ONION-object 入門 講習会資料

ONION-object

=簡易操作手順書=

2021 年 12 月

Cloudian 株式会社

目次

はじめに

ONION は、大阪大学サイバーメディアセンターが提供するストレージサービスです。
ONION-object は、同サービスの中で S3 API に対応したストレージサービスを提供するサブシステムで、Cloudian HyperStore を採用しています。

ONION の概要や利用方法について知りたい方は、下記の URL を参照ください。
http://www.hpc.cmc.osaka-u.ac.jp/onion/
ONION-object の利用申請や問い合わせは、下記の URL を参照ください。
http://www.hpc.cmc.osaka-u.ac.jp/service/onion-form/

ONION-object で採用している、Cloudian HyperStore（以降、HyperStore）はオブジェクトストレージと呼ばれるカテゴリーに属する製品です。オブジェクトストレージは、従来型ストレージ（NAS など）にはない、高い拡張性を有するだけではなく、ファイル（以降、オブジェクト）を安全に保護・格納する多くの仕組みが実装されており、安心してご利用頂くことが出来ます。

HyperStore はクラウドストレージの標準とも言える、AWS S3 の API と高い互換性を有しており、AWS S3 API に対応した様々なクライアントアプリケーションを介して、オブジェクトの操作を行うことが出来ます。

S3 API クライアントアプリケーションの例： AWS CLI や AWS SDK

又、S3 API の他に、Admin API（管理者用の API）が具備されており、管理者は、グループ、ユーザの管理等を API 経由で行うことも出来ます。

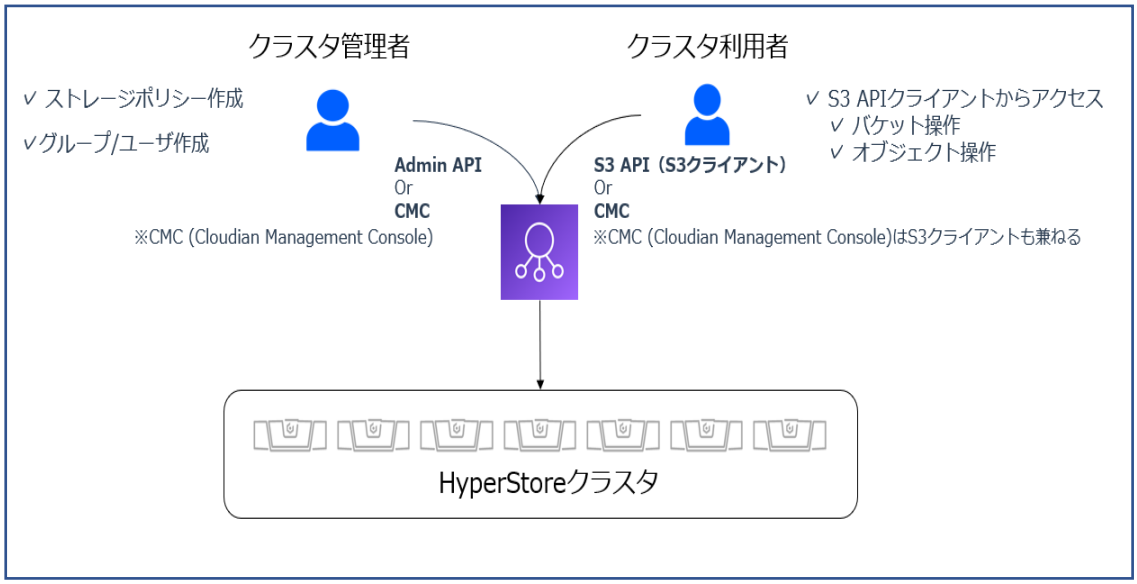
HyperStore が正常にインストールされると、Cloudian Management Console（以降、CMC）を利用することが出来ます。

CMC は Web GUI を提供、管理者は、直感的にクラスタの管理、グループ/ユーザの管理（作成/削除）を行うことが出来ます。又、CMC は簡易的な S3 API クライアント機能を併せて具備しており、ユーザは GUI 経由でオブジェクトのアップロード/ダウンロードを行うことが出来ます。

HyperStore がサポートする S3 API の使い方などは、下記を参照ください。
http://www.hpc.cmc.osaka-u.ac.jp/system/manual/onion-use/

各種 API の詳細な内容については、管理者ガイドに記載されています。管理者ガイドは下記の URL をご参照ください。
http://www.hpc.cmc.osaka-u.ac.jp/wp-content/uploads/2021/10/HyperStoreAdminGuide_v-7.2.3.pdf

HyperStore アクセスイメージ図



[補足]

