

S3 サービス利用 マニュアル

日本電気株式会社

2024 年 7 月 9 日

第 2 版

<< 改版履歴 >>

版数	改版日	改版理由	改版者
第 0 版	2024/2/29	運用評価用として作成	NEC
第 1 版	2024/3/29	正式運用版として改版	NEC
第 2 版	2024/7/9	Linux 相互利用版として改版	NEC

目次

1	はじめに	3
2	アクセスキー操作.....	4
2.1	アクセスキー発行.....	4
2.2	アクセスキー表示.....	4
2.3	アクセスキー無効化.....	5
2.4	シークレットキー再生成	5
3	バケット操作.....	6
3.1	バケット作成.....	6
3.2	バケット表示.....	7
3.3	バケット削除.....	7
3.4	バケット同期.....	7
4	S3 Browser (GUI)	9
4.1	インストール.....	9
4.2	アクセスキー設定.....	9
4.3	S3 オブジェクト PUT.....	11
4.4	S3 オブジェクト GET.....	13
4.5	ACL 設定	15
4.6	バケットポリシー設定	18
5	S3cmd (CLI)	20
5.1	インストール.....	20
5.2	アクセスキー設定.....	20
5.3	S3 オブジェクト PUT.....	21
5.4	S3 オブジェクト GET.....	21
5.5	S3 オブジェクト LIST	22
5.6	ACL 設定	22
5.7	バケットポリシー設定	23
6	ファイルシステムアクセス.....	24
	参考資料 : Windows への S3cmd インストール方法	25

1 はじめに

AOBA-S ストレージの S3 サービス用領域(以下 S3 サービスとする)の利用概要を以下に記載します。なお、S3 サービスを利用するには AOBA の利用者 ID を取得している必要があります。

S3 サービスの利用概要は以下のとおりです。

- ① AOBA 管理者へ S3 サービスの利用申請を行う
- ② 利用申請承認後、AOBA-S フロントエンドサーバにログインし、アクセスキーの発行およびバケット作成を行う（「2.1 アクセスキー発行」、「3.1 バケット作成」を参照）
- ③ S3 クライアントツールにアクセスキーを設定し、利用する（「4 S3Browser」もしくは「5 S3cmd」を参照）
 - ・S3 クライアントツールで操作したオブジェクトを、AOBA-S フロントエンドサーバから操作する方法は「6 ファイルシステムアクセス」を参照してください。
 - ・AOBA-S フロントエンドサーバから操作したファイルを、S3 クライアントツールで操作するにはフロントエンドサーバ上で同期操作が必要です。「3.4 バケット同期」を実施後、S3 クライアントツールでの操作が行えます。

S3 領域の利用には任意の S3 クライアントツールが使用できますが、本書では、S3 Browser(GUI)と S3cmd(CLI)の基本操作手順を記載します。本書に記載されていない操作については、各ツールのマニュアルを参照してください。

ツール名	マニュアル URL
S3 Browser	https://s3browser.com/help.aspx
S3cmd	https://s3tools.org/usage

2 アクセスキー操作

AOBA-S フロントエンドサーバで、アクセスキー操作コマンド(s3keys)を実行することで、アクセスキーの発行・表示・無効化・再発行が可能です。

2.1 アクセスキー発行

以下のコマンドを実行して、アクセスキーを発行します。

注意：アクセスキーの発行は、ひとりの利用者当たり、ひとつに制限しています。

```
$ s3keys create
```

実行例) w29999 ユーザで実行した場合

```
$ s3keys create
+-----+-----+-----+-----+-----+-----+
| tag      | w29999_1 |
| accesskey | XXXXXXXXXXXXXXXXXXXXXXXX |
| secretkey | xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx |
| uuid     | 328de0590caa33ab1e8dde463aa83460079fa7f2 |
| root_uuid | 328de0590caa33ab1e8dde463aa83460079fa7f2 |
| user_type | ROOT_USER |
| fsuid     | 2999:1000 |
| fspaths   | /mnt/lustre/S3/w29999 |
| enabled   | True |
+-----+-----+-----+-----+-----+-----+-----+
```

2.2 アクセスキー表示

以下のコマンドを実行して、発行したアクセスキーを表示します。

```
$ s3keys list
```

実行例) w29999 ユーザで実行した場合

```
$ s3keys list
+-----+-----+-----+-----+-----+-----+-----+
| accesskey | enabled | root_uuid | secretkey | tag      | user_type | uuid      |
+-----+-----+-----+-----+-----+-----+-----+
| XXXXX.... | True    | 328de0... | xxxxxx... | w29999_1 | ROOT_USER | 328de0... |
```

2.3 アクセスキー無効化

以下のコマンドを実行して、発行したアクセスキーを無効化します。

注意：アクセスキーを一度無効化すると、再度有効化することはできません。

```
$ s3keys disable
```

実行例) w29999 ユーザで実行した場合

```
$ s3keys disable
+-----+
| tag      | w29999_1 |
| accesskey | XXXXXXXXXXXXXXXXXXXXXXXX |
| secretkey | xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx |
| uuid     | 328de0590caa33ab1e8dde463aa83460079fa7f2 |
| root_uuid | 328de0590caa33ab1e8dde463aa83460079fa7f2 |
| user_type | ROOT_USER |
| fsuid     | 2999:1000 |
| fspaths   | /mnt/lustre/S3/w29999 |
| enabled   | False |
+-----+
```

2.4 シークレットキー再生成

以下のコマンドを実行して、シークレットキーの再生成が可能です。

```
$ s3keys regen
```

実行例) w29999 ユーザで実行した場合

```
$ s3keys regen
```

tag	w29999_1
accesskey	XXXXXXXXXXXXXXXXXXXXXX
secretkey	vvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvv
uuid	328de0590caa33ab1e8dde463aa83460079fa7f2
root_uuid	328de0590caa33ab1e8dde463aa83460079fa7f2
user_type	ROOT_USER
fuid	2999:1000
fspath	/mnt/lustre/S3/w29999
enabled	True

3 バケット操作

AOBA-S フロントエンドサーバで、バケット操作ツールコマンド(s3bucket)を実行することで、バケットの作成・表示・削除・同期を行います。

なお、本コマンドは大阪大学サイバーメディアセンターからの利用許諾に基づき利用しています。

3.1 バケット作成

以下のコマンドを実行して、バケットを作成します。

注意：S3 クライアントツール(S3Browser, s3cmd など)からもバケット作成は可能ですが、S3 クライアントツールで作成したバケットは、ファイルシステム(AOBA-S)と相互利用することはできません。

```
$ s3bucket create -k [アクセスキー] -b [バケット名]
```

