除されます。

バケットの削除

バケットを空にするか、バケットからすべてのオブジェクトを削除した後、バケットを削除できます。

1. バケットを削除するには、[Buckets (バケット)] リストでバケットを選択します。
2. [削除] を選択します。
3. 削除を確認するには、[Delete bucket (バケットの削除)] にバケットの名前を入力します。

   Important

   バケットを削除すると、元に戻すことはできません。バケット名は一意です。バケットを削除すると、別の AWS ユーザーがその名前を使用できます。同じバケット名を引き続き使用する場合は、バケットを削除しないでください。代わりに、バケットを空にして保管しておきます。
4. バケットを削除するには、[Delete bucket (バケットの削除)] を選択します。

Amazon S3 の使用方法については、「次のステップ (p. 12)」を参照してください。

次のステップ

上記の例で、いくつかの基本的な Amazon S3 のタスクをどのように実行するかを学びました。さらに詳しい情報は、次の Amazon S3 ガイドのいずれかを参照してください。

- Amazon S3 コンソールの使用方法の詳細については、Amazon Simple Storage Service コンソールユーザーガイド。
- Amazon S3 機能の詳細とこれらの機能をサポートするコード例については、Amazon Simple Storage Service 開発者ガイド。
- Amazon S3 REST API の詳細については、Amazon Simple Storage Service API リファレンスを参照してください。

以下のトピックでは、様々な方法で Amazon S3 の理解を深めてアプリケーションに実装できるようにします。

トピック

一般的な使用シナリオ

AWS ソリューションのサイトには、Amazon S3 を使用する多くの方法が示されています。次のリストは、それらのいくつかの方法をまとめたものです。

- バックアップおよびストレージ – 他のユーザー向けにデータのバックアップおよびストレージサービスを提供します。
- アプリケーションホスティング – ウェブアプリケーションをデプロイ、インストール、管理するサービスを提供します。
- メディアホスティング – ビデオ、写真、音楽のアップロードとダウンロードをホスティングし、高い冗長性、拡張性、可用性を備えるインフラストラクチャを構築します。
- ソフトウェア配信 – 顧客がダウンロードできるソフトウェアアプリケーションをホスティングします。

詳細については、「AWS ソリューション」を参照してください。

今後の注意事項

このセクションでは、お客様独自の Amazon S3 製品を起動する前に考慮すべきトピックを紹介します。

トピック

AWS アカウントおよびセキュリティ認証情報

サービスへのサインアップ時に、E メールアドレスとパスワードを使用して AWS アカウントを作成しました。このアドレスとパスワードは、AWS アカウントのルートユーザー認証情報となります。ベストプラクティスとして、ルートユーザーの認証情報を使用して AWS にアクセスしないでください。また、認証情報は誰にも教えないでください。代わりに、AWS アカウントにアクセスする必要のある人に対してそれぞれユーザーを作成します。まず、AWS Identity and Access Management (IAM) 管理者ユーザーを自分用に作成し、毎日の作業に使用します。詳細については、IAM ユーザーガイドの「最初の IAM 管理者のユーザーおよびグループの作成」を参照してください。次に、別のユーザー用の追加の IAM ユーザーを作成します。詳細については、IAM ユーザーガイドの「IAM が委任した最初のユーザーおよびグループの作成」を参照してください。

アカウントの所有者または管理者で、IAM についての詳細をご希望の場合は、製品の説明 (https://aws.amazon.com/iam) か、IAM ユーザーガイドの技術文書を参照してください。

セキュリティ

Amazon S3 は、Amazon S3 に保存されているデータを不正アクセスから守るための認証メカニズムを提供します。特に指定がない限り、AWS アカウントの所有者だけが、Amazon S3 にアップロードされたデータにアクセスすることができます。バケットとオブジェクトへのアクセスを管理する方法の詳細については、Amazon Simple Storage Service 開発者ガイドの「Amazon S3 の Identity and Access Management」を参照してください。

また、Amazon S3 にデータをアップロードする前に、それを暗号化することもできます。

AWS の統合

Amazon S3 は単体で、または複数の他の Amazon 製品と組み合わせて使用することができます。Amazon S3 と共に使用される一般的な製品は以下のとおりです。

- Amazon EC2
- Amazon EMR
- Amazon SQS
- Amazon CloudFront

料金

Amazon S3 でのデータの保管と転送に関する料金体系を学びます。詳細については、「Amazon S3 の料金」を参照してください。

Amazon S3 のアドバンスト機能

このガイドの例では、バケットの作成、バケットへのデータのアップロードとバケットからのダウンロード、データの移動と削除といった、基本的なタスクを実行する方法を示しています。次の表では、よく使用される Amazon S3 のアドバンスト機能をまとめています。一部、AWS マネジメントコンソールで利用できないもの、Amazon S3 API の使用が必要なものがありますのでご注意ください。すべてのアドバンスト機能とその使用方法については、Amazon Simple Storage Service 開発者ガイドで説明されています。