・HyperStore には IP ネットワーク（HTTP[s]）経由でアクセスします。

・クラスタ利用者（ユーザ）は、HyperStore に「バケット」と呼ばれるオブジェクトの格納先（フォルダみたいなもの）を作成し、オブジェクト操作を実施します。

■■■ S3 API アクセス

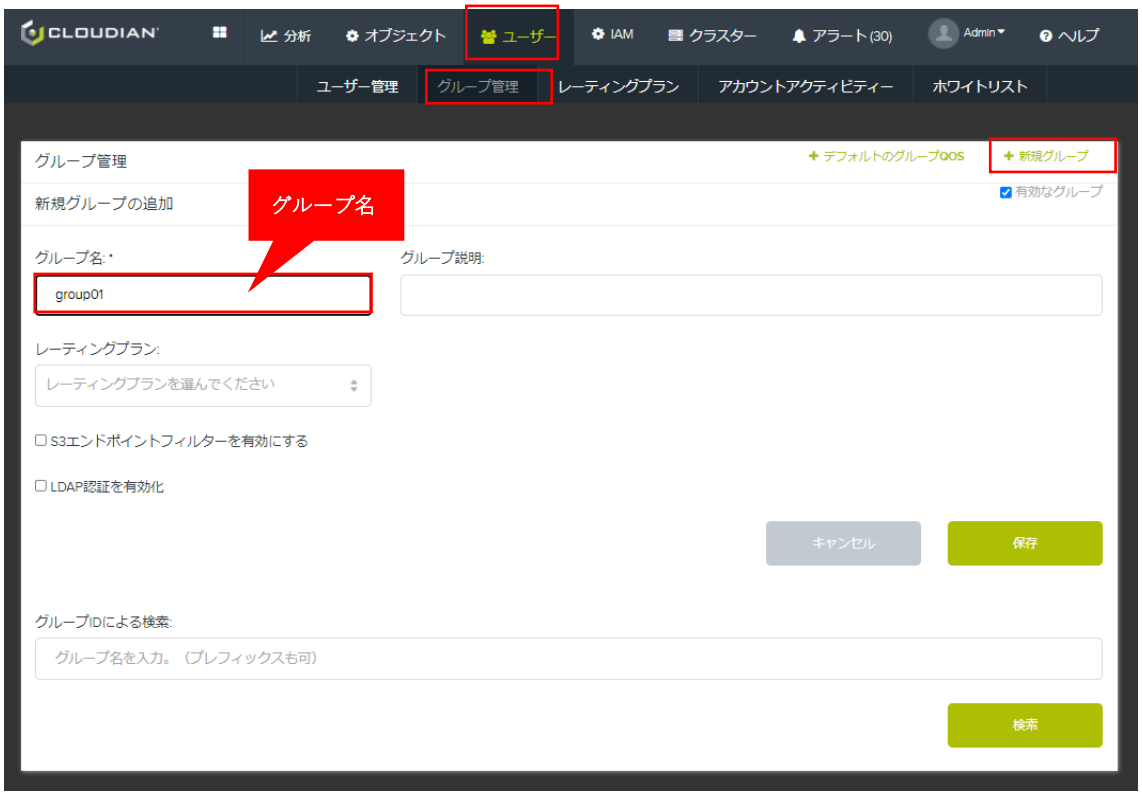
■■ グループ作成

グループはテナントとも呼ばれます。グループを作成することで、HyperStore を論理的に区分けしてご利用頂くことが出来ます。

■CMC に admin（もしくは admin 権限付与ユーザ）でログイン

※ グループ作成は、システム管理者にて実施します。

■グループ作成

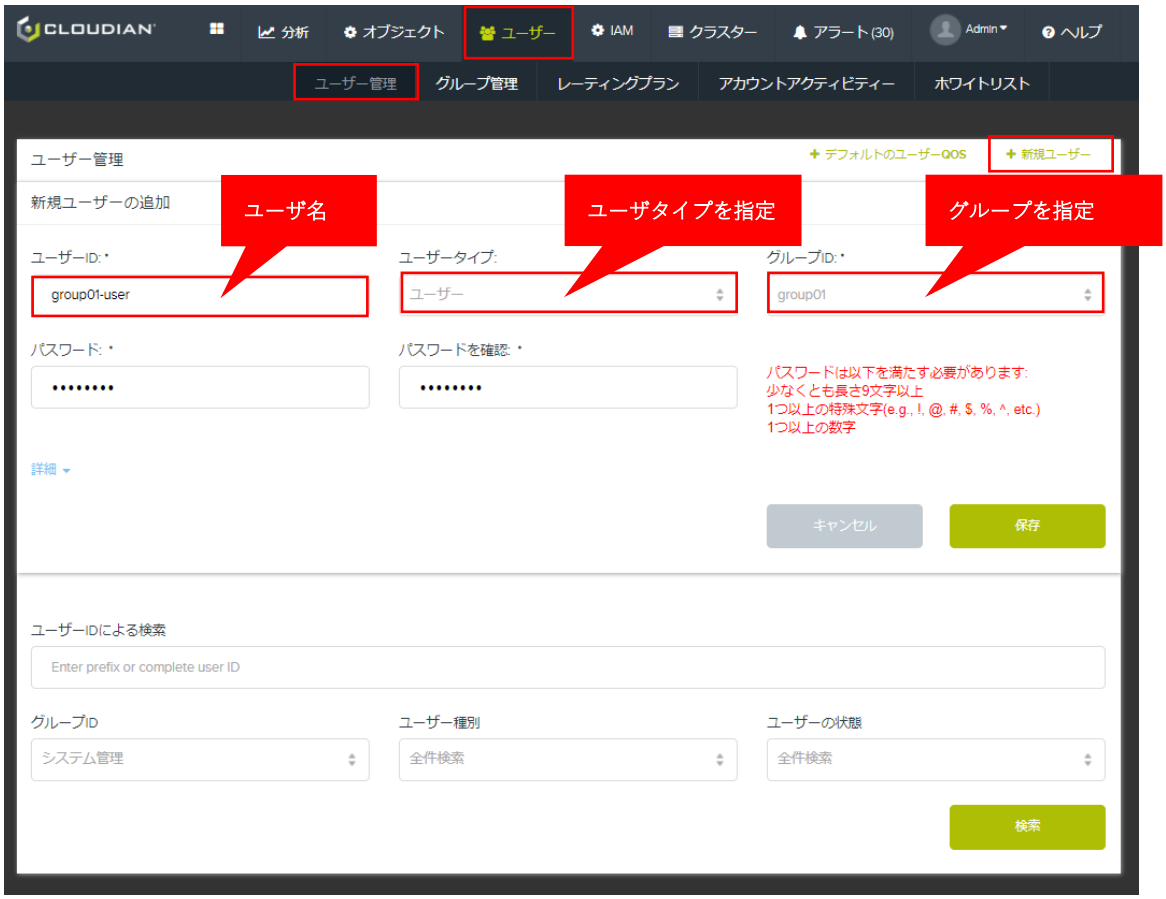


■■ ユーザ作成

■CMC にグループ管理権限でログイン

https://onionportal.hpc.cmc.osaka-u.ac.jp:8443/

■グループを指定し、ユーザを作成

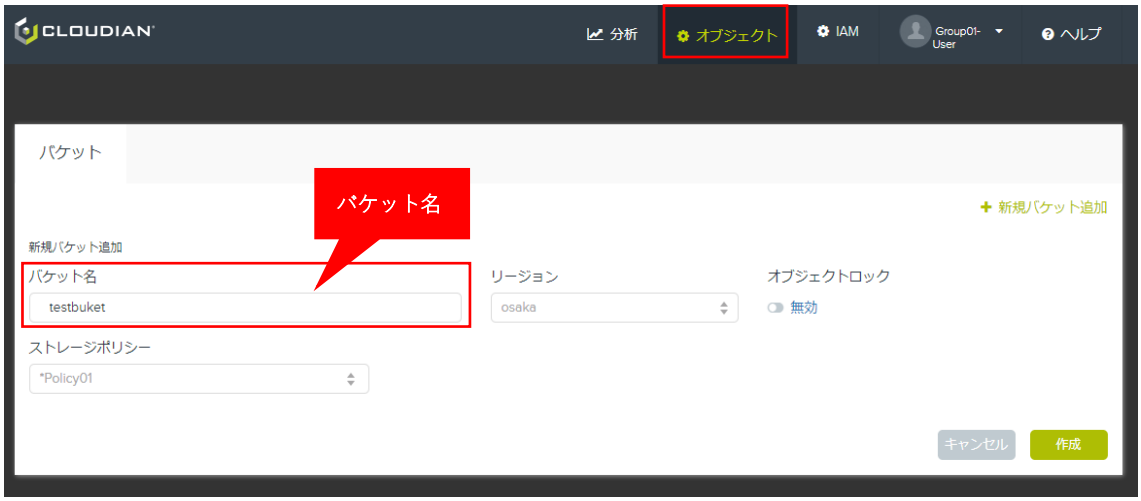


■■ S3 API アクセス（CMC を利用する場合）

■CMC にユーザでログイン

https://onionportal.hpc.cmc.osaka-u.ac.jp:8443/

■バケットの作成



・作成後、作成済みのバケット一覧が表示されます

・バケットをクリックすると、当該バケットに対してオブジェクト操作が出来ます。

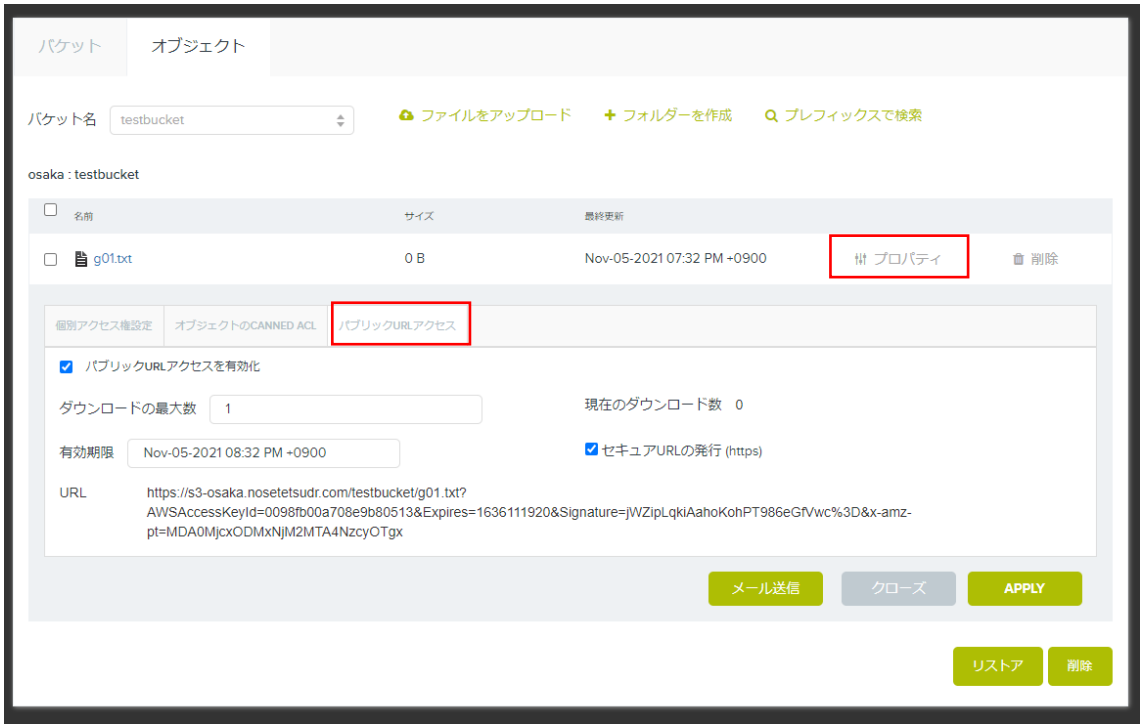
■オブジェクト操作

バケットに対してオブジェクトのアップロード、削除操作等が可能です。

■オブジェクト操作（その他）

オブジェクトは各々プロパティを有しており、個別にアクセス権の設定等が可能です。

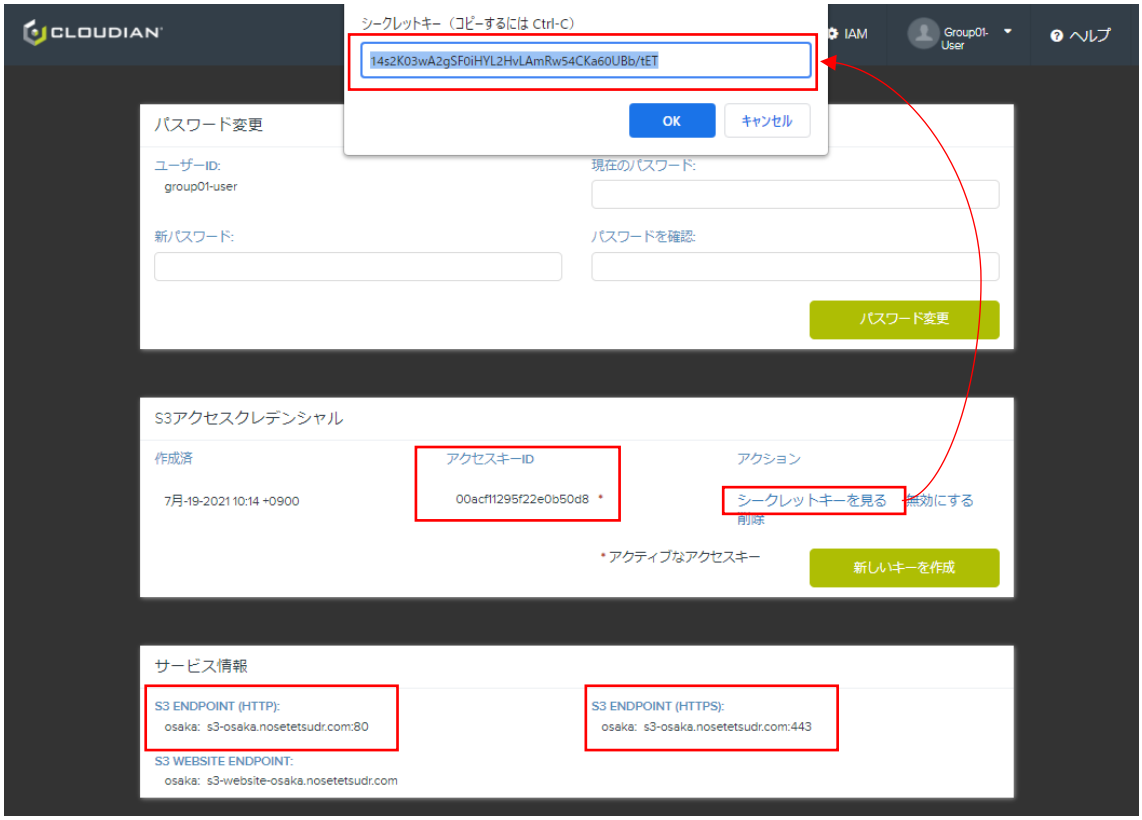
下記は、オブジェクトに対して、URL を発行する例です。データ共有したい相手に URL を送付することで、データ共有（URL からダウンロード）することが出来ます。



■Access Key / Secret Key と S3 API エンドポイントの確認

CMC ではなく、S3 API に対応しているクライアントから S3 API にアクセスするには Access key / Secret Key、S3 API エンドポイントの情報が必要です。

これらの情報は、CMC から確認することが出来ます。



・Access Key と Secret Key はユーザ毎に払い出されます。

・Access Key と Secret Key、S3 API エンドポイントをメモしてください。