[アクセスキー]： 2.1 で作成したアクセスキーを指定

[バケット名]： 作成するバケット名を指定

※ バケット名の命名規則は以下の通りです

- ・ 4 文字以上 62 文字以下
- ・ 数字または文字から開始
- ・ 小文字アルファベット(a-z), 数字(0-9), ピリオド(.), ハイフン(-)が使用可能
- ・ アンダースコア(_)は使用不可能
- ・ 末尾がハイフン(-)は不可能
- ・ “..”, “.-”, “--”のような組み合わせは使用不可能

実行例)

```
$ s3bucket create -k XXXXXXXXXXXXXXXXXXXX -b test-bucket
```

3.2 バケット表示

以下のコマンドを実行して、作成したバケットを表示します。

```
$ s3bucket list -k [アクセスキー]
```

[アクセスキー]： 2.1 で作成したアクセスキーを指定

実行例)

```
$ s3bucket list -k XXXXXXXXXXXXXXXXXXXX
+-----+-----+
| Name      | CreationDate      |
+-----+-----+
| test-bucket | YYYY-MM-DD hh:mm:ss |
+-----+-----+
```

3.3 バケット削除

「3.1 バケット作成」の手順で作成したバケットを削除するには、以下のコマンドを実行します。

注意：バケット削除する前にバケット内のすべてのオブジェクトが削除されている必要があります。

また、S3 クライアントツール(S3Browser, s3cmd など)から作成したバケットは、本手順では削除できません。S3 クライアントツールで作成したバケットは、S3 クライアントツールから削除操作を行ってください。

```
$ s3bucket delete -k [アクセスキー] -b [バケット名]
```

[アクセスキー]： 2.1 で作成したアクセスキーを指定

[バケット名]： 削除するバケット名を指定

実行例)

```
$ s3bucket delete -k XXXXXXXXXXXXXXXXXXXX -b test-bucket
```

3.4 バケット同期

3.1 の方法で作成したバケットは、ファイルシステム(AOBA-S)の「/mnt/lustre/S3/<ユーザ名>/<バケット名>」に作成され、S3 クライアントツールおよびファイルシステム(AOBA-S)から利用す

ることができます。

しかし、ファイルシステム(AOBA-S)から「/mnt/lustre/S3/<ユーザ名>/<バケット名>」配下のファイル进行操作した場合、自動では S3 クライアントツールから操作することはできません。

ファイルシステム(AOBA-S)からファイルを作成、移動、削除などの操作をした場合には、以下のコマンドを実行した上で S3 クライアントツールから利用します。

注意：S3 クライアントツール(S3Browser, s3cmd など)かで作成したバケットは、ファイルシステム(AOBA-S)から利用することはできませんので、本手順による同期を行うことはできません。

```
$ s3bucket sync -k [アクセスキー] -b [バケット名]
```

[アクセスキー]： 2.1 で作成したアクセスキーを指定

[バケット名]： 作成するバケット名を指定

実行例)

```
$ s3bucket sync -k XXXXXXXXXXXXXXXXXXXX -b test-bucket
```

4 S3 Browser (GUI)

4.1 インストール

以下からインストーラをダウンロードし、クライアント端末に「S3 Browser」をインストールします。

<https://s3browser.com/download.aspx>

4.2 アクセスキー設定

- ① S3 Browser を初めて起動すると、新しいアカウントの追加ダイアログが開きます。ダイアログが表示されない場合、[Accounts] -> [Add new account]の順にクリックします。

Add New Account online help

Enter new account details and click Add new account

Display name:

Assign any name to your account.

Account type:

Choose the storage you want to work with. Default is Amazon S3 Storage.

REST Endpoint:

Specify S3-compatible API endpoint. It can be found in storage documentation. Example: rest.server.com:8080

Access Key ID:

Required to sign the requests you send to Amazon S3, see more details at <https://s3browser.com/keys>

Secret Access Key:

Required to sign the requests you send to Amazon S3, see more details at <https://s3browser.com/keys>

☐ Encrypt Access Keys with a password:

Turn this option on if you want to protect your Access Keys with a master password.

☒ Use secure transfer (SSL/TLS)
If checked, all communications with the storage will go through encrypted SSL/TLS channel

[advanced settings..](#)

- ② ダイアログに下記を入力します。

項目	設定値
Display name	表示したい名前
Account type	S3 Compatible Storage
REST Endpoint	s3ds.cc.tohoku.ac.jp
Access Key ID	アクセスキー
Secret Access Key	シークレットキー
Encrypt Access Keys with a password	ブランクのまま
Use secure transfer (SSL/TLS)	チェックが付いたまま

- ③ 「advances settings…」をクリックします。

- ④ 以下のポップアップが表示されるため、下記を入力し、「Close」をクリックします。

Advanced S3-Compatible Storage Settings

Storage settings [online help](#)

Advanced settings for S3-compatible storage

S3-Compatible Miscellaneous

Signature version:
 Signature V2
Choose supported signature version. Default value is Signature V2.

Addressing model:
 Path style
Choose supported addressing model for your storage. Path style addressing is default value.

☐ Override storage regions
 Default Region=us-east-1
You may define custom regions here, format is Region Name=region-code, one region per line

Region-specific endpoint (optional):

Specify endpoint using the {region-code} variable, for example s3.{region-code}.wasabisys.com

Close

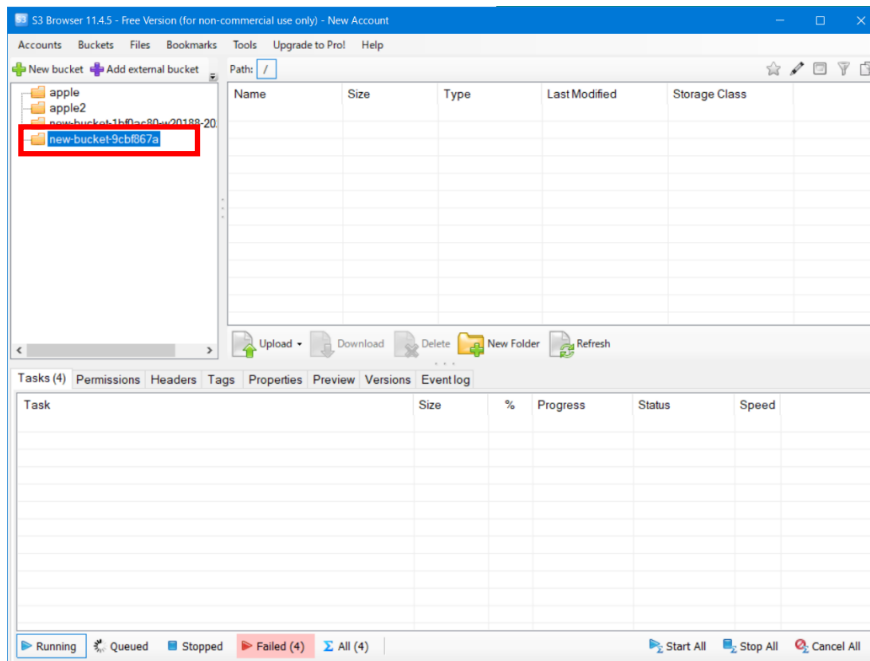
項目	設定値
Signature version	Singnature V2
Addressing model	Path style

