オブジェクトストレージサービス
アクセス制限
バケットPolicy設定ガイド

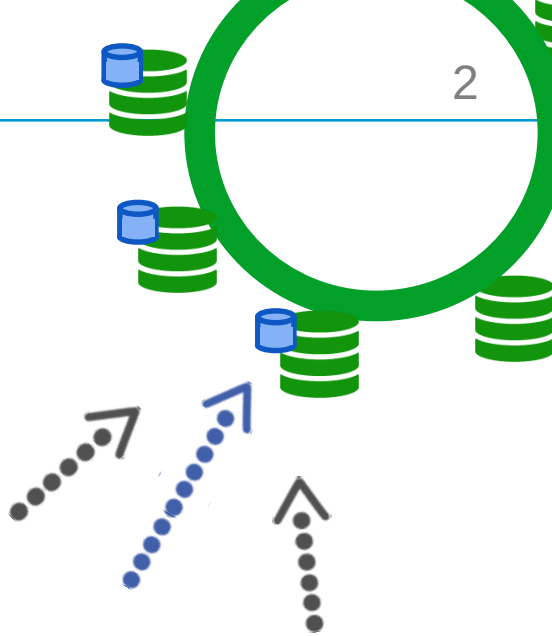
サービスマニュアル

ver 1.1

2017年8月21日

株式会社IDCフロンティア

はじめに



この文書では、当社オブジェクトストレージサービスのバケットを公開するにあたって、
アクセス制限を行うためのPolicy設定方法についてご案内します。

Policy設定に関するご不明な点は、以下をご参照ください。

▼RiakCS PUT Bucket Policy
http://docs.basho.com/riakcs/latest/references/apis/storage/s3/RiakCS-PUT-Bucket-policy/

▼お問い合わせ
IDCFクラウドの「お問い合わせチケット」より、お問い合わせください。

【ご注意点】
当ガイドのご案内は、当社にて検証を行っておりますが、ご利用の際は、
予めお客様にても検証を行い、Policyに問題が無いことをよくご確認の上、ご利用ください。

IDCFrontier

Policyの基本設定

当書では、特定のIPアドレス範囲からのみアクセス可能にしたい場合のPolicy 設定方法をご案内します。

■**バケットにPolicyを適用する**（s3cmd を使用した場合の例）

Policy適用コマンド： **s3cmd setpolicy <policy-file> s3://<bucket-name>**

Policyファイルのパス　Policyをかける対象バケット名

上記実行により、Policyファイルが対象のバケットにアップロードされます。アップロードされたPolicyファイルは表示されません。
修正の際は、上書き保存してください。

■**Policyファイルの記述項目説明（例）**

```
{
  "Id": "Policy1381122551879",
  "Statement": [
    {
      "Sid": "Stmt1381122547899",
      "Action": [ "s3:GetObject" ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::testbucket/*",
      "Condition": {
        "IpAddress": {
          "aws:SourceIp": “xxx.xxx.xxx.xxx/xx”
        },
        "NotIpAddress": {
          "aws:SourceIp": " yyy.yyy.yyy.yyy/yy"
        }
      },
      "Principal": {
          "AWS": [ "*" ]
      }
    }
  ]
}
```

※JSON 形式で記述します。

Policyファイルは、左記例のような内容を手動で入力いただき作成します。
ファイル名、ファイルの置き場所は任意です。

・**Id :**　ポリシーのIDを指定。（任意の英数字を入力）APIユーザー内で重複不可。

・**Statement :** ポリシーの主要素。必須。下記の複数の要素を持つ。

・**Sid :** StatementID（任意の英数字を入力）APIユーザー内で重複不可。

・**Action:** 適用する作業内容を記述する。

・**Effect:** Allow … 指定した内容に対しアクセスを許可する。
Deny … 指定した内容に対しアクセスを拒否する。

・**Resource:** arn:aws:s3:::<Policyの対象バケット名>/*　を記述する。
対象サービス
＊この下線部値は固定ですのでこのまま入力してください。

・**Condition:** ポリシーの条件を指定します。
- IpAddress … 指定したIPアドレスがEffectの範囲対象となる。
- NotIpAddress … 指定したIPアドレスがEffectの範囲外となる。
└ - aws:SourceIp(IP アドレスの制御)
- aws:SecureTransport(SSL利用許可／拒否の制御
値は“true”/“false”で指定)