■■ AWS CLI 導入　// Ubuntu の例

公式ドキュメント
https://docs.aws.amazon.com/cli/latest/userguide/install-cliv2-linux.html#cliv2-linux-prereq

■インストール

```
$ curl "https://awscli.amazonaws.com/awscli-exe-linux-x86_64.zip" -o "awscliv2.zip"
$ unzip awscliv2.zip
$ sudo ./aws/install
$ aws --version
```

■初期設定

```
$ aws configure
AWS Access Key ID [None]: 00acf11295f22e0b50d8
AWS Secret Access Key [None]: 14s2K03wA2gSF0iHYL2HvLAmRw54CKa60UBb/tET
Default region name [None]:osakau
Default output format [None]: json
```

■■ S3 API アクセス（AWS CLI を利用する場合）

■バケット作成

・バケット test000 を作成

```
$ aws s3 --endpoint-url https://s3-osakau.oniongw.hpc.cmc.osaka-u.ac.jp mb s3://test000
```

■バケット確認（リスト ）

```
$ aws s3 --endpoint-url https://s3-osakau.oniongw.hpc.cmc.osaka-u.ac.jp ls
```

■オブジェクト（ファイル）アップロード

・ローカルディレクトの test.log をバケット test000 にアップロード

```
$ aws s3 --endpoint-url https://s3-osakau.oniongw.hpc.cmc.osaka-u.ac.jp cp test.log
```

■バケット内のオブジェクト確認（リスト）

・バケット test000 内のオブジェクトをリスト

```
$ aws s3 --endpoint-url https://s3-osakau.oniongw.hpc.cmc.osaka-u.ac.jp ls s3://test000
```

=補足=
オブジェクトストレージには「フォルダ」という概念がありません。
※管理上フォルダを作成する必要がある場合は、（aws s3 コマンドでは作成できないため）下記の s3 api を利用、もしくは CMC、その他アプリケーション（Cloud Berry など）をご利用下さい。