- ⑤ 入力後, [Add new account]をクリックします。

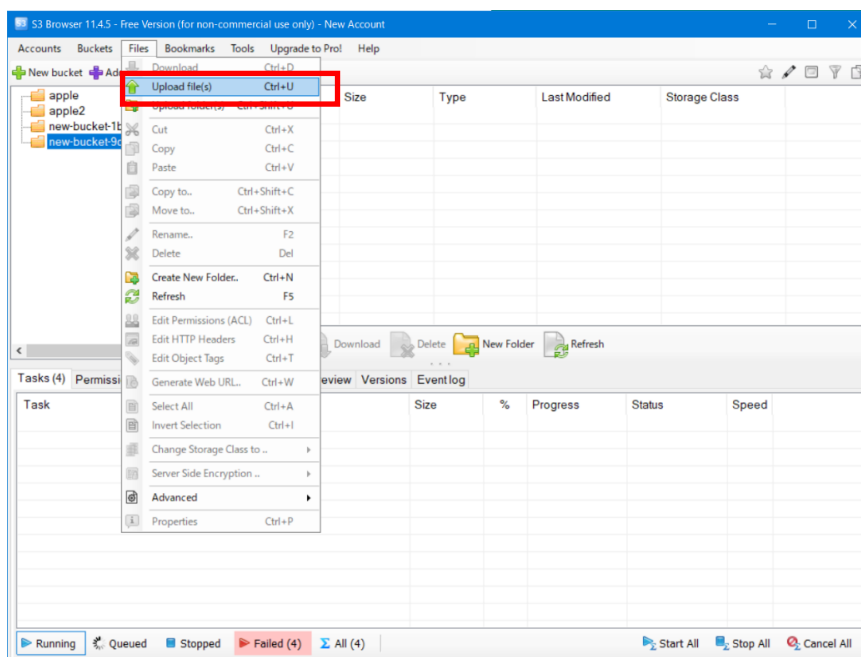
4.3 S3 オブジェクト PUT

- ① S3 Browser で操作対象のバケットを選択します。

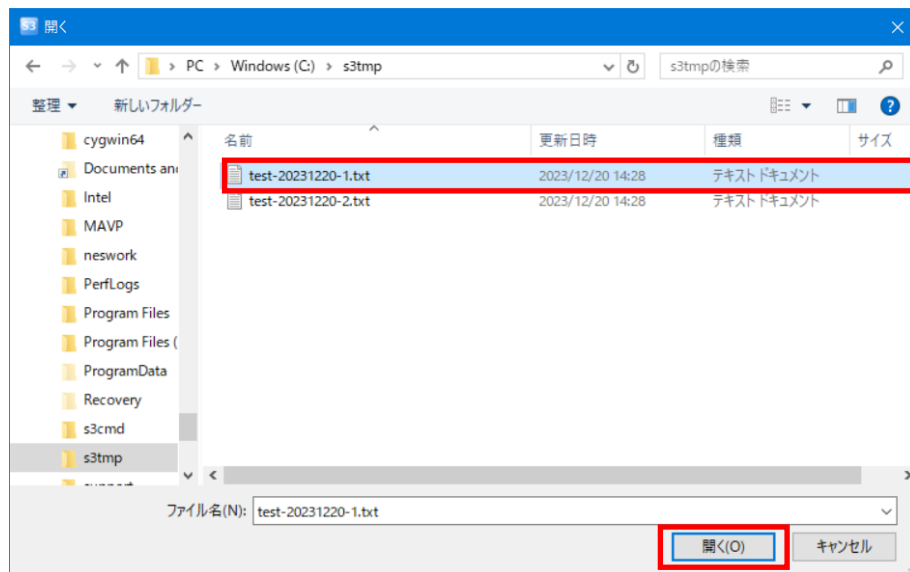
注意：操作するバケットは、「3.1 バケットの作成」の手順で事前に作成します。
S3Browser で作成したバケットは、ファイルシステム(AOBA-S)と相互利用することはできません。



