

# 【Katacoda環境を利用したLinuCハンズオンセミナー】ファイルの所有者とパーミッション/アカウント管理

- ・ LinuC 101試験の出題範囲対応  
「1.02.1 ファイルの所有者とパーミッション」  
「1.08.1 アカウント管理」

担当：河原木忠司

## ■河原木忠司（かわらぎただし）

- 20数年ほど、講師/エンジニアとして活動しております。
- 最近では講師、研修コンサルティング、執筆業に従事させていただいております。
  - サーバーインフラ系のコース、セキュリティ系のコースを中心に担当させていただいております。

## ■最近執筆したものの



「最短突破 LinuCレベル1  
合格教本 ver.10対応」  
(技術評論社)  
好評発売中です。

[https://gihyo.jp/book/  
2020/978-4-297-11527-2](https://gihyo.jp/book/2020/978-4-297-11527-2)



「標準テキスト CentOS8 構  
築・運用・管理パーフェクトガ  
イド[CentOS Stream対応]」  
(SBクリエイティブ)  
7月21日発売予定、共著。

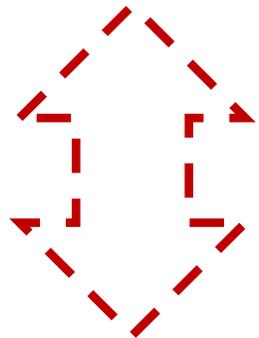
[https://www.sbcr.jp/  
product/4815602567/](https://www.sbcr.jp/product/4815602567/)

## ■LinuCとは

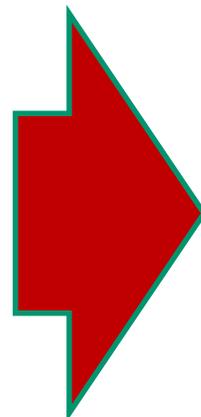
クラウド時代の即戦力エンジニアであることを証明するLinux技術者認定

- ✓現場で「今」求められている新しい技術要素に対応
  - オンプレミス／仮想化・コンテナを問わず様々な環境下でのサーバー構築
  - 他社とのコラボレーションの前提となるオープンソースへの理解
  - システムの多様化に対応できるアーキテクチャへの知見
- ✓全面的に見直した「今」身につけておくべき技術範囲を網羅
  - 今となっては使わない技術やコマンドの削除、アップデート、新領域の取り込み
- ✓Linuxの範疇だけにとどまらない領域までカバー
  - セキュリティや監視など、ITエンジニアであれば必須の領域もカバー

AWSなどの  
パブリッククラウドを  
活用するための技術



間が  
欠けて  
いる状態



AWSなどの  
パブリッククラウドを  
活用するための技術

仮想マシン/コンテナ技術、  
クラウドセキュリティ、  
アーキテクチャ、ほか

オンプレミスの  
サーバーサイドLinux技術

オンプレミスの  
サーバーサイドLinux技術

【今まで/その他】



# 今回のテーマ

- Katacodaとは
- アカウント管理
- 【ハンズオン】 アカウントの追加
- ファイルの所有者とパーミッション
- 【ハンズオン】 パーミッション設定の確認

- ファイルの内容を読み取るには、ファイルの読み取り権限が必要
  - それに加えて、ディレクトリの実行権限が必要
- ファイルを削除するにはファイルの書き込み権限は**必要ない**
  - ディレクトリの書き込み権限が必要
- ディレクトリ内のファイル一覧を読み取るにはディレクトリの読み取り権限が必要
  - ディレクトリ内に存在するファイルの名前はこれで読み取れるが、**属性情報は読み取れない**