■s3 api の利用例（フォルダ作成例）

・バケット test000 内にフォルダ folder を作成する

```
$ aws s3api put-object --bucket test000 --key "folder/" ¥
                --endpoint-url https://s3-osakau.oniongw.hpc.cmc.osaka-u.ac.jp
```

■AWS s3 コマンド

コマンド	説明
aws s3 ls	バケットの一覧を表示する
aws s3 ls s3://{バケット名}/{パス}	バケットの内容を表示する
aws s3 mb s3://{バケット名}	バケットを作成する
aws s3 rb s3://{バケット名}	バケットを削除する(空でない場合は削除されない)
aws s3 rb s3://{バケット名} –force	バケットを削除する(空でなくても削除される)
aws s3 sync {フォルダパス} s3://{バケット名}/{パス}	バケットの内容をローカルのフォルダと同期する(追加・更新のみで削除されない)
aws s3 sync {フォルダパス} s3://{バケット名}/{パス} --delete	バケットの内容をローカルのフォルダと同期する(削除もされる)
aws s3 cp {ファイルパス} s3://{バケット名}/{パス}	ローカルのファイルをバケットにコピーする
aws s3 mv {ファイルパス} s3://{バケット名}/{パス}	ローカルのファイルをバケットに移動する
aws s3 rm s3://{バケット名}/{ファイルパス}	バケットのファイルを削除する
aws s3 rm s3://{バケット名}/{フォルダパス} --recursive	バケットのフォルダを削除する

※AWS マニュアル

https://docs.aws.amazon.com/ja_jp/cli/latest/userguide/cli-services-s3-commands.html#using-s3-commands-managing-objects-param

■■■ S3 API クライアント（その他フリーソフト）

S3 API を介してオブジェクト/バケット操作ができる無料ソフトウェアが存在します。
ここでは、いくつかのソフトウェアを紹介します。
詳細にご興味がある方は、Google で検索してください。製品情報だけでなく利用法など多くのコンテンツが存在します。、

■■ CloudBerry (Windows/Mac)

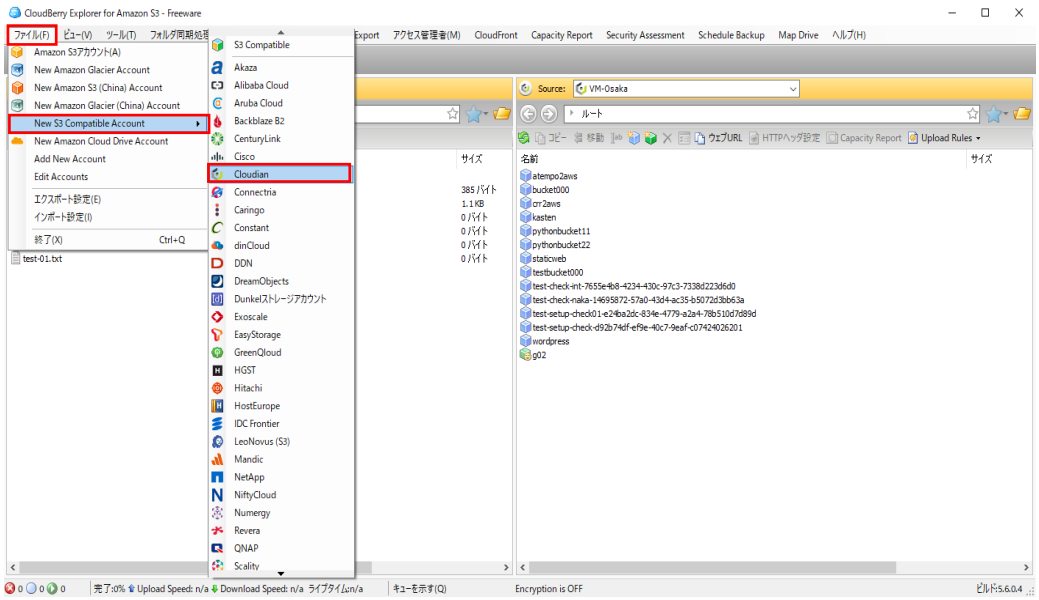
ダウンロードサイト
https://www.msp360.com/explorer/windows/amazon-s3.aspx

■インストール

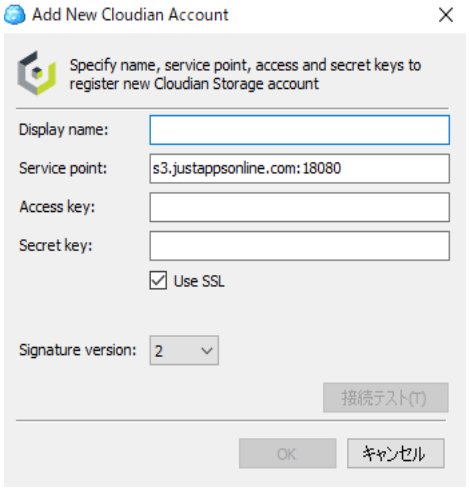
インストーラを上記からダウンロード、手順に沿ってインストールして下さい。

■Cloudian HyperStore の登録

・起動後、メニュー[ファイル]-[New S3 Compatible Account]-[Cloudian]を
アクセス先として選択



・選択後、アクセス登録に必要な情報を入力

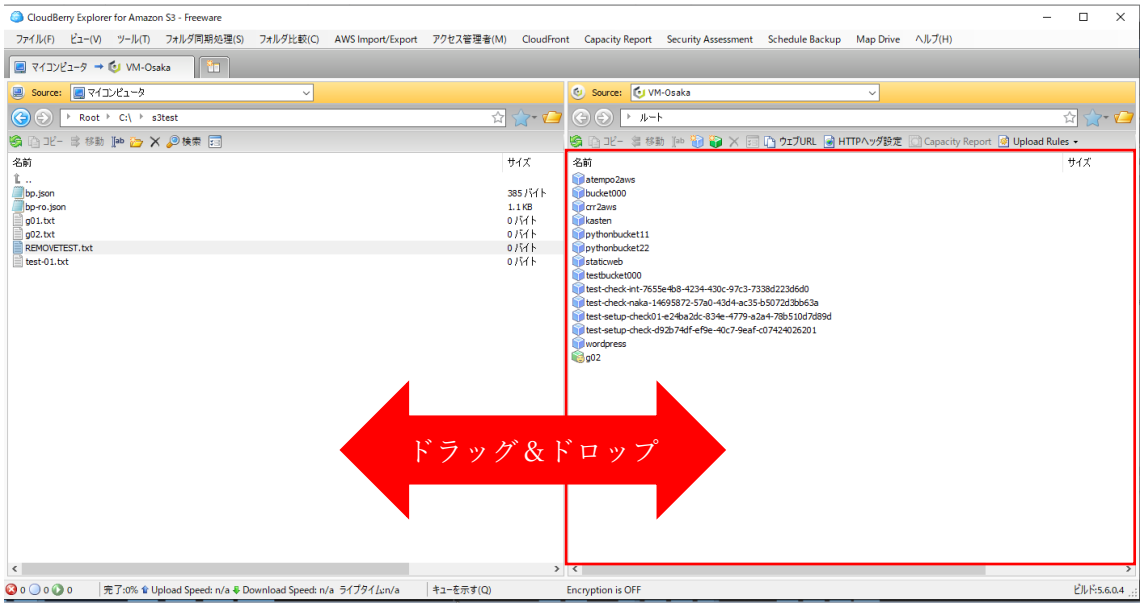


表示名
HyperStore の S3 API エンドポイント
（s3-osakau.oniongw.hpc.cmc.osaka-u.ac.jp）
アクセスキー
シークレットキー
SSL 通信か否かの選択（チェック）

