FLEX Historical Service
S3 data acquisition manual

Ver. 3.1.5

JPX Market Innovation & Research, Inc.

February, 2024

1. Operation flow

➢ File provisioning is achieved by copying files from the S3 bucket on the AWS account of the JPX Market Innovation & Research to the S3 bucket on the AWS account of the users. This manual shows the necessary operations for file provisioning.

➢ In this section, we will describe the specific operation procedure using the AWS CLI. The flow of the operation is as follows.

➢ Please prepare your AWS account and install AWS CLI in advance.

No	USER	TSE
	・Service Application - ・Receipt of this manual	・Receipt of service application ・conclusion of a contract ・Provision of this manual
1-1.	・Create S3 ・Linking account information	- ・Receipt account information （Account ID/Bucket Name/Data Acquisition Period）
1-2.	- ・Edit bucket policy	・Registering Receiving Information -
1-3.	・Creating an IAM Policy （sts:AssumeRole）	-
1-4.	・Creating an IAM ID （Attaching an IAM policy）	-
1-5.	・AWS CLI （Setting authentication information）	-
1-6.	・AWS CLI（S3 Copy）	-

1-1. Creating S3

■ Creating a bucket on the user account where the files will be stored.

Execution screen	Operation details
- - -- ● [S3] Creating S3	【**AWS Management Console**】 ・ **Select "S3" from Services** -- ・ **Creating S3（FLEX Historicalデータをコピー用）**

<Setting contents>
Bucket name: Specify any bucket name.
AWS Region: Specify Asia Pacific (Tokyo)
※Other bucket settings are based on the rules of each environment.

● [S3] Confirmation

・ **Confirm that S3 has been created.**

<Confirmation>
□The bucket name is the specified bucket name.
□AWS region is "Asia Pacific (Tokyo)".

・ **Linking account information**
Account ID ／ Bucket Name

1-2. Edit bucket policy

■ Add a bucket policy to allow access from buckets on the TSE account.

Execution screen	Operation details
- - - - -- - - - - -- ● [S3] Edit bucket policy 	**・ Receipted notification from JPX that the setup is complete （Approximately 5 business days later)** 　The bucket policy cannot be saved until you receive a notification that the configuration is complete. -- **【AWS Management Console】** ・ Select "S3" from Services ・ Select the bucket you created and display the "Permissions" tab. -- **・ Edit the bucket policy and save the changes.** 　※See next page for details. <Edited contents> 　Principal 　　→ Specify the IAM role for the JPX information distribution account. 　Action 　　→ Specify "ListBucket", "PutObject", "PutObjectAcl" 　Resource 　　→ Specify the bucket name created in 1-1. 　Condition 　　→ Specify granting owner rights as a condition for copying.

1-2. bucket policy (Editing Templates)

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "S3CopyStmtList",
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::461810399597:role/JeuServiceRoleForS3Copy_[Account ID]"
                ]
            },
            "Action": "s3:ListBucket",
            "Resource": [
                "arn:aws:s3:::[Bucket Name]"
            ]
        },
        {
            "Sid": "S3CopyStmtPutObject",
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::461810399597:role/JeuServiceRoleForS3Copy_[Account ID]"
                ]
            },
            "Action": [
                "s3:PutObject",
                "s3:PutObjectAcl"
            ],
            "Resource": [
                "arn:aws:s3:::[Bucket Name]",
                "arn:aws:s3:::[Bucket Name]/*"
            ],
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control"
                }
            }
        }
    ]
}
```

1-3. Creating an IAM Policy (sts:AssumeRole)

JPX

■ Creating an IAM policy to allow copying from a bucket on the JPXI account.

Execution screen	Operation details
● [IAM] Creating IAM Policy	**【AWS Management Console】** ・ Select "S3" from Services ・ From Policies, click "Create Policy" and display the "JSON" tab. ＜Edited contents＞ 　　Action : sts（Security Token Service） 　　　→Specify AssumeRole 　　Resource 　　→ Specify the IAM role for the JPX information distribution account --- ・Click "Next Step: Tags" → "Next Step: Confirm". ・Enter a name and description in the policy confirmation, and then click "Create Policy". ＜Setting contents＞ 　　name → Specify the name of the IAM policy to be created 　　description → any

IAM Policy（Editing Templates）

※ The red bold text is the string to be replaced.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": "sts:AssumeRole",
            "Effect": "Allow",
            "Resource": "arn:aws:iam::461810399597:role/JeuServiceRoleForS3Copy_[Account ID]"
        }
    ]
}
```