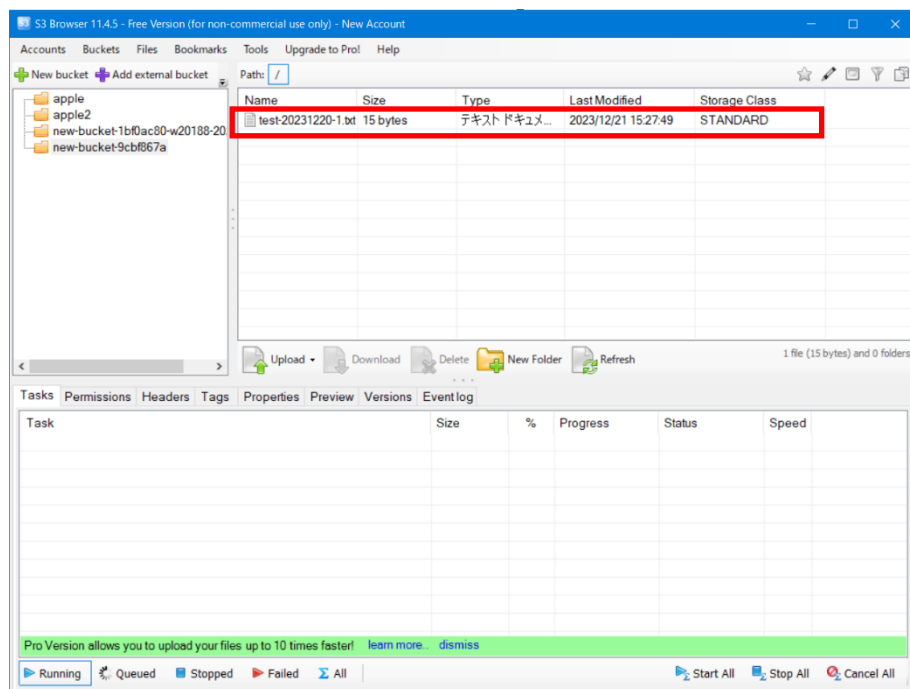
- ② [Files] ->[Upload file(s)]をクリックします。



- ③ アップロードするファイルを選択し、[開く]をクリックします。

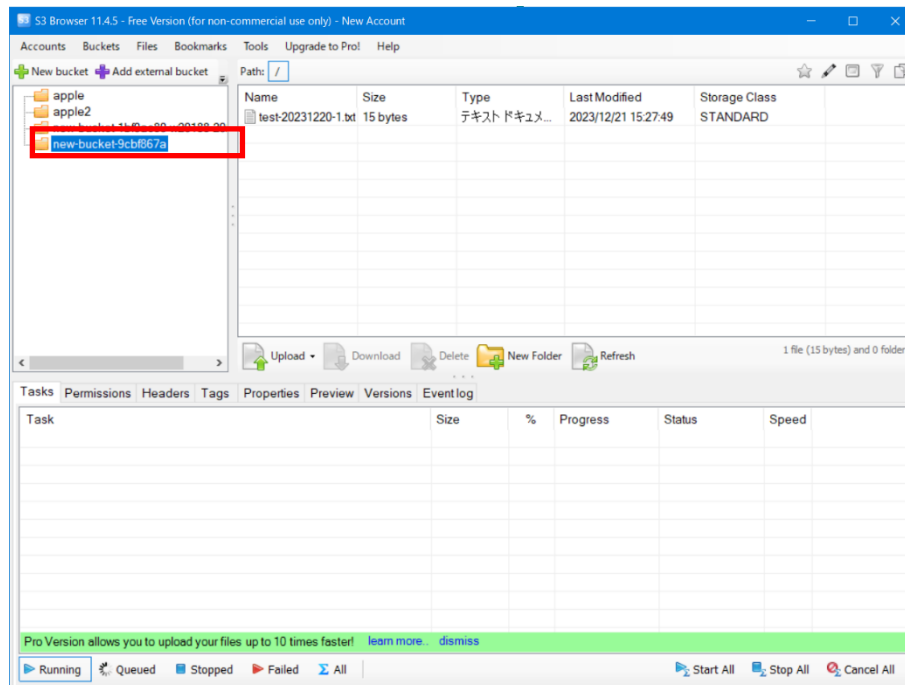


ファイルがバケットにアップロードされます。

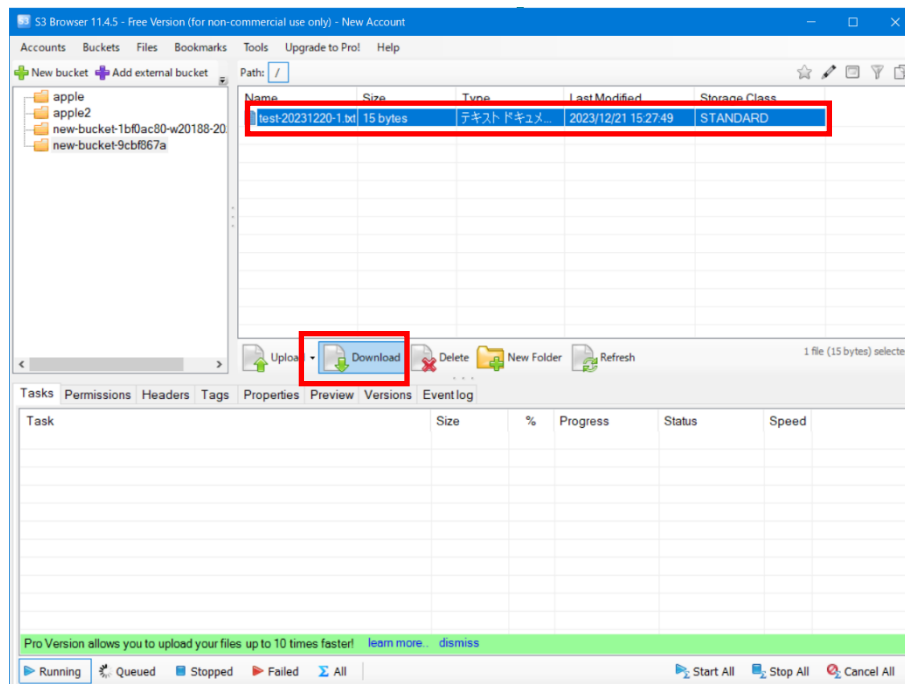


4.4 S3 オブジェクト GET

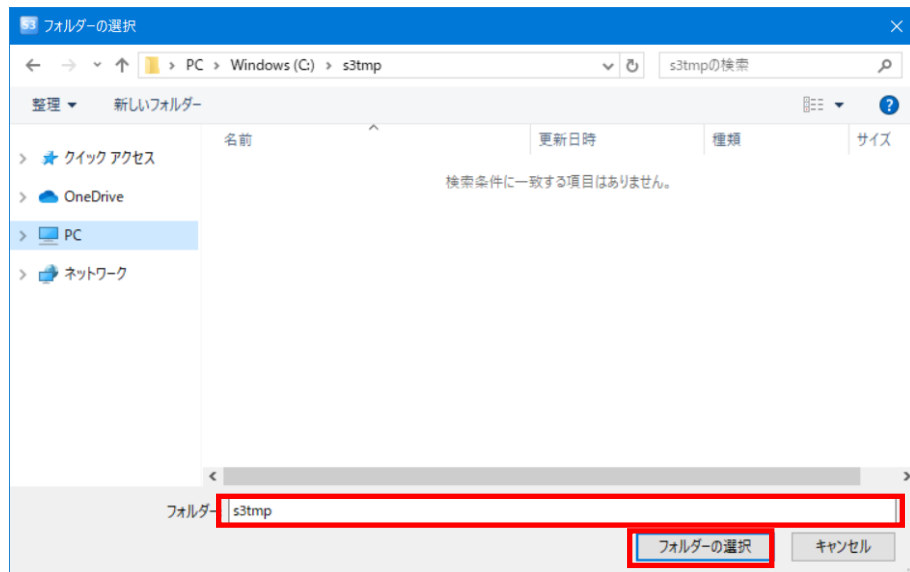
- ① S3 Browser で、ダウンロードするファイルを含むバケットを選択します。