これらの内容を実際に動作確認してみる  
 ※最後の項目は、時間に余裕があれば・・・

## ■O'Reilly社で提供している学習用プラットフォーム

<https://www.katacoda.com/>

- 「インタラクティブなライブデモやトレーニング環境を構築するためのプラットフォームを提供」
- Webブラウザベースの学習環境を提供
  - アカウント登録さえすれば、事前準備無しで様々な環境を利用することができる。
  - プログラミング言語やOSなどの技術ごとに様々なテーマが用意されている。
    - テーマによってはシナリオが用意されており、シナリオに沿った学習が可能。
  - 今回、利用するのはCentOSのPlayground
    - シナリオ無しで自由に動作確認ができる「遊び場」を利用。

## ■利用する際の注意点

- 時間制限あり
- ログアウトもしくはは時間制限に達したら、環境は消失



## ■ <https://www.katacoda.com/login> にアクセス

**SNSアカウントでログイン**

**下にスクロール**

**Linux & Operating Systemの [Start Course] をクリック**

**登録したアカウント情報を入力してログイン**

**アカウントの登録**

Log In with Github | Log In with LinkedIn | Log In with Twitter | Log In with Google

or log in using your email

Email Address

Password

Create a new account here.

Machine Learning (39 SCENARIOS)

Linux & Operating Systems (7 SCENARIOS)

Continuous Integration (30 SCENARIOS)

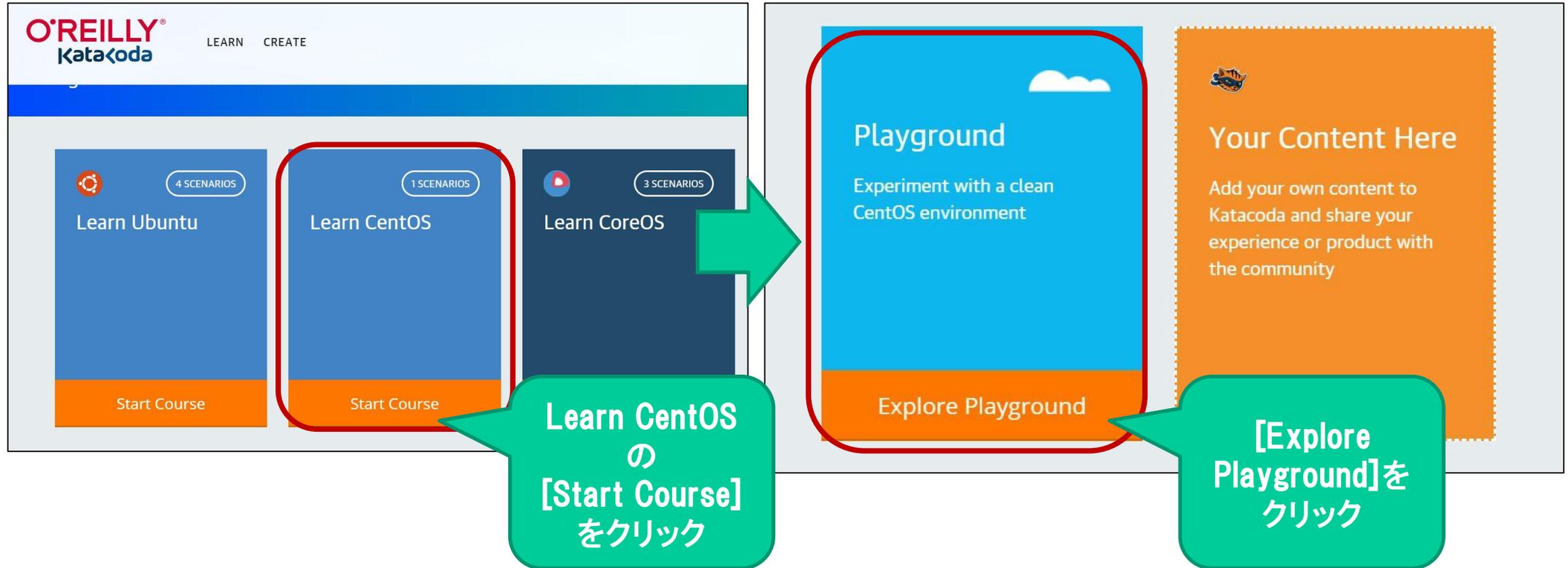
Start Course

Start Course

Observability & (40 SCENARIOS)