・**Principal :** アクセスを許可するユーザーやアカウントを記述する。

IDCFrontier

Policyのアクセス制限参考表

EffectとConditionの指定内容により、アクセスが許可されるのか、拒否されるのか
結果が複雑に変わってきます。
下記の表は、どのように設定を行うと許可され、または拒否さるのかを一覧で表したものです。

○･･･アクセス許可される
× ･･･アクセス拒否される

アクセス元での認証情報(APIｷｰ)の有無	アクセス方法	Effect	Allow			Deny		
		SourceIPとConditionとの合致	合致しない	IpAddressのみに合致	NotIpAddress & IpAddress両方に合致	合致しない	IpAddressのみに合致	NotIpAddress & IpAddress両方に合致
有り	s3cmd など	アクセス結果→	○	○	○	○	×	○
無し	wget Curl など		×	○	×	×	×	×

IDCFrontier

アクセス制限例１【 Allow / IpAddress 】を設定

Policyファイル記述

```
{
  "Id": "Policy1381122551879",
  "Statement": [
    {
      "Sid": "Stmt1381122547899",
      "Action": [ "s3:GetObject“ ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::ptest/*",
      "Condition": {
        "IpAddress": {
          "aws:SourceIp”: "210.140.144.0/24"
        }
      },
      "Principal": {
        "AWS": [ "*" ]
      }
    }
  ]
}
```

210.140.144 セグメントからのアクセスは許可される。

検証例：左のPolicyが設定されたバケットにアクセス

210.140.144.106　からアクセス　　IpAddress指定範囲内

①　wget　http://ptest.ds.jp-east.idcfcloud.com/objtest.bin

```
--2014-06-30 10:15:23--  http://ptest.ds.jp-east.idcfcloud.com/objtest.bin
ptest.ds.jp-east.idcfcloud.com をDNSに問いあわせています... 210.140.132.22
ptest.ds.jp-east.idcfcloud.com|210.140.132.22|:80 に接続しています... 接続しました。
HTTP による接続要求を送信しました、応答を待っています... 200 OK
長さ: 8856 (8.6K) [application/octet-stream]
`objtest.bin' に保存中
100%[======================================>] 8,856       --.-K/s 時間 0s
 2014-06-30 10:15:23 (42.5 MB/s) - `objtest.bin‘ へ保存完了 [8856/8856]
```

認証無し　⇒○

210.168.36.157　からアクセス　　IpAddressの指定範囲外

②　wget　http://ptest.ds.jp-east.idcfcloud.com/objtest.bin

```
Resolving ptest.ds.jp-east.idcfcloud.com... 210.140.132.21
Connecting to ptest.ds.jp-east.idcfcloud.com|210.140.132.21|:80... connected.
HTTP request sent, awaiting response... 403 Forbidden
2014-06-30 10:14:12 ERROR 403: Forbidden.
```

認証無し　⇒×

IDCFrontier

アクセス制限例２【 Allow / IpAddress と Not IpAddress 】を設定

Policyファイル記述

```
{
  "Id": "Policy1381122551879",
  "Statement": [
    {
      "Sid": "Stmt1381122547899",
      "Action": [ "s3:GetObject" ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::ptest/*",
      "Condition": {
        "IpAddress": {
          "aws:SourceIp": "210.140.144.0/24"
        },
        "NotIpAddress": {
          "aws:SourceIp": "210.140.144.106/32"
        }
      },
      "Principal": {
          "AWS": [ "*" ]
      }
    }
  ]
}
```

210.140.144 セグメントからのアクセスは許可される。

但し、210.140.144.106 からのアクセスは拒否される。

検証例：左のPolicy設定されたバケットにアクセスした場合

210.140.144.106　からアクセス　　IpAddress指定範囲内
NotIpAddressの指定範囲内でもある

③ wget http://ptest.ds.jp-east.idcfcloud.com/objtest.bin

```
--2014-06-30 13:22:37--  http://bashoplat-ptest.ds.jp-east.idcfcloud.jp/objtest.bin
bashoplat-ptest.ds.jp-east.idcfcloud.jp をDNSに問いあわせています... 210.140.132.2
bashoplat-ptest.ds.jp-east.idcfcloud.jp|210.140.132.2|:80 に接続しています... 接続しました。
HTTP による接続要求を送信しました、応答を待っています... 403 Forbidden
2014-06-30 13:22:37 エラー 403: Forbidden.
```