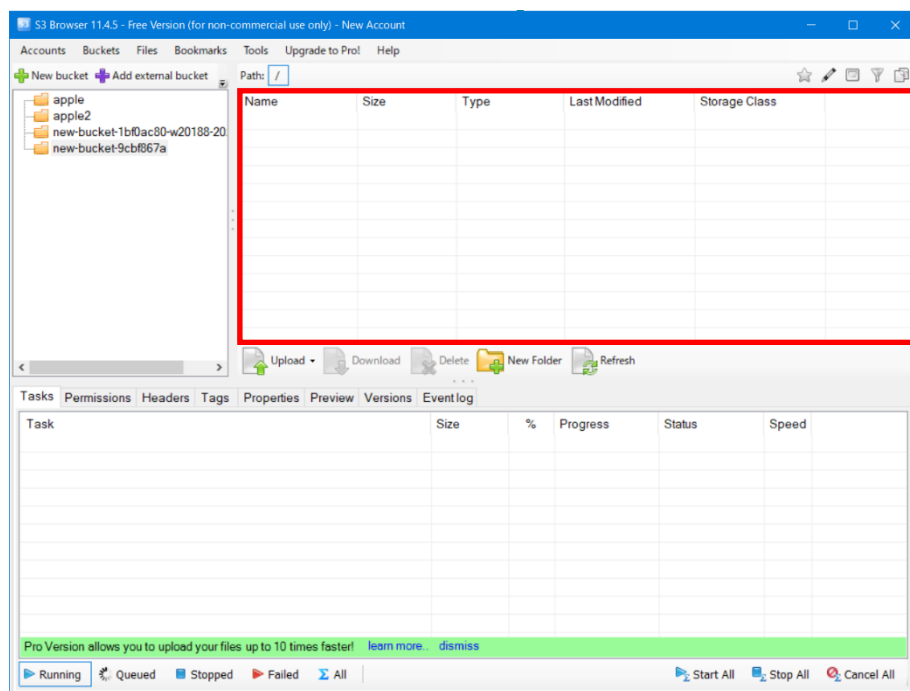
- ② ダウンロードするファイルを選択し、[Download]をクリックします。



- ③ ローカルディスク上の保存先フォルダーを選択し、[フォルダーの選択]をクリックします。



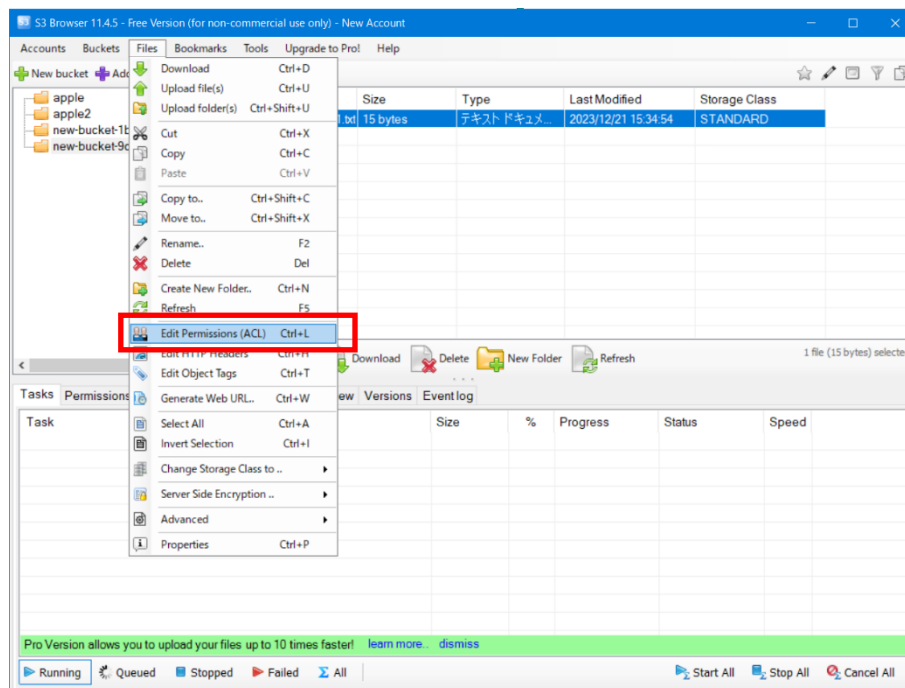
ファイルがローカルディスク上の保存先にダウンロードされます。



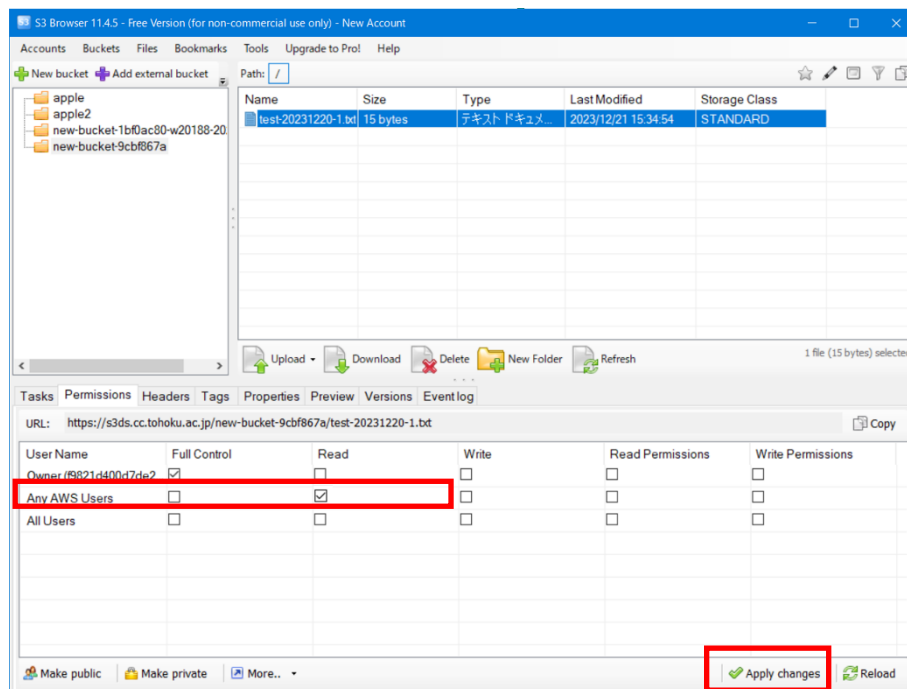
4.5 ACL 設定

ACL を設定することによって、S3 領域の他利用者とバケットやオブジェクトを共有したりすることが可能です。例として、S3 領域の他利用者に、自バケット内のオブジェクトの読み取り権限を与える手順を以下に記載します。