Service Proxy (27 SCENARIOS)

50 SCENARIOS



O'REILLY Katakoda KATACODA OVERVIEW & SOLUTIONS CLAIM YOUR PROFILE LOG OUT >

## Welcome!

CentOS Playground

★ Difficulty: Beginner Estimated Time: 10 minutes

START SCENARIO

[START SCENARIO]をクリック

O'REILLY Katakoda KATACODA OVERVIEW & SOLUTIONS CLAIM YOUR PROFILE LOG OUT >

## CentOS Playground

### Hello World

Interested in writing your own scenarios and demos? Visit [www.katacoda.com/teach](http://www.katacoda.com/teach)

CONTINUE

```
Terminal +
Your Interactive Bash Terminal. A safe place to learn and execute commands.
[root@dc126d7706c0 ~]#
```

ターミナル上で、コマンドを実行し、動作確認が可能

- **useradd** [オプション] ユーザー名
  - ユーザーの追加
- **usermod** [オプション] ユーザー名
  - ユーザー設定の変更
- **userdel** [オプション] ユーザー名
  - ユーザーの削除
  - -rでホームディレクトリも一緒に削除
- **groupadd** [オプション] グループ名
  - グループの追加
- **passwd** [オプション] [ユーザー名]
  - パスワードの設定
  - ユーザー名を省略するとログインしているユーザー自身のパスワードを変更
    - この操作に限り、一般ユーザーでも実行可能
  - パスワードが設定されていないユーザーはログイン不可

オプション	説明
-u UID	UIDを設定
-g グループ名/GID	プライマリグループを設定
-G グループ名/GID	セカンダリグループを設定
-aG グループ名/GID	セカンダリグループを追加
-c コメント	コメントを登録
-d ディレクトリ	ホームディレクトリを設定
-s シェル	ログインシェルを設定

- **id** [オプション] ユーザー名
  - ユーザーのIDや所属グループ情報を表示
- **su** [オプション] ユーザー名
  - ユーザー環境の切り替え

今回は、下線のコマンドをハンズオンで使用

## ■登録したユーザーの情報は次の設定ファイルに格納

- **/etc/passwd** : ユーザー情報を保存。パーミッションは644  
`test01:x:500:600::/home/test01:/bin/bash`

ユーザー名

- **/etc/shadow** : パスワード情報を保存。パーミッションは000もしくは400  
`test01:$6$HTUBwjdV$w7YdIKDg/3KRz73D2...:14952:0:99999:7:::`

パスワード情報

**/etc/passwd**  
の記述内容

列	項目	説明
1	ユーザー	ユーザー名
2	パスワード	パスワード。passwdファイルでは「x」と記述されており、/etc/shadowで管理
3	UID	ユーザーに割り当てられているID
4	GID	ユーザーがプライマリグループとして所属しているグループのID
5	コメント	コメント。ユーザーの本名などを記載
6	ホームディレクトリ	ユーザーのホームディレクトリ
7	ログインシェル	ログインしたときに起動するシェル

```
[root@eaf0b1ff0f4d ~]# groupadd testG
```

```
[root@eaf0b1ff0f4d ~]# useradd -g testG user01
```

```
[root@eaf0b1ff0f4d ~]# useradd -g testG user02
```

```
[root@eaf0b1ff0f4d ~]# useradd user03
```

```
[root@eaf0b1ff0f4d ~]# id user01
```

```
uid=1001(user01) gid=1001(testG) groups=1001(testG)
```

```
[root@eaf0b1ff0f4d ~]# id user03
```