リンク	機能
リクエスタ支払いバケット	顧客がダウンロードしたものに支払いができるように、バケットを環境設定する方法について学びます。
Amazon S3 で BitTorrent を使用	BitTorrent (ファイル配布のためのオープンなピアツーピアプロトコル) を使用します。
バージョニング	Amazon S3 のバージョニング機能について学びます。
静的ウェブサイトのホスティング	Amazon S3 で静的 Web サイトをホストする方法を学びます。
オブジェクトのライフサイクル管理	バケットのオブジェクトのライフサイクルを管理する方法を学びます。ライフサイクルの管理には、オブジェクトの失効やアーカイブ (オブジェクトの `S3` `S3 Glacier` ストレージクラスへの移行) が含まれます。

アクセスコントロールのベストプラクティス

Amazon S3 には、さまざまなセキュリティ機能とツールが用意されています。次のシナリオは、特定のタスクを実行する場合や特定の環境で操作する場合に使用するツールや設定のガイドとして役立ちます。これらのツールを適切に適用すると、データの整合性を維持し、目的のユーザーがリソースにアクセスできるようにするために役立ちます。

トピック

新しいバケットの作成

新しいバケットを作成するときは、Amazon S3 リソースを確実に保護できるように、以下のツールと設定を適用する必要があります。

ブロックパブリックアクセス

S3 のブロックパブリックアクセスには、S3 リソースが誤って公開されないようにするための 4 つの設定が用意されています。これらの設定は、個別のアクセスポイント、バケット、または AWS アカウント全体に任意の組み合わせで適用できます。設定をアカウントに適用すると、その設定はアカウントが所有するすべてのバケットとアクセスポイントに適用されます。デフォルトでは、[Block all public access (すべてのパブリックアクセスをブロックする)] 設定が、Amazon S3 コンソールで作成された新しいバケットに適用されます。

詳細については、Amazon Simple Storage Service 開発者ガイドの「「パブリック」の意味」を参照してください。

S3 のブロックパブリックアクセス設定の制限が厳しすぎる場合は、すべてのブロックパブリックアクセス設定を無効にする代わりに、AWS Identity and Access Management (IAM) ID を使用して特定のユーザーにアクセスを許可できます。IAM ID でブロックパブリックアクセスを使用すると、ブロックパブリックアク

セス設定によってブロックされたオペレーションは、リクエストしたユーザーに特定のアクセス許可が与えられていない限り、確実に拒否されます。

詳細については、Amazon Simple Storage Service 開発者ガイドの「パブリックアクセスブロック設定」を参照してください。

IAM ID によるアクセス許可

S3 アクセスを必要とする新しいチームメンバーのアカウントを設定するときは、IAM ユーザーとロールを使用して、権限を最小限にします。また、強力な ID 基盤をサポートするために、IAM の多要素認証 (MFA) 形式を実装することもできます。IAM ID を使用すると、ユーザーに固有のアクセス許可を付与し、ユーザーがアクセスできるリソースや実行できるアクションを指定できます。IAM ID を使用すると、共有リソースにアクセスする前にログイン認証情報の入力を要求したり、単一バケット内の異なるオブジェクトにアクセス許可階層を適用するなど、機能を強化できます。

詳細については、Amazon Simple Storage サービス開発者ガイドの「例 1: バケット所有者がユーザーにバケットのアクセス許可を付与する」を参照してください。

バケットポリシー

バケットポリシーを使用すると、承認されたユーザーのみがリソースにアクセスしてアクションを実行できるように、バケットアクセスをパーソナライズすることができます。バケットポリシーに加えて、バケットレベルでブロックパブリックアクセス設定を使用して、データへのパブリックアクセスをさらに制限する必要があります。

詳細については、Amazon Simple Storage Service 開発者ガイドの「Amazon S3 でのポリシーとアクセス許可」を参照してください。

ポリシーを作成するときは、`Principal` 要素にワイルドカードを使用しないでください。ワイルドカードを使用すると、実質上すべてのユーザーが Amazon S3 リソースにアクセスできるようになるためです。バケットへのアクセスを許可されているユーザーまたはグループを明示的にリストすることをお勧めします。アクションにワイルドカードを含めるのではなく、該当する場合に特定のアクセス許可を付与します。