- ① 共有するファイルを選択し、[Files] ->[Edit Permissions(ACL)] をクリックします。



- ② [Permissions] タブで、「Any AWS Users」の「Read」にチェックを付け、[Apply Changes] をクリックします。



[User Name]

パラメータ	意味
Any AWS Users	S3 サービスを利用する（アクセスキーを有する）すべてのユーザ
All Users	すべてのユーザ ※例えば Read 権限を与えた場合、インターネットへ公開されます

次のメッセージが表示されます。

S3 Browser 11.4.5 - Free Version (for non-commercial use only) - New Account

Accounts Buckets Files Bookmarks Tools Upgrade to Pro! Help

+ New bucket + Add external bucket

Path: /

Name	Size	Type	Last Modified	Storage Class
test-20231220-1.txt	15 bytes	テキストドキュメント	2023/12/21 15:34:54	STANDARD

Upload Download Delete New Folder Refresh 1 file (15 bytes) selected

Tasks Permissions Headers Tags Properties Preview Versions Event log

URL: <https://s3ds.cc.tohoku.ac.jp/new-bucket-9cbf867a/test-20231220-1.txt> Copy

User Name	Full Control	Read	Write	Read Permissions	Write Permissions
Owner (f9821d400d7de2...)	☒	☐	☐	☐	☐
Any AWS Users	☐	☒	☐	☐	☐
All Users	☐	☐	☐	☐	☐

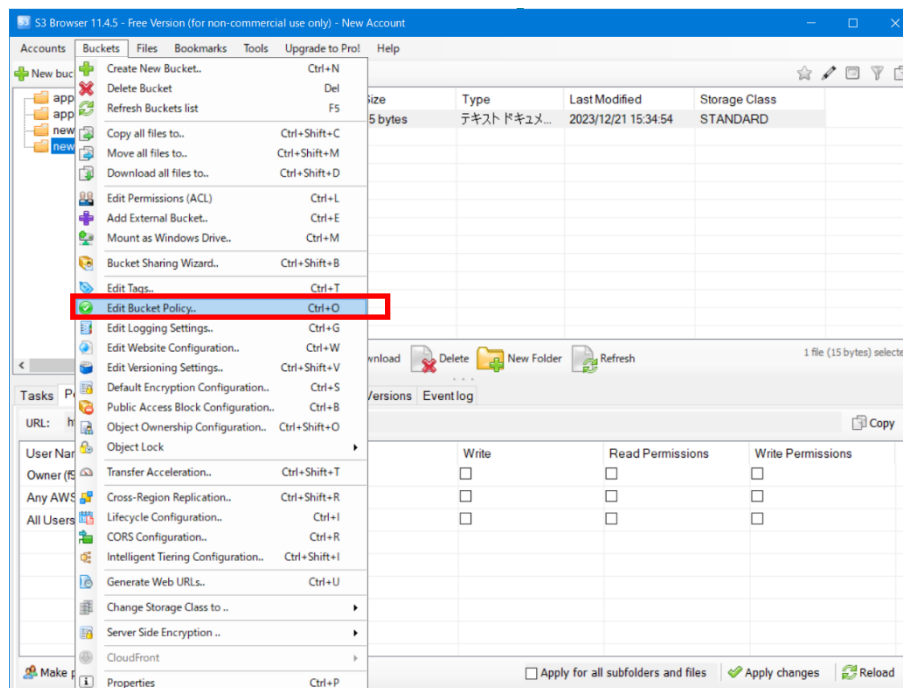
Permissions have been successfully updated for test-20231220-1.txt

Make public Make private More.. Apply changes Reload

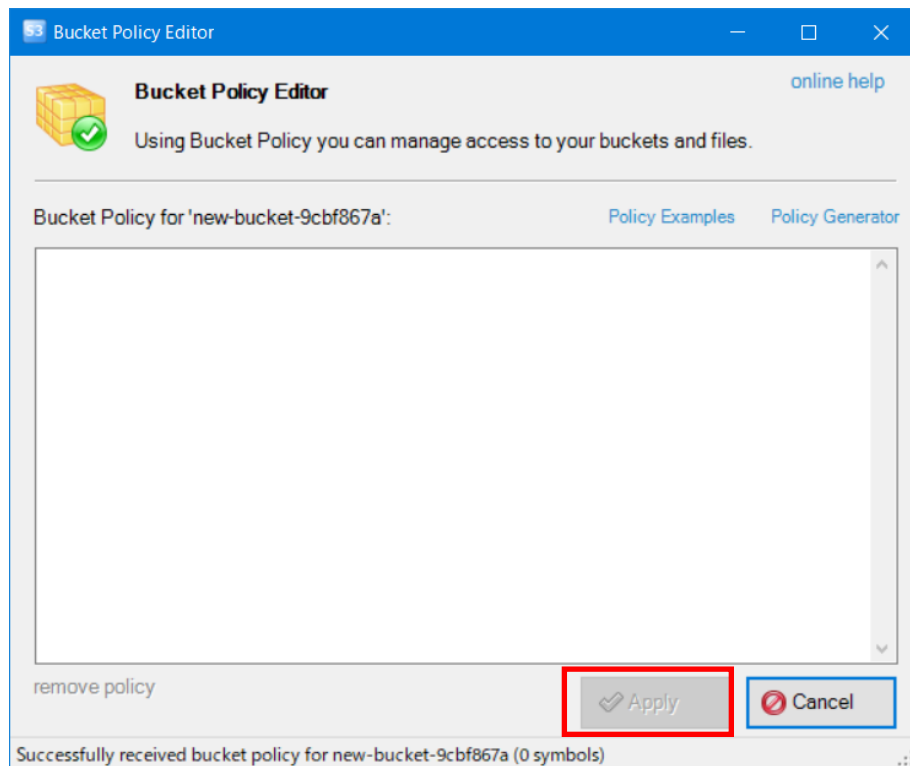
4.6 バケットポリシー設定

バケットやオブジェクトへの権限制御はバケットポリシーでも可能です。例として、特定ユーザにバケット内のオブジェクトの読み取り権限を与える、バケットポリシーの設定手順を以下に記載します。