認証無し ⇒×

210.140.144.160　からアクセス　　IpAddress指定範囲内

④ wget http://ptest.ds.jp-east.idcfcloud.com/objtest.bin

```
--2014-06-30 13:22:59--  http://bashoplat-ptest.ds.jp-east.idcfcloud.jp/objtest.bin
bashoplat-ptest.ds.jp-east.idcfcloud.jp をDNSに問いあわせています... 210.140.132.1
bashoplat-ptest.ds.jp-east.idcfcloud.jp|210.140.132.1|:80 に接続しています... 接続しました。
HTTP による接続要求を送信しました、応答を待っています... 200 OK
長さ: 8856 (8.6K) [application/octet-stream]
`objtest.bin' に保存中
 100%[======================================>] 8,856       --.-K/s 時間 0s
 2014-06-30 13:22:59 (40.0 MB/s) - `objtest.bin‘ へ保存完了 [8856/8856]
```

認証無し ⇒○

210.168.36.157　からアクセス　　IpAddress指定範囲外

⑤ wget http://ptest.ds.jp-east.idcfcloud.com/objtest.bin

```
--2014-06-30 13:22:22--  http://bashoplat-ptest.ds.jp-east.idcfcloud.jp/objtest.bin
Resolving bashoplat-ptest.ds.jp-east.idcfcloud.jp... 210.140.132.2
Connecting to bashoplat-ptest.ds.jp-east.idcfcloud.jp|210.140.132.2|:80... connected.
HTTP request sent, awaiting response... 403 Forbidden
2014-06-30 13:22:22 ERROR 403: Forbidden.
```

認証無し ⇒×

アクセス制限例３【 Deny / IpAddress 】を設定

Policyファイル記述

```
{
  "Id": "Policy1381122551879",
  "Statement": [
    {
      "Sid": "Stmt1381122547899",
      "Action": [ "s3:GetObject“ ],
      "Effect": "Deny",
      "Resource": "arn:aws:s3:::ptest/*",
      "Condition": {
        "IpAddress": {
          "aws:SourceIp": "210.140.144.0/24"
        }
      },
      "Principal": {
        "AWS": [ "*" ]
      }
    }
  ]
}
```

210.140.144.0のセグメントからのアクセスは拒否される。

認証（APIキー）の有無に関わらず。

検証例：左のpolicy設定されたバケットにアクセスした場合

210.140.144.106　からアクセス　　IpAddress指定範囲内

⑥ -1 **s3cmd get s3://ptest/dummy.bin /tmp/dummy.bin**

```
s3://ptest/dummy.bin -> /tmp/dummy.bin  [1 of 1]
ERROR: S3 error: 404 (Object Not Found):
```

認証有り ⇒×

⑥ -2 **wget http://ptest.ds.jp-east.idcfcloud.com/dummy.bin > /tmp/dummy.bin**

```
--2014-07-01 12:03:39--  http://ptest.ds.jp-east.idcfcloud.com/dummy.bin
ptest.ds.jp-east.idcfcloud.com をDNSに問いあわせています... 210.140.132.22
ptest.ds.jp-east.idcfcloud.com|210.140.132.22|:80 に接続しています... 接続しました。
HTTP による接続要求を送信しました、応答を待っています... 403 Forbidden
2014-07-01 12:03:39 エラー 403: Forbidden.
```

認証無し ⇒×

210.168.36.157　からアクセス　　IpAddress指定範囲外

⑦-1 **s3cmd get s3://ptest/dummy.bin /tmp/dummy.bin**

```
s3://ptest/dummy.bin -> /tmp/dummy.bin  [1 of 1]
 541 of 541   100% in    0s    12.54 kB/s  done
```

認証有り ⇒○

⑦-2 **wget http://ptest.ds.jp-east.idcfcloud.com/dummy.bin > /tmp/dummy.bin**

```
--2014-07-01 12:04:43--  http://ptest.ds.jp-east.idcfcloud.com/dummy.bin
Resolving ptest.ds.jp-east.idcfcloud.com... 210.140.132.21
Connecting to ptest.ds.jp-east.idcfcloud.com|210.140.132.21|:80... connected.
HTTP request sent, awaiting response... 403 Forbidden
2014-07-01 12:04:43 ERROR 403: Forbidden.
```

認証無し ⇒×

アクセス制限例４【 Deny / IpAddress と Not IpAddress 】を設定

Policyファイル記述

```
{
  "Id": "Policy1381122551879",
  "Statement": [
    {
      "Sid": "Stmt1381122547899",
      "Action": [ "s3:GetObject“ ],
      "Effect": "Deny",
      "Resource": "arn:aws:s3:::ptest/*",
      "Condition": {
        "IpAddress": {
          "aws:SourceIp": "210.140.144.0/24"
        },
        "NotIpAddress": {
          "aws:SourceIp": "210.140.144.106/32"
        }
      },
      "Principal": {
        "AWS": [ "*" ]
      }
    }
  ]
}
```