最小限の特権の使用をさらに強化するには、`Effect` 要素内の Deny ステートメントはできるだけ広く、Allow ステートメントをできるだけ狭く指定する必要があります。ポリシー条件ステートメントに含まれるユーザーに対して、オプトインに関するベストプラクティスを実装するには、Effect の Deny に `"s3:*"` アクションを組み合わせる方法もあります。

ポリシーが有効になる条件を指定する方法の詳細については、Amazon Simple Storage サービス開発者ガイドの「Amazon S3 条件キー」を参照してください。

VPC 設定のバケット

企業設定でユーザーを追加する場合、Virtual Private Cloud (VPC) エンドポイントを使用すると、仮想ネットワークのすべてのユーザーが Amazon S3 リソースにアクセスできます。開発者は、VPC エンドポイントを使用すると、ユーザーが接続しているネットワークに基づいて、ユーザーのグループに特定のアクセスとアクセス許可を提供できます。各ユーザーを IAM ロールまたはグループに追加する代わりに、VPC エンドポイントを使用すると、指定されたエンドポイントから発信されたリクエストではない場合にバケットアクセスを拒否できます。

詳細については、Amazon Simple Storage Service 開発者ガイドの「Amazon S3 の VPC エンドポイント用のバケットポリシーの例」を参照してください。

データの保存と共有

Amazon S3 データを保存および共有するには、次のツールとベストプラクティスを使用します。

データの完全性のためのバージョニングとオブジェクトロック

Amazon S3 コンソールを使用してバケットとオブジェクトを管理する場合は、S3 バージョニングと S3 オブジェクトロックを実装する必要があります。これらの機能により、重要なデータが誤って変更されるのを防ぎ、意図しない操作をロールバックできます。この機能は、完全な書き込みおよび実行アクセス許可を持つ複数のユーザーが Amazon S3 コンソールにアクセスする場合に特に便利です。

S3 バージョニングの詳細については、Amazon Simple Storage サービス開発者ガイドの「バージョニングの使用」を参照してください。オブジェクトロックの詳細については、Amazon Simple Storage Service 開発者ガイドの「S3 オブジェクトロックを使用したオブジェクトのロック」を参照してください。

オブジェクトのライフサイクル管理によるコスト効率の向上

ライフサイクル全体にわたって優れたコスト効率で保存できるようにオブジェクトを管理するには、ライフサイクルポリシーとオブジェクトのバージョニングを組み合わせて使用します。ライフサイクルポリシーでは、オブジェクトの存続期間中に S3 が実行するアクションを定義します。たとえば、指定した期間後にオブジェクトを別のストレージクラスに移行する、アーカイブする、削除するなどを指定いて、ライフサイクルポリシーを作成できます。共有プレフィックスまたはタグを使用することで、すべてのオブジェクトや、バケット内のオブジェクトのサブセットを対象おして、ライフサイクルポリシーを定義できます。

詳細については、Amazon Simple Storage Service 開発者ガイドの「オブジェクトのライフサイクル管理」を参照してください。

複数のオフィスでのクロスリージョンレプリケーション

異なるオフィスからアクセスされるバケットを作成する場合は、S3 クロスリージョンレプリケーションの実装を検討する必要があります。クロスリージョンレプリケーションを使用すると、すべてのユーザーが必要なリソースにアクセスでき、運用効率が向上します。クロスリージョンレプリケーションでは、異なる AWS リージョンの S3 バケット間でオブジェクトをコピーすることにより、可用性の向上を図ります。ただし、このツールを使用すると、ストレージコストが増加します。

詳細については、Amazon Simple Storage Service 開発者ガイドの「レプリケーション」を参照してください。

セキュアな静的ウェブサイトホスティングのアクセス許可

パブリックアクセス対象の静的ウェブサイトとして使用するようにバケットを設定する場合、すべてのブロックパブリックアクセス設定を無効にする必要があります。静的ウェブサイトのバケットポリシーを記述するときは、`ListObject` または `PutObject` アクセス許可を指定せず、`s3:GetObject` アクションのみを指定することが重要です。これにより、ユーザーがバケット内のすべてのオブジェクトを表示したり、独自のコンテンツを追加したりできなくなります。

詳細については、Amazon Simple Storage Service 開発者ガイドの「ウェブサイトアクセスのアクセス許可の設定」を参照してください。

Amazon CloudFront は、セキュアな静的ウェブサイトをセットアップするために必要な機能を提供します。Amazon S3 静的ウェブサイトは、HTTP エンドポイントのみをサポートしています。CloudFront は、耐久性に優れた Amazon S3 のあるストレージを使用し、HTTPS などの、追加のセキュリティヘッダーを提供します。HTTPS では、通常の HTTP 要求を暗号化し、一般的なサイバー攻撃から保護することで、セキュリティが強化されます。