JPX

■ Creating an IAM ID with the policy created in 1-3. (Please create an ID for this service)

Execution screen	Operation details

This manual describes an example of IAM user usage (IAM roles, etc. can also be used if the IAM policy created in 1-3 can be attached)

● [IAM] Creating an IAM ID

ユーザーを追加

① ② ③ ④ ⑤

ユーザー詳細の設定

同じアクセスの種類とアクセス権限を使用して複数のユーザーを一度に追加できます。詳細はこちら

ユーザー名*

➕ 別のユーザーの追加

AWS アクセスの種類を選択

これらのユーザーから AWS にアクセスする方法を選択します。アクセスキーと自動生成パスワードは前のステップで提供されています。詳細はこちら

アクセスの種類* ☑ プログラムによるアクセス
AWS API、CLI、SDK などの開発ツールの **アクセスキー ID** と **シークレットアクセスキー** を有効にします。

☐ AWS マネジメントコンソールへのアクセス
ユーザーに AWS マネジメントコンソールへのサインインを許可するための **パスワード** を有効にします。

● [IAM] Attaching an IAM policy

▼ アクセス許可の設定

[👥 ユーザーをグループに追加] [👤 アクセス権限を既存のユーザーからコピー] [📄 既存のポリシーを直接アタッチ]

ポリシーの作成

ポリシーのフィルタ ▾ 🔍 検索 650 件の結果を表示中

	ポリシー名 ▾	タイプ	次として使用
☐ ▸	🟧 AdministratorAccess	ジョブ機能	Permissions policy (1)

【AWS Management Console】
・ Select "S3" from Services
・ From Users, select "Create User"

<Setting contents>
　User name: Specify the IAM user name to be created.
　Access type: Select the check box for programmatic access

・ Click "Next Step: Access Permissions"

・Attach the IAM policy, and click "Next Step: Tags".
Set the IAM policy created in 1-3 in one of the following ways.
※In the manual, "Directly attach existing policy" is used as an example.

<Content>
　Policy filter: IAM policy created in 1-3.
　　→ **Select the check box of the displayed policy name**

"Next Step: Confirmation" → "Create UserButton"
"Download .csv" to obtain the authentication information.
　→ Use "Access key ID" and "Secret access key" in AWS CLI

1-5. AWS CLI (Setting authentication information)

■ Obtain authentication information to JPXI account using your IAM ID

Execution screen on PowerShell	Operation details

Execution screen on PowerShell

● [CLI] Set up authentication information

```
PS C:¥work> aws configure
AWS Access Key ID [*****************]:
AWS Secret Access Key [*****************]:
Default region name []: ap-northeast-1
Default output format []: json
```

※ Set the Key in the CSV file obtained in 1-4

● [CLI] Set the temporary authentication information

```
PS C:¥work> aws sts assume-role
>> --role-arn arn:aws:iam::461810399597:role/JeuServiceRoleForS3Copy_
>> --role-session-name s3copy
>> --duration-seconds $(60*60*12)
[
    "Credentials": [
        "AccessKeyId":
        "SecretAccessKe
        "SessionToken":
        "Expiration :
```

```
PS C:¥work> $env:AWS_ACCESS_KEY_ID = "AS
PS C:¥work> $env:AWS_SECRET_ACCESS_KEY="
PS C:¥work> $env:AWS_SESSION_TOKEN="IQoJ
```

Set the result of outputting temporary authentication information.