210.140.144.0 のセグメントからのアクセスは、
認証のあるなしに関わらず拒否される。
ただし、210.140.144.106および
210.168.36.157からの認証付きアクセスは許可

210.140.144.106　からアクセス　　IpAddress指定範囲内
NotIpAddressの指定範囲内でもある

⑧−1　s3cmd get s3://ptest/dummy.bin /tmp/dummy.bin

```
s3://ptest/dummy.bin -> /tmp/dummy.bin  [1 of 1]
 541 of 541   100% in    0s     3.07 kB/s  done
```

認証有り ⇒○

⑧−2　wget http://ptest.ds.jp-east.idcfcloud.com/dummy.bin > /tmp/dummy.bin

```
--2014-07-01 13:29:12--  http://ptest.ds.jp-east.idcfcloud.com/dummy.bin
ptest.ds.jp-east.idcfcloud.com をDNSに問いあわせています... 210.140.132.21
ptest.ds.jp-east.idcfcloud.com|210.140.132.21|:80 に接続しています... 接続しました。
HTTP による接続要求を送信しました、応答を待っています... 403 Forbidden
2014-07-01 13:29:12 エラー 403: Forbidden.
```

認証無し ⇒×

210.140.144.160　からアクセス　　IpAddress指定範囲内

⑨−1　s3cmd get s3://ptest/dummy.bin /tmp/dummy.bin

```
s3://ptest/dummy.bin -> /tmp/dummy.bin  [1 of 1]
ERROR: S3 error: 404 (Object Not Found):
```

認証有り ⇒×

⑨−2　wget http://ptest.ds.jp-east.idcfcloud.com/dummy.bin > /tmp/dummy.bin

```
--2014-07-01 13:29:34--  http://ptest.ds.jp-east.idcfcloud.com/dummy.bin
pest.ds.jp-east.idcfcloud.com をDNSに問いあわせています... 210.140.132.21
ptest.ds.jp-east.idcfcloud.com|210.140.132.21|:80 に接続しています... 接続しました。
HTTP による接続要求を送信しました、応答を待っています... 403 Forbidden
2014-07-01 13:29:34 エラー 403: Forbidden.
```

認証無し ⇒×

210.168.36.157　からアクセス　　IpAddress指定範囲外

⑩−1　s3cmd get s3://ptest/dummy.bin /tmp/dummy.bin

```
s3://ptest/dummy.bin -> /tmp/dummy.bin  [1 of 1]
 541 of 541   100% in    0s     13.67 kB/s  done
```

認証有り ⇒○

⑩−2　wget http://ptest.ds.jp-east.idcfcloud.com/dummy.bin > /tmp/dummy.bin

```
--2014-07-01 13:31:41--  http://ptest.ds.jp-east.idcfcloud.com/dummy.bin
Resolving bashoplat-ptest.ds.jp-east.idcfcloud.com... 210.140.132.22
Connecting to ptest.ds.jp-east.idcfcloud.com|210.140.132.22|:80... connected.
HTTP request sent, awaiting response... 403 Forbidden
2014-07-01 13:31:41 ERROR 403: Forbidden.
```

認証無し ⇒×

設定確認と制約について

■ **設定したPolicy内容を確認するコマンド：** s3cmd info s3://<bucket-name>

Policy が設定されていれば、info 情報中の policy: 以降に設定内容が表示されます。
（設定されていなければ none ）と表示されます。

■ **設定の制限：**

現在、以下の制限が有ります。

- **Action ：**「s3:*」（*は全ての意味）は書けません。明示的にActionの内容を指定してください。
  現在、「GetObject」,「DeleteObject」のアクションは設定できます。
  「PutObject」は、動作しません。（httpステータスコード：500 が返ります）
  複数指定する場合は以下の様に記述します。
  "s3:GetObject", "s3: DeleteObject"

- **Condition :**「IpAddress」,「NotIpAddress」 は、各一つずつまでしか設定できません。
  「IpAddress」,「NotIpAddress」内の「SourceIp」は、複数のアドレス
  セグメントを書くことはできません。（１つしか設定できません）

- **principal ：**「*」しか書けません。それ以外は設定できません。

IDCFrontier