■バケット/オブジェクト操作

登録が完了すると、右ペインにユーザ所有のバケットが表示されます。
以下のような操作を直感的に行うことができます。

・ローカルディスクからオブジェクトのアップロード/ダウンロード
・バケットの作成/削除
・ACL 更新
など



■■ S3 Browser (Windows)

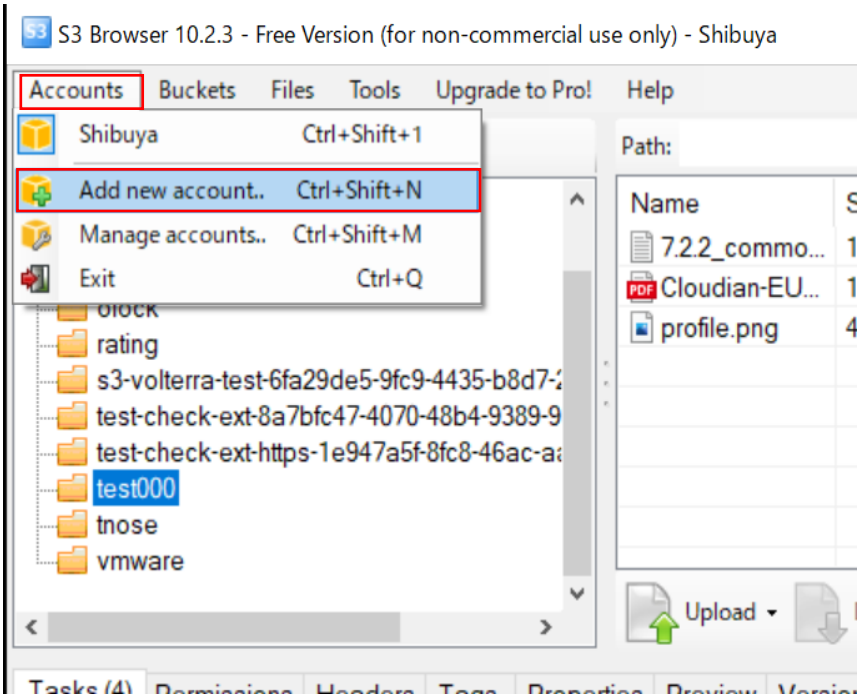
ダウンロードサイト
https://s3browser.com/

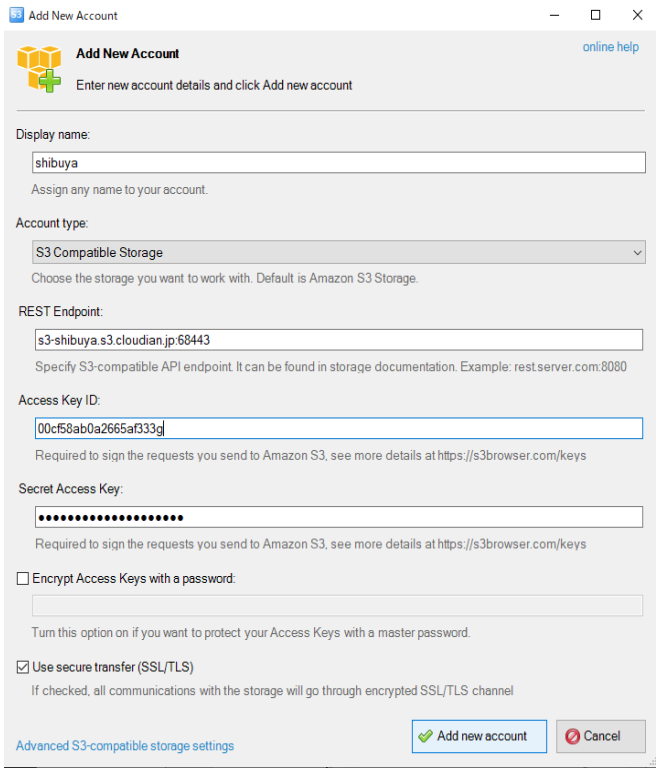
■インストール

インストーラを上記からダウンロード、手順に沿ってインストールして下さい。

■Cloudian HyperStore の登録

・起動後、メニュー[Account]-[Add new account]-[New S3 Compatible Account]-[Cloudian]をアクセス先として選択





表示名

S3 Compatible Storage

HyperStore の S3 API エンドポイント
(s3-osakau.oniongw.hpc.cmc.osaka-u.ac.jp)

アクセスキー

シークレットキー

SSL 通信か否かの選択
(チェック)