詳細については、Amazon CloudFront 開発者ガイドの「安全な静的ウェブサイトの使用開始」を参照してください。

リソースの共有

特定のユーザーグループとリソースを共有するには、いくつかの方法があります。ドキュメントやその他のリソースをユーザーのグループ、部署、またはオフィス全体と共有するには、次のツールを使用できます。これらのツールはすべて同じ目的で使用できますが、ツールによって既存の設定との相性が異なる場合があります。

ユーザーポリシー

限られたユーザーのグループとリソースを共有する場合は、IAM のグループおよびユーザーポリシーを使用できます。新しい IAM ユーザーを作成するときには、グループを作成してユーザーを追加するよう求められます。ただし、グループを作成してユーザーを追加する操作は、いつでも行うことができます。これらのリソースを共有する予定のユーザーが IAM 内で既にセットアップされている場合は、これらのユーザーを共通グループに追加し、ユーザーポリシー内でそのグループとのバケットの共有を指定できます。IAM ユーザーポリシーを使用して、バケット内の個々のオブジェクトを共有することもできます。

詳細については、Amazon Simple Storage Service 開発者ガイドの「バケットの 1 つへのアクセスを IAM ユーザーに許可する」を参照してください。

アクセスコントロールリスト

原則として、アクセスコントロールには S3 バケットポリシーまたは IAM ポリシーを使用することをお勧めします。Amazon S3 アクセスコントロールリスト (ACL) は、アクセスコントロール用としては IAM より旧式のメカニズムです。S3 ACL をすでに使用していて、問題がなければ、変更する必要はありません。ただし、特定のアクセスコントロールシナリオでは、ACL を使用する必要があります。たとえば、バケット所有者がオブジェクトへのアクセス許可を付与する際に、すべてのオブジェクトがそのバケット所有者の所有ではない場合、まずオブジェクト所有者がバケット所有者にアクセス許可を付与する必要があります。このような場合の処理は、オブジェクトの ACL を使用して行います。

詳細については、Amazon Simple Storage Service 開発者ガイドの「例 3: バケット所有者が所有していないオブジェクトに対するアクセス許可をユーザーに付与する」を参照してください。

プレフィックス

バケット内の特定のリソースを共有する場合、プレフィックスを使用してフォルダレベルのアクセス許可をレプリケートできます。Amazon S3 コンソールでは、オブジェクトの共有名プレフィックスを使用してオブジェクトをグループ化する方法として、フォルダの概念がサポートされています。 その後、IAM ユーザーのポリシーの条件内でプレフィックスを指定し、そのプレフィックスに関連付けられたリソースにアクセスする明示的なアクセス許可をユーザーに付与できます。

詳細については、Amazon Simple Storage Service コンソールユーザーガイドの「S3 バケットでフォルダを使用する方法」を参照してください。

タグ付け

オブジェクトのタグ付けを使用してストレージを分類する場合、特定の値でタグ付けされたオブジェクトを指定されたユーザーと共有できます。リソースタグを使用すると、ユーザーがアクセスしようとしているリソースに関連付けられたタグに基づいて、オブジェクトへのアクセスを制御できます。これを行うには、IAM ユーザーポリシー内で `ResourceTag/key-name` 条件を使用して、タグ付きリソースへのアクセスを許可します。

詳細については、IAM ユーザーガイドの「リソースタグを使用した AWS リソースへのアクセスの制御」を参照してください。

データの保護

転送中および保管時のデータを保護するには、次のツールを使用します。どちらのツールも、データの完全性とアクセシビリティを維持するために重要です。

オブジェクト暗号化

Amazon S3 には、転送中および保管時のデータを保護するために使用できる、複数のオブジェクト暗号化オプションがあります。サーバー側の暗号化では、オブジェクトをデータセンター内のディスクに保存する前に暗号化し、オブジェクトをダウンロードするときに復号します。リクエストが認証され、お客様がアクセス許可を持っていれば、オブジェクトが暗号化されているかどうかに関係なく同じ方法でアクセ

スできます。サーバー側の暗号化をセットアップする場合には、相互に排他的なオプションが 3 つあります。

- Amazon S3 が管理するキー (SSE-S3)
- AWS Key Management Service (SSE-KMS) に保存されているカスタマーマスターキー (CMK)
- 顧客提供のキー (SSE-C)