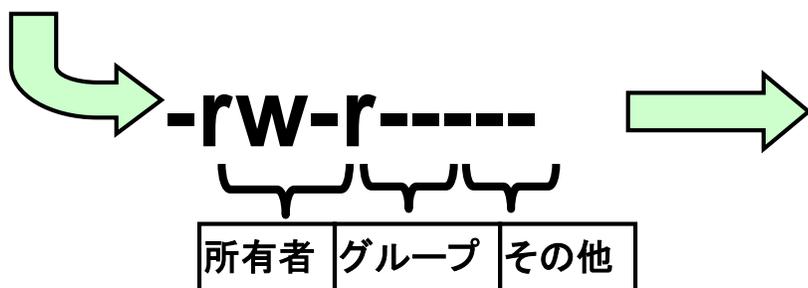
```
uid=1003(user03) gid=1003(user03) groups=1003(user03)
```

## ■LinuC Lv.1試験では、Linuxの基本パーミッションについて出題

- 所有者、所有グループに対して、特別な権限設定が可能
  - **所有者**：既定では、ファイル/ディレクトリの作成者
  - **所有グループ**：所有者が所属するプライマリグループ
  - それ以外は「**その他のユーザー**」

```
[root@localhost ~]# ls -l sample.txt
```

```
-rw-r----- 1 root users 26 12月 9 22:52 sample.txt
```



r	4	読み取り
w	2	書き込み
x	1	実行

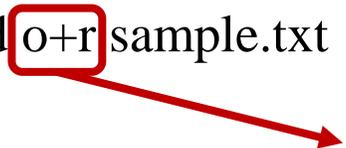
- $6 = 4 + 2$  (読み取り・書き込みが可能)

	ファイル	ディレクトリ
r	ファイル内容の読み取り 例> cat sample.txt	ディレクトリ内のファイル一覧の読み取り 例> ls /sampledir
w	ファイル内容の編集 例> vi sample.txt	ディレクトリ内にファイルを作成・削除 例> rm /sampledir/sample.txt
x	ファイルの実行 例> /bin/ls	ディレクトリにアクセス可能 例> cd /sampledir ディレクトリ内の属性情報の読み取り 例> ls -l /sampledir

- **chown** [オプション] 所有者[:所有グループ] ファイル/ディレクトリ名
  - 所有者の変更（所有グループの変更も可能）
  - rootユーザーのみ実行可能
- **chgrp** [オプション] 所有グループ ファイル/ディレクトリ名
  - 所有グループの変更
  - rootユーザー/所有者が実行可能
- **chmod** [オプション] パーミッション ファイル/ディレクトリ名
  - パーMISSIONの変更
  - rootユーザー/所有者が実行可能
  - chmodコマンドの実行例

– chmod 640 sample.txt

– chmod **o+r** sample.txt



	クラス(対象)		処理		権限
u	所有者	+	追加	r	読み取り
g	所有グループ	-	削除	w	書き込み
o	その他のユーザー	=	付与	x	実行
a	全クラス			s	SUID/SGID
				t	スティッキービット

```
[root@eaf0b1ff0f4d ~]# mkdir /testdir1
```

```
[root@eaf0b1ff0f4d ~]# ls -ld /testdir1
```

```
drwxr-xr-x. 2 root root 4096 Jun 19 09:58 /testdir1
```

ディレクトリの既定のパー  
ミッションは755 or 775  
※umaskの設定による

```
[root@eaf0b1ff0f4d ~]# echo test > /testdir1/user01.txt
```

```
[root@eaf0b1ff0f4d ~]# echo test > /testdir1/testg.txt
```

ファイルを新規作成  
echoコマンドの内容を出力

```
[root@eaf0b1ff0f4d ~]# ls -l /testdir1
```

```
total 8
```

```
-rw-r--r--. 1 root root 5 Jun 19 09:59 testg.txt
```

```
-rw-r--r--. 1 root root 5 Jun 19 09:59 user01.txt
```

ファイルの既定のパーミッ  
ションは644 or 664  
※umaskの設定による

```
[root@eaf0b1ff0f4d ~]# chmod 600 /testdir1/user01.txt
```

```
[root@eaf0b1ff0f4d ~]# chmod 640 /testdir1/testg.txt
```