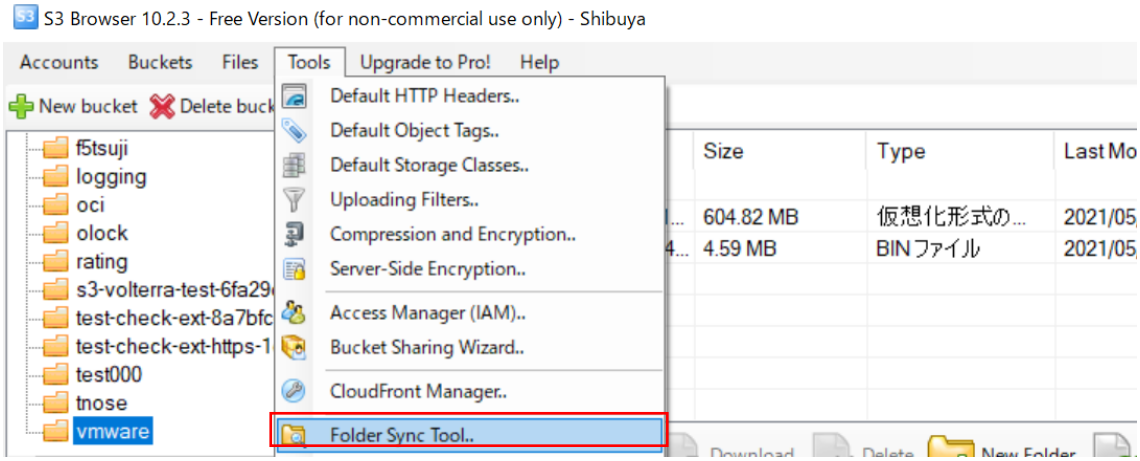
■バケット/オブジェクト操作

登録が完了すると、左ペインにユーザ所有のバケットが表示されます。
以下のような操作を直感的に行うことができます。

・ローカルディスクからオブジェクトのアップロード/ダウンロード
・バケットの作成/削除
・ACL 更新
など

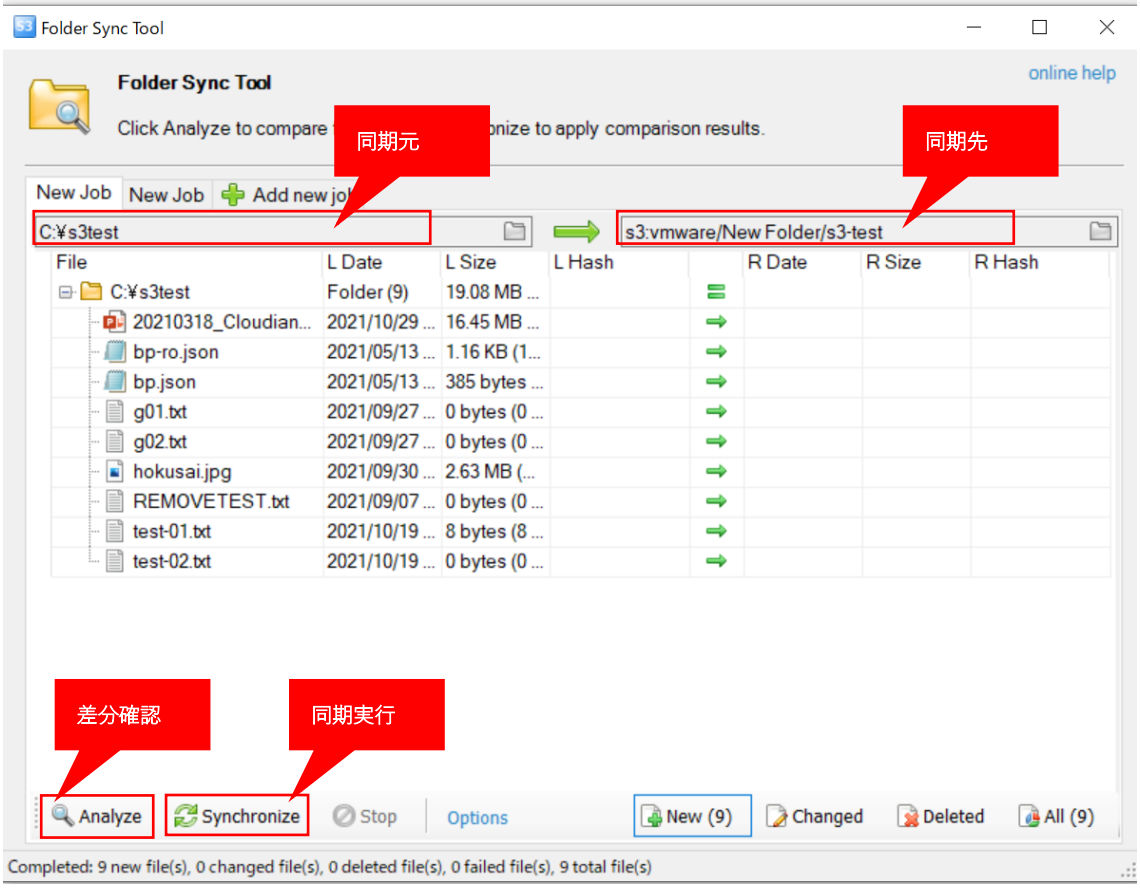
★便利な機能として「Folder Sync Tool」があります。
この機能を使うとローカルディスクのオブジェクトを HyperStore に定期的に同期してくれます。

・メニュー[Tools]-[Folder Sync Tool]を選択



・同期元（ローカルディスク）と同期先（HyperStore）を指定する

・[Analyze]で差分を確認、[Synchronize]で同期が開始される



■■ Rclone (Linux/Windows/Mac)

■インストール

```
sudo curl https://rclone.org/install.sh | sudo bash
```

■設定ファイルの編集

・HOME ディレクトリ配下に設定ファイル(rclone.conf)が配備されているので編集します。

```
sudo vi /home/tnose/.config/rclone/rclone.conf
```

・編集（追加）内容は下記の通りです。
Access key、Secret key、Endpoint はご自身の環境に置き換えて下さい

```
[cloudian01]
type = s3
provider = Other
env_auth = false
access_key_id = 00cf58ab0a3333af333f
secret_access_key = 0F75NRPLQV33333p1RfKGjF92urQ8zLXjC8Hvh1k
endpoint = https://s3-osakau.oniongw.hpc.cmc.osaka-u.ac.jp
#location_constraint = region1
acl = private
```

■設定動作確認（バケットの表示）

```
$ rclone lsd cloudian01:
          -1 2021-05-20 18:48:25        -1 7.2.3
          -1 2021-11-07 20:09:21        -1 bucket000
          -1 2021-09-26 17:38:29        -1 ccpe
          -1 2021-06-04 02:00:50        -1 logging
          -1 2021-10-27 21:48:57        -1 oci
          -1 2021-11-02 21:28:07        -1 olock
```

■バケット/オブジェクト操作

Rclone は AWS, GCP, Oracle Cloud, BOX, DropBox, Google Drive, Nextcloud など多くのクラウドストレージに対応、これらのストレージ間でデータのコピーや同期を行うことが出来ます。

・Rclone コマンド一覧
https://rclone.org/commands/

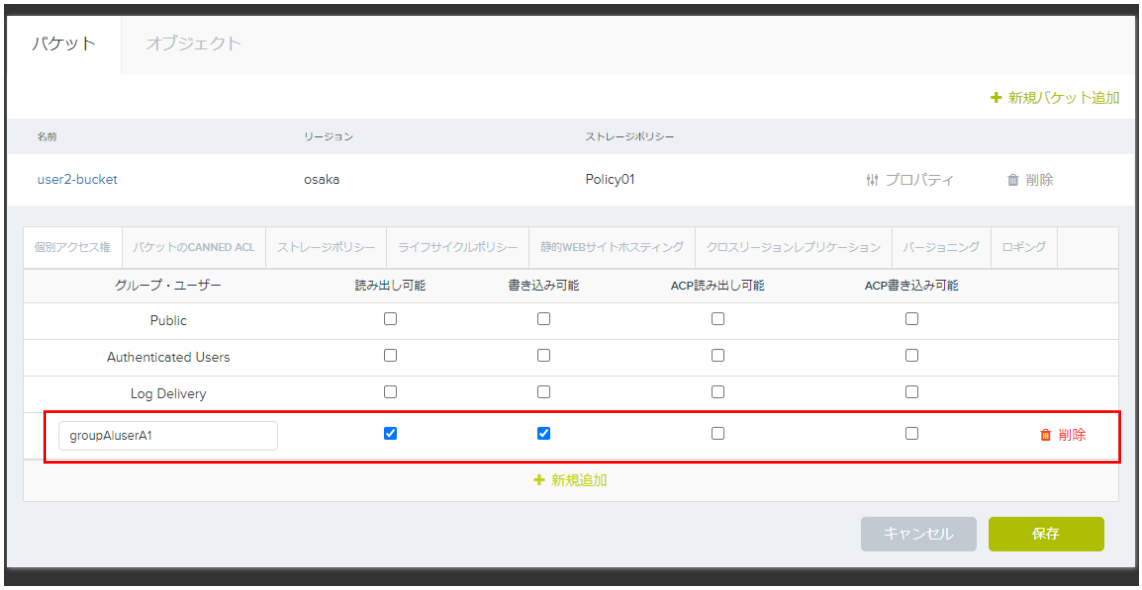
■■■ その他バケットに対して設定可能な項目（CMC）

バケット毎にバケットのプロパティを介して、各種個別設定ができます。
代表的な機能（青枠）をいくつかご紹介します。

■■ 個別アクセス権

Public/Authenticated Users/個別グループ・ユーザに対して当該バケットに対するアクセス権の設定ができます。

・“ACP”というの ACL へのアクセス権です。
・Authenticated Users というのは、CMC に登録されている全ユーザです。
・特定グループ/ユーザ毎に対して設定する場合は、+新規追加で対応できます。
例）groupA の userA1 に読み書きアクセス権を設定する場合
groupA|userA1