【Example of environment variable settings : Linux】
export AWS_ACCESS_KEY_ID=XXX

【When the temporary authentication information has expired : ExpiredToken】
①Clear the environment variables you set.
<Command>
PowerShell → Remove-Item env:AWS_ACCESS_KEY_ID
Linux → unset AWS_ACCESS_KEY_ID

②Re-run

Operation details

【AWS CLI : Linux, Windows PowerShell etc.】
· **Set up authentication information**
<Command>
> aws configure
→ AWS Access Key ID : ※1
→ AWS Secret Access Key : ※1
→ Default region name : 「ap-northeast-1」
→ Default output format : 「json」

※1 : Set the Key in the CSV file obtained in 1-4

· **Obtain temporary authentication information for data acquisition and set it to an environment variable.**
<Command>
> aws sts assume-role `
--role-arn arn:aws:iam::461810399597:role/[※2] `
--role-session-name s3copy ` ※3
--duration-seconds $(60*60*12) ※4

→ temporary authentication information.
(AccesskeyId, SecretAccessKey,SessionToken)

> $env:AWS_ACCESS_KEY_ID =
> $env:AWS_SECRET_ACCESS_KEY = ※5
> $env:AWS_SESSION_TOKEN =

※2 : JeuServiceRoleForS3Copy_[Account ID]
※3 : Specify an any session name
※4 : Period of validity

· Specify the maximum time (12 hours) for the setting period
· Data linkage (AssumeRole) speed between S3: Approximately 200Mbps

※5 : Set the result of outputting temporary authentication information.

1-6. AWS CLI (S3 Copy)

■ Copy the specified file from the JPXI account to the bucket created in 1-1.

Execution screen on PowerShell	Operation details

Execution screen on PowerShell

● [CLI] data Acquisition

```
PS C:¥work> aws s3 cp s3://dataservice-flex-bucket/2021/05/31 `
>> s3://sample-myawsbucket/2021/05/31 `
>> --recursive --exclude "*" --include "*" `
>> --acl bucket-owner-full-control
copy: s3://dataservice-flex-bucket/2021/05/31/20210531_1_001.pcap.gz to s3://sample-
copy: s3://dataservice-flex-bucket/2021/05/31/20210531_1_002.pcap.gz to s3://sample-
```

<表：データ取得の想定時間>

period（year）	size（TB）	Required Time (minute)
2010	0.17	14
2011	0.21	18
2012	0.22	19
2013	0.44	37
2014	0.55	47
2015	0.84	72
2016	1.24	106
2017	0.99	84
2018	1.21	103
2019	1.11	95
2020	1.48	127

● [CLI] confirmation

```
PS C:¥work> aws s3 ls sample-myawsbucket/2021/05/31 --recursive
2021-03-23 21:53:37        0 2021/05/31/
2021-03-24 13:31:36       52 2021/05/31/20210531_1_001.pcap.gz
2021-03-24 13:31:36       52 2021/05/31/20210531_1_002.pcap.gz
```

Operation details

【AWS CLI : Linux, Windows PowerShell etc.】
・data Acquisition

> Even if you have a contract for the All-period Service, please obtain data in annual units based on the validity period of the temporary authentication information.

<Command>
> aws s3 cp s3://dataservice-flex-bucket/[Target date※] `
  s3://[Bucket name]/[Target date※] `
  --recursive --exclude "*" --include "*" `
  --acl bucket-owner-full-control

※ : format : YYYY/MM/DD
  (example)
  Day : 2021/05/31
  Month : 2021/05
  Year : 2021

・**confirmation**
<Command>
> aws s3 ls s3://[Bucket name]/[Target date] `
  --recursive

※In Copying the FLEX Connection Specifications, please change [Target date] to [ConnectionSpec/[Version]/[Language]].
(Example) List: aws s3 ls s3://dataservice-flex-bucket/ConnectionSpec/version 17.4/English --recursive
   Acquisition: aws s3 cp s3://dataservice-flex-bucket/ConnectionSpec/version 17.4/English s3://[Bucket name]/～[(The rest is omitted)]