ファイルのパーミッションと  
所有者/グループを変更

```
[root@eaf0b1ff0f4d ~]# chown user01:testG /testdir1/*
```

```
[root@eaf0b1ff0f4d ~]# ls -l /testdir1
```

```
total 8
```

```
-rw-r-----. 1 user01 testG 5 Jun 19 09:59 testg.txt
```

```
-rw-----. 1 user01 testG 5 Jun 19 09:59 user01.txt
```

上記の操作が正しく行わ  
れたことを確認

```
[root@eaf0b1ff0f4d ~]# su - user01
```

```
Last login: Sat Jun 19 10:01:52 UTC 2021 on pts/0
```

```
[user01@eaf0b1ff0f4d ~]$ cat /testdir1/user01.txt
```

```
test
```

```
[user01@eaf0b1ff0f4d ~]$ cat /testdir1/testg.txt
```

```
test
```

```
[user01@eaf0b1ff0f4d ~]$ echo user01 >> /testdir1/testg.txt
```

```
[user01@eaf0b1ff0f4d ~]$ cat /testdir1/testg.txt
```

```
test
```

```
user01
```

```
[user01@eaf0b1ff0f4d ~]$ exit
```

```
logout
```

user01の環境に切り替え、  
動作確認

作成したどちらのファイルも  
参照できることを確認

書き込みもできていることを  
確認

user01の環境を終了  
rootユーザーの環境に戻る

```
[root@eaf0b1ff0f4d ~]# su - user02
```

```
Last login: Sat Jun 19 10:08:22 UTC 2021 on pts/0
```

```
[user02@eaf0b1ff0f4d ~]$ cat /testdir1/user01.txt
```

```
cat: /testdir1/user01.txt: Permission denied
```

```
[user02@eaf0b1ff0f4d ~]$ cat /testdir1/testg.txt
```

```
test
```

```
user01
```

```
[user02@eaf0b1ff0f4d ~]$ echo user02 >> /testdir1/testg.txt
```

```
-bash: /testdir1/testg.txt: Permission denied
```

```
[user02@eaf0b1ff0f4d ~]$ exit
```

```
logout
```

```
[root@eaf0b1ff0f4d ~]# su - user03
```

```
[user03@eaf0b1ff0f4d ~]$ cat /testdir1/testg.txt
```

```
cat: /testdir1/testg.txt: Permission denied
```

```
[user03@eaf0b1ff0f4d ~]$ exit
```

```
logout
```

user02の環境に切り替え、  
動作確認

user01.txtは読み取り不可

testg.txtは読み取りOK

書き込みは不可

user03はtestGのメンバーでは  
ないので、読み取り不可

```
[root@eaf0b1ff0f4d ~]# mkdir -m 700 /testdir2
[root@eaf0b1ff0f4d ~]# chown user01 /testdir2
[root@eaf0b1ff0f4d ~]# echo test > /testdir2/test.txt
[root@eaf0b1ff0f4d ~]# ls -ld /testdir2
drwx-----. 2 user01 root 4096 Jun 19 10:11 /testdir2
[root@eaf0b1ff0f4d ~]# ls -l /testdir2
total 4
-rw-r--r--. 1 root root 5 Jun 19 10:11 test.txt
[root@eaf0b1ff0f4d ~]# su - user01
Last login: Sat Jun 19 10:12:24 UTC 2021 on pts/0
[user01@eaf0b1ff0f4d ~]$ cat /testdir2/test.txt
test
[user01@eaf0b1ff0f4d ~]$ exit
logout
```