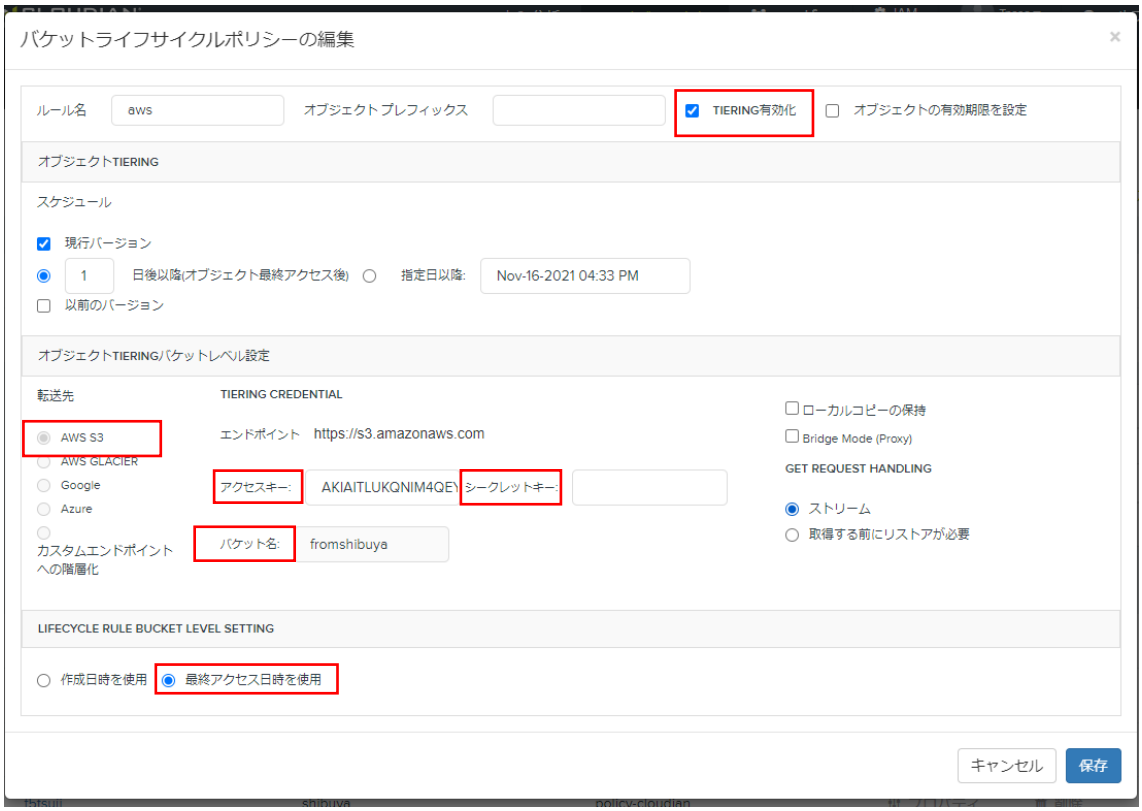
※バケットに設定を施しても、バケットに格納されるオブジェクトには反映（引継ぎ）されません。これは AWS S3 でも同様です。

■■ ライフサイクルポリシー（オブジェクト階層化）　★要ライセンス機能

バケットに格納されているオブジェクトをポリシーに沿って、各種クラウドサービスに階層化（オブジェクトを指定したクラウドサービスに移動）することが出来ます。

★ライセンス機能の為、管理者がクラスタに対して階層化機能を有効化しておく必要あり。
・階層化先は AWS/Azure/GCP だけでなく、OCI など S3 互換ストレージも指定できます。
・S3 クライアントからは、HyperStore 経由で透過的にオブジェクト操作が可能です。
・オブジェクトのメタデータは HS 側に保持されます。
・階層化されたオブジェクトはクラウドサービスから読み出し可能です。（Read Only）
※クラウドサービス側で上書き、削除は行わないでください。

例）最終アクセス日から 1 日経過したオブジェクトを AWS S3 に階層化する



階層化されたオブジェクトは下記のようにイメージアイコンが変化します。

■■ バージョニング

バケット毎に有効化することが出来ます、有効化することにより更新前のオブジェクトが保持されます。

・削除したオブジェクトについても（内部的に）保持されます。
・更新/削除前のオブジェクトは全て保持されます。
・上記により、誤って削除/更新したオブジェクトを復元することが出来ます。
・差分保持ではない為（オブジェクトそのものを保持する為）容量を消費します。

例）バージョンを有効化した場合
　　「バージョンを表示」をリックすることで過去のバージョンが表示されます、

下記のように（赤枠のように）過去のバージョンが表示されます。クリックするとダウンロードが出来ます。

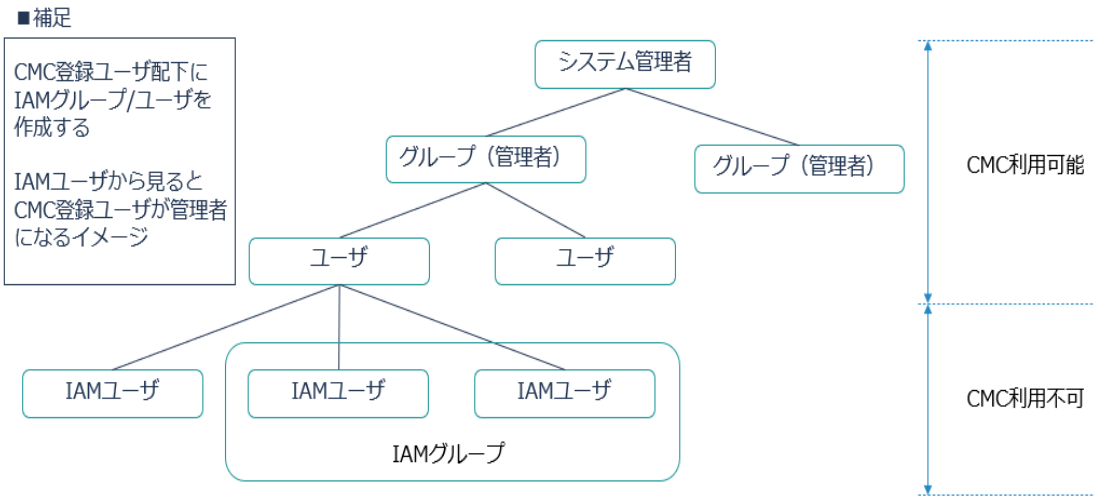
最新のオブジェクトを削除した場合、以下（赤枠）のように「ディレートマーカ」が付与されるだけで（S3 クライアントからは見えなくなるだけで）、実体（青枠）は保持されています。

■■■ IAM（AWS Identity and Access Management）概要

HyperStore では、IAM API をサポートしています。IAM グループ、ユーザを作成、IAM ポリシーに則したアクセスコントールが可能になります。
※一部対応していない API もあります。詳細はマニュアルをご参照下さい。