- ① [Buckets] → [Edit Bucket Policy] をクリックします。



- ② バケットポリシーエディタダイアログが開くため、バケットポリシーを入力し、[Apply]をクリックします。



バケットポリシー

```
{
  "Id": "test", <任意>
  "Version": "2008-10-17",
  "Statement": [
    {
      "Sid": "test", <任意>
      "Effect": "Allow",
      "Principal": {
        "DDN": [
          " ac04d2a28ab45153ef2f7b89e513ftef02585f3a " <権限を与えるユーザの UUID>
        ]
      },
      "Action": [
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:ListBucket"
      ],
      "Resource": "my-bucket" <バケット名>
    }
  ]
}
```

5 S3cmd (CLI)

5.1 インストール

以下を参照して、S3cmd をインストールします。(Windows へのインストール方法を「5 参考」に記載します。)

<https://github.com/s3tools/s3cmd/blob/master/INSTALL.md>

※クライアント環境が Windows の場合、接頭に「python」を付けてコマンドを実行する必要があります。

5.2 アクセスキー設定

アクセスキーの設定は以下のコマンドで実施します。

```
$ s3cmd --configure
```

(実行例)

```
$ s3cmd --configure
```

Enter new values or accept defaults in brackets with Enter.
Refer to user manual for detailed description of all options.

Access key and Secret key are your identifiers for Amazon S3. Leave them empty for using the env variables.

Access Key: ★[アクセスキー]を入力

Secret Key: ★[シークレットキー]を入力

Default Region [US]: ★[us-east-1]を入力

Use "s3.amazonaws.com" for S3 Endpoint and not modify it to the target Amazon S3.
S3 Endpoint [s3.amazonaws.com]: ★[s3ds.cc.tohoku.ac.jp]を入力

Use "%(bucket)s.s3.amazonaws.com" to the target Amazon S3. "%(bucket)s" and "%(location)s" vars can be used
if the target S3 system supports dns based buckets.

DNS-style bucket+hostname:port template for accessing a bucket
[% (bucket)s.s3.amazonaws.com]: ★[s3ds.cc.tohoku.ac.jp]を入力

Encryption password is used to protect your files from reading
by unauthorized persons while in transfer to S3

Encryption password: ★Enter

Path to GPG program: ★Enter

When using secure HTTPS protocol all communication with Amazon S3
servers is protected from 3rd party eavesdropping. This method is
slower than plain HTTP, and can only be proxied with Python 2.7 or newer
Use HTTPS protocol [Yes]: ★Enter

On some networks all internet access must go through a HTTP proxy.
Try setting it here if you can't connect to S3 directly
HTTP Proxy server name: ★Enter

New settings:

Access Key: [アクセスキー]

Secret Key: [シークレットキー]

Default Region: us-east-1

S3 Endpoint: s3ds.cc.tohoku.ac.jp

DNS-style bucket+hostname:port template for accessing a bucket:

s3ds.cc.tohoku.ac.jp

Encryption password:

Path to GPG program: None

Use HTTPS protocol: True

HTTP Proxy server name:

HTTP Proxy server port: 0

Test access with supplied credentials? [Y/n] ★[Y]を入力

Please wait, attempting to list all buckets...

Success. Your access key and secret key worked fine :-)

Now verifying that encryption works...

Not configured. Never mind.

Save settings? [y/N] ★[y]を入力

Configuration saved to '/home/user/.s3cfg'

5.3 S3 オブジェクト PUT

S3 オブジェクトの PUT は以下のコマンドで実施します。

注意：操作するバケットは、「3.1 バケットの作成」の手順で事前に作成します。

```
$ s3cmd put <アップロードファイルパス> s3://<バケット名>/
```

(実行例)

```
$ s3cmd put test_txt1.txt s3://my-bucket/  
upload: 'test_txt1.txt' -> 's3://my-bucket/test_txt1.txt' [1 of 1]  
8 of 8 100% in 0s 14.54 B/s done
```

5.4 S3 オブジェクト GET

S3 オブジェクトの GET は以下のコマンドで実施します。

```
$ s3cmd get s3://<バケット名>/<ダウンファイルパス> <ローカル保存パス>
```

(実行例)

```
$ s3cmd get s3://my-bucket/test_txt1.txt ./
download: 's3://my-bucket/test_txt1.txt' -> './test_txt1.txt' [1 of 1]
8 of 8 100% in 0s 110.24 B/s done
```

5.5 S3 オブジェクト LIST

S3 オブジェクトの LIST は以下のコマンドで実施します。

```
$ s3cmd ls s3://<バケット名>/
```

(実行例)

```
$ s3cmd ls s3://my-bucket/
2023-12-22 02:03          9 s3://my-bucket/test.txt
```

5.6 ACL 設定

ACL を設定することによって、S3 領域の他利用者とバケットやオブジェクトを共有したりすることが可能です。例として、特定ユーザに、自バケット内のオブジェクトの読み取り権限を与える手順を以下に記載します。

(ACL 設定コマンド)

```
$ s3cmd <ACL 設定オプション> setacl s3://<バケット名>/<オブジェクト名>
```

(ACL 設定確認)

```
$ s3cmd info s3://BUCKET[/OBJECT]
```

(実行例)

権限を与えるユーザの UUID が以下の場合：

```
ac04d2a28ab45153ef2f7b89e513ftef02585f3a
```

```
$ s3cmd --acl-grant=read:ac04d2a28ab45153ef2f7b89e513ftef02585f3 setacl
s3://my-bucket/test_txt1.txt
s3://my-bucket/test_txt1.txt: ACL updated

$ s3cmd info s3://my-bucket/test_txt1.txt
s3://my-bucket/test_txt1.txt (object):
  File size: 8
  Last mod:  Thu, 21 Dec 2023 08:18:09 GMT
  MIME type: text/plain
  Storage:   STANDARD
  MD5 sum:   73e89a42b88f06aa7467de62669e16f5
```

SSE:	none
Policy:	none
CORS:	none
ACL:	gd9yd2a28ab45153ef2f7b43e513ftef02585f3r: FULL_CONTROL
ACL:	ac04d2a28ab45153ef2f7b89e513ftef02585f3a: READ

5.7 バケットポリシー設定

バケットやオブジェクトへの権限制御はバケットポリシーでも可能です。例として、特定ユーザにバケット内のオブジェクトの読み取り権限を与える、バケットポリシーの設定手順を以下に記載します。