-mオプションで、パーミッションの指定

作成したtest.txt自体のパーミッションはすべてのユーザーに読み取り権限がついていることを確認

所有者であるuser01は/testdir2ディレクトリ内のファイルも参照可能

```
[root@eaf0b1ff0f4d ~]# su - user02
```

```
Last login: Sat Jun 19 10:08:39 UTC 2021 on pts/0
```

```
[user02@eaf0b1ff0f4d ~]$ cat /testdir2/test.txt
```

```
cat: /testdir2/test.txt: Permission denied
```

```
[user02@eaf0b1ff0f4d ~]$ exit
```

```
logout
```

```
[root@eaf0b1ff0f4d ~]# chmod 711 /testdir2
```

```
[root@eaf0b1ff0f4d ~]# su - user02
```

```
Last login: Sat Jun 19 10:16:01 UTC 2021 on pts/0
```

```
[user02@eaf0b1ff0f4d ~]$ cat /testdir2/test.txt
```

```
test
```

```
[user02@eaf0b1ff0f4d ~]$ ls /testdir2
```

```
ls: cannot open directory /testdir2: Permission denied
```

```
[user02@eaf0b1ff0f4d ~]$ exit
```

```
logout
```

ファイルに読み取り権限がある  
はずなのに読み取り不可

ファイルの読み取り  
ファイルの読み取り権限  
+  
ディレクトリの実行権限

ディレクトリに実行権限があれば  
読み取れることを確認

ディレクトリ内のファイル一覧を読み取るには、  
読み取り権限が必要

```
[root@eaf0b1ff0f4d ~]$ chmod 777 /testdir1
```

```
[root@eaf0b1ff0f4d ~]# su - user03
```

```
[user03@eaf0b1ff0f4d ~]$ cat /testdir1/user01.txt
```

```
cat: /testdir1/user01.txt: Permission denied
```

user03はuser01.txtを読み取れないことを確認

```
[user03@eaf0b1ff0f4d ~]$ rm /testdir1/user01.txt
```

```
rm: remove write-protected regular file '/testdir1/user01.txt'? y
```

```
[user03@eaf0b1ff0f4d ~]$ ls /testdir1
```

```
testg.txt
```

user01.txtが削除されていることを確認

ファイルの削除は、ディレクトリの書き込み権限が必要

```
[root@1e1552773b2d ~]# ls -l /etc/shadow
-----. 1 root root 1211 Jun 19 11:02 /etc/shadow
[root@1e1552773b2d ~]# cat /etc/shadow
root:$1$KZxje3XR$yzuN6NJZePb4OV7MoUKJU1::0:99999:7:::
bin:*:17834:0:99999:7:::
:
user01:!!!:18797:0:99999:7:::
user02:!!!:18797:0:99999:7:::
user03:!!!:18797:0:99999:7:::
```

パーミッション:000  
誰も何もできないという設定

rootユーザーはパーミッション  
設定の制約を受けずにファイル  
の読み書きが可能

```
[root@1e1552773b2d ~]# chmod 444 /testdir1
[root@1e1552773b2d ~]# su - user03
Last login: Sat Jun 19 11:05:37 UTC 2021 on pts/0
[user03@1e1552773b2d ~]$ ls -l /testdir1
ls: cannot access /testdir1/testg.txt: Permission denied
total 0
-????????? ? ? ? ?      ? testg.txt
```

ディレクトリの読み取り権限があるので、ファイルの存在は確認できるが、パーミッションやタイムスタンプなどの属性情報は読み取れない

ファイル属性の読み取りは、ディレクトリの実行権限が必要

- ご参加いただき、ありがとうございました。
- ご質問がありましたら、よろしく願いたします。
  - ・答えきれなかったご質問については、後日YouTube動画公開の際に掲載させていただきます。
- 参考文献



「最短突破 LinuCレベル1  
合格教本 ver.10対応」(技  
術評論社)  
好評発売中です。



「標準テキスト CentOS8 構  
築・運用・管理パーフェクトガ  
イド[CentOS Stream対応]」  
(SBクリエイティブ)



「Linux標準教科書」(LPI-  
Japan)  
※オンラインでダウンロード  
して利用できます