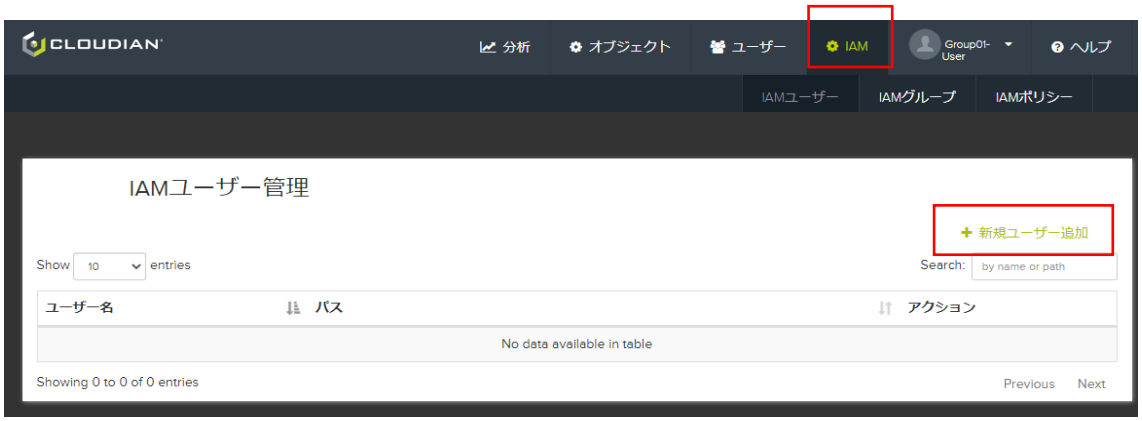
尚、IAM ユーザは CMC を介したバケット/オブジェクトが出来ないため、CMC 以外の S3 クライアント（本ドキュメントで紹介している AWS CLI など）からの利用が前提となります。

下記は HyperStore における、CMC グループ/ユーザと IAM グループ/ユーザの相関図です。



■■ IAM グループ/ユーザ/ポリシー作成

CMC ユーザでログイン後、メニュー「IAM」から「ユーザ」「グループ」「ポリシー」が作成できます。下記はサブメニューで、「ユーザ」を選択した際の画面です。
「＋新規ユーザ追加をクリック」するとユーザを作成できます。
※同様に、「グループ」「ポリシー」も作成可能



■■ IAM ユーザキーの作成

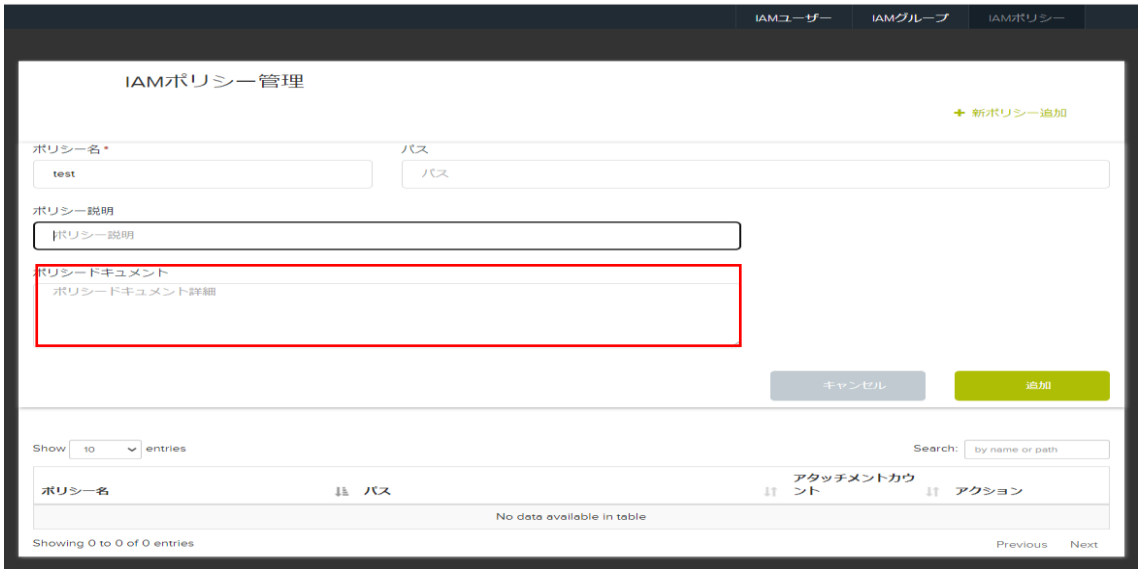
IAM ユーザ毎に Access key / Secret Key を作成します。
作成済みのユーザをクリックすると、下記画面に遷移して発行できます。

■■ IAM ポリシーの作成

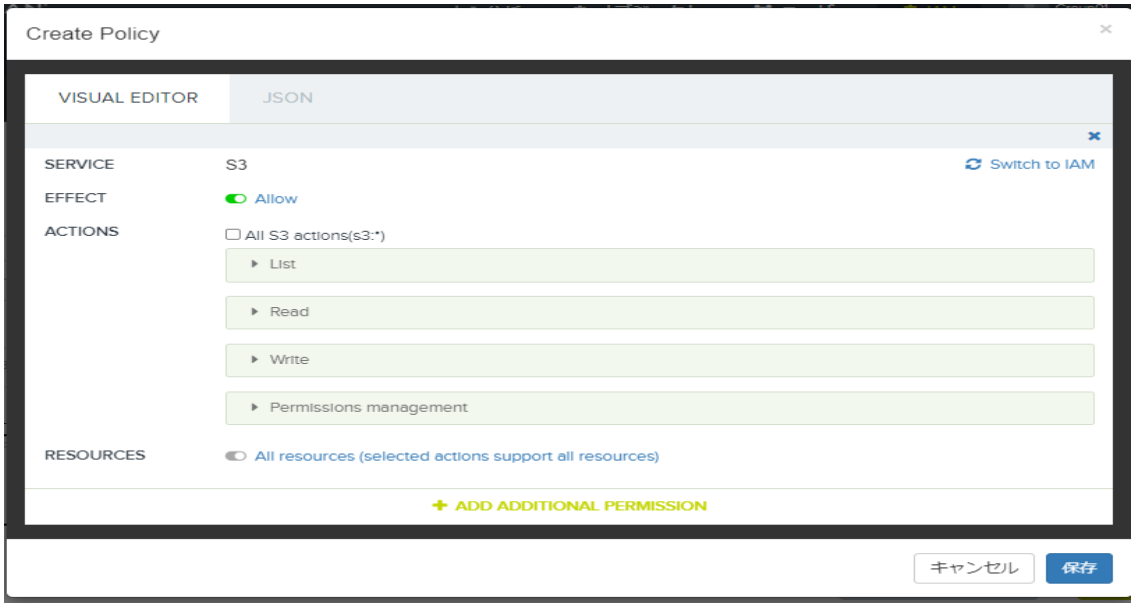
IAM ユーザがバケット/オブジェクトを操作するにあたり、IAM ポリシーの適用は必須です。

下記がポリシー作成のおおまかな流れです。

「IAM ポリシー」メニューをクリックすると、以下の画面に遷移します。
ポリシー名を入力後、赤枠「ポリシードキュメント詳細」をクリックすると、ポリシー設定の別ウインドウが表示されます。



下記のポリシー設定画面で「Action」と対象バケットを取捨選択します。



■■ IAM ポリシーの適用

作成した IAM ポリシーをグループ/ユーザに適用します。
ポリシーを適用したいグループもしくはユーザをクリック、「IAM ポリシー」タブ内の「+ IAM ポリシー追加」をクリックすると作成済みの IAM ポリシーを適用できます。

下記の画面は IAM ユーザ test に、IAM ポリシーtest を適用（追加）した画面です。