詳細については、Amazon Simple Storage Service 開発者ガイドの「サーバー側の暗号化を使用したデータの保護」を参照してください。

クライアント側の暗号化では、Amazon S3 に送信する前にデータを暗号化します。詳細については、Amazon Simple Storage Service 開発者ガイドの「クライアント側の暗号化を使用したデータの保護」を参照してください。

署名方法

署名バージョン 4 は、HTTP で送信される AWS リクエストに認証情報を追加するプロセスです。セキュリティ対策として、AWS へのほとんどのリクエストにはアクセスキーによる署名が必要です。アクセスキーは、アクセスキー ID とシークレットアクセスキーで構成されます。これらの 2 つのキーは、一般的にセキュリティ認証情報と呼ばれます。

詳細については、「リクエストの認証 (AWS 署名バージョン 4)」および「署名バージョン 4 の署名プロセス」を参照してください。

ログ記録とモニタリング

モニタリングは、マルチポイント障害が発生した場合に簡単にデバッグできるように、Amazon S3 ソリューションの信頼性、可用性、パフォーマンスを維持するうえで重要な部分です。ログ記録は、ユーザーが受け取るエラーの内容や、いつどのようなリクエストが行われたかを把握するために使用できます。AWS には、Amazon S3 リソースをモニタリングするためのツールがいくつか用意されています。

- Amazon CloudWatch
- AWS CloudTrail
- Amazon S3 アクセスログ
- AWS Trusted Advisor

詳細については、Amazon Simple Storage Service 開発者ガイドの「Amazon S3 でのログ記録とモニタリング」を参照してください。

Amazon S3 は、Amazon S3 のユーザー、ロール、または AWS の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。この機能は、CloudTrail 管理イベントと CloudTrail S3 データイベントを分析して Amazon S3 リソースに対する脅威をモニタリングする Amazon GuardDuty と組み合わせることができます。これらのデータソースでは、さまざまな種類のアクティビティについてモニタリングが行われます。たとえば、S3 に関連する CloudTrail 管理イベントには、S3 プロジェクトをリストまたは設定するオペレーションが含まれます。GuardDuty は、すべての S3 バケットに関する S3 データイベントを分析し、悪意のあるアクティビティや疑わしいアクティビティがないかをモニタリングします。

詳細については、Amazon GuardDuty ユーザーガイドの「Amazon GuardDuty での Amazon S3 の保護」を参照してください。

開発リソース

お客様が選択した言語を使用してアプリケーションを構築できるよう、以下のリソースを提供しています。

- サンプルコードとライブラリ – AWS デベロッパーセンターに、Amazon S3 用のサンプルコードとライブラリが用意されています。

  これらのサンプルコードを、Amazon S3 API の実装方法を理解する教材としてご利用いただけます。詳細については、AWS デベロッパーセンターを参照してください。
- チュートリアル – リソースセンターには、他の Amazon S3 チュートリアルが用意されています。

  Amazon S3 の機能を学習するための演習にご利用ください。詳細については、「記事 & チュートリアル」を参照してください。
- カスタマーフォーラム – Amazon S3 フォーラムをぜひご覧ください。他のユーザーがどのような使い方をしているのかを把握し、他のユーザーからの質問を参考にすることができます。

  このフォーラムは、Amazon S3 を使用して何ができるのか、何ができないのかを理解するのに役立ちます。フォーラムはまた、あなたが質問できる場でもあり、他のユーザーや AWS 担当者がそれに答えてくれるかもしれません。サービスや API に関する問題を報告するのにフォーラムを利用することもできます。詳細については、「ディスカッションフォーラム」を参照してください。

リファレンスリソース

以下のリストは、Amazon S3 の理解を深めるために使用できるその他のリソースです。

- Amazon Simple Storage Service コンソールユーザーガイドでは、Amazon S3 に関連する AWS マネジメントコンソールのすべての機能について説明しています。
- このAmazon Simple Storage Service 開発者ガイドは、本サービスを詳しく解説したものです。

  アーキテクチャの概要、概念の詳しい説明、API の使用手順などが含まれます。
- Amazon Simple Storage Service API リファレンスでは、Amazon S3 のアクションとパラメータについて詳しく説明しています。
- Service Health Dashboardでは、Amazon S3 のウェブサービスのステータスを見ることができます。

  ダッシュボードには、Amazon S3 (および他のすべての AWS 製品) が正しく機能しているかどうかが表示されます。詳細については、「サービスヘルスダッシュボード」を参照してください。

本ガイドについて

本ガイドは、Amazon Simple Storage Service 入門ガイドです。

このガイドでは、「Amazon Simple Storage Service」を「Amazon S3」と表記することがあります。 その場合も、すべての著作権および法的保護が適用されます。