(バケットポリシー設定コマンド)

```
$ s3cmd setpolicy <ポリシーファイルパス> s3://<バケット名>
```

(バケットポリシー確認)

```
$ s3cmd info s3://<バケット名>
```

(実行例)

```
$ s3cmd setpolicy bucket_policy.json s3://my-bucket
s3://my-bucket/: Policy updated

$ s3cmd info s3://my-bucket
s3://my-bucket/ (bucket):
  Location: us-east-1
  Payer: none
  Ownership: none
  Versioning: none
  Expiration rule: none
  Block Public Access: none
  Policy: {"Id": "policy1", "Version": "2008-10-17", "Statement": [{"Sid": "statement1_Allow", "Effect": "Allow", "Principal": {"DDN": ["ac04d2a28ab45153ef2f7b89e513ftef02585f3a"]}, "Action": ["s3:GetObject"], "Resource": "my-bucket"}]}
  CORS: none
  ACL: gd9yd2a28ab45153ef2f7b43e513ftef02585f3r: FULL_CONTROL
```

6 ファイルシステムアクセス

S3 クライアントツールによって操作したオブジェクトは、AOBA-S 環境からファイルシステムアクセスが可能です。AOBA-S のフロントエンドサーバからのアクセス方法を以下に記載します。

注意：S3 ACL やバケットポリシーで他利用者へアクセス権限を付与しても、ファイルシステムアクセスには権限情報が引き継がれません。

- ① AOBA-S フロントエンドサーバにログインします。
- ② 以下のコマンドで、S3 領域に移動します。

(バケットを 3.1 の方法で作成した場合)

```
$ cd /mnt/lustre/S3/<ユーザ名>
```

- ③ バケット名のディレクトリ配下に S3 オブジェクトファイルがあることを確認します。
\$ ls <バケット名>

注意：ファイルシステム(AOBA-S)と、S3 クライアントツールから相互にアクセスしたい場合には、「3. バケット操作」に従って、バケットの作成およびバケットの同期 を行ってください。

参考資料：Windows への S3cmd インストール方法

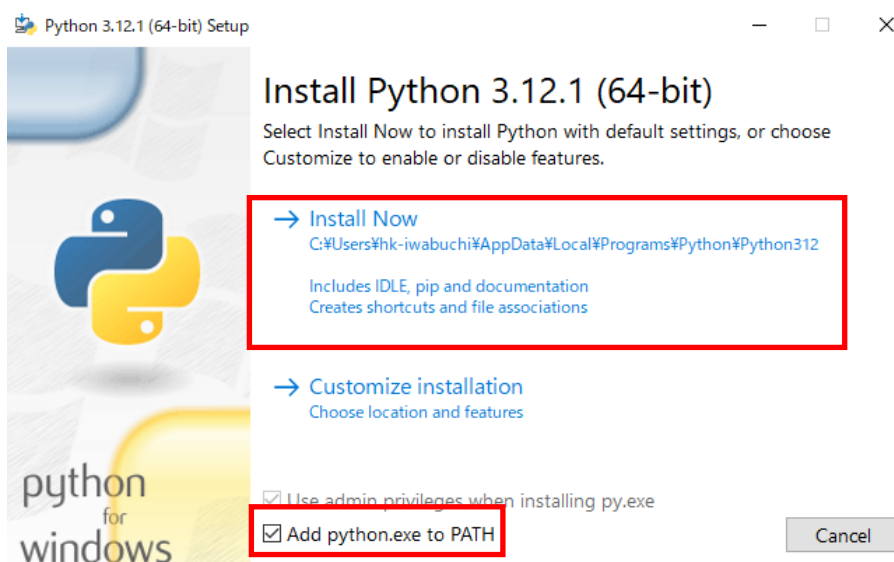
[確認環境]

OS : Windows 11

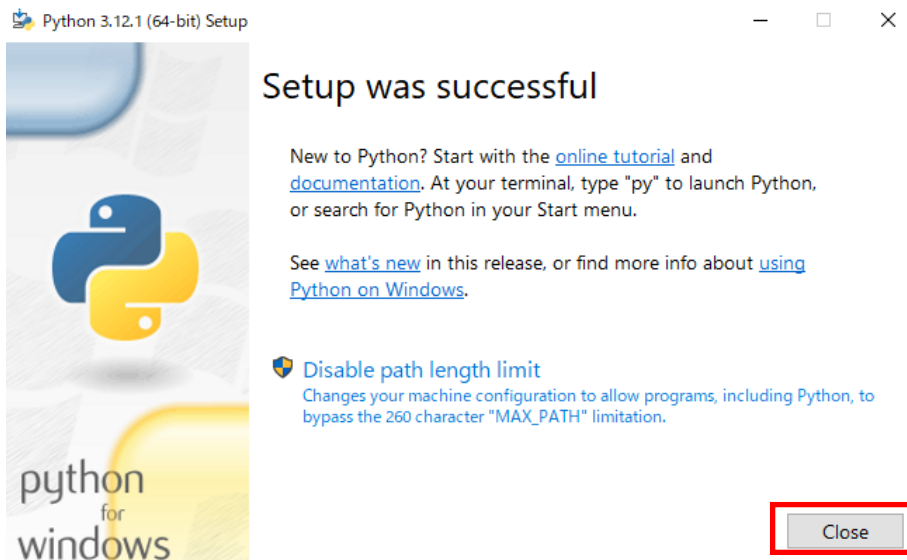
Python : 3.11

S3cmd : 2.4.0

- ① 以下から, Python インストーラをダウンロードします.
<https://www.python.org/downloads/windows>
- ② インストーラを起動します.
- ③ インストーラ起動後, 以下の画面で「Add python.exe to PATH」にチェックを入れ, 「Install Now」を選択します.



- ④ インストール完了後, 「Close」をクリックします.



- ⑤ 再起動を行います。
- ⑥ 以下より、ZIP ファイルをダウンロードします。
<https://sourceforge.net/projects/s3tools/files/s3cmd/>
- ⑦ ZIP ファイルを解凍します。
- ⑧ コマンドプロンプトを開き、以下のコマンドで、ZIP ファイルを解凍したフォルダパスへ移動します。
\$ cd [フォルダパス]
- ⑨ 以下のコマンドを実行し、S3cmd に必要なモジュールをインストールします。
\$ pip install setuptools
- ⑩ 以下のコマンドを実行し、S3cmd をインストールします。
\$ python setup.py install
- ⑪ インストール完了後、以下のコマンドを実行します。
\$ python s3cmd --version
バージョン情報が表示されればインストールは完了です。