

??????

????????

- [SSL??](#)
  - [SSL??????????](#)
  - [SSL??????????](#)

SSL??

SSL??

# SSL???????????

????????????????

??

????SSL??????

- ??????
- ???????

????????????????????????????????

## 1.???????????????

- ?????????????????

```
openssl x509 -pubkey -in /etc/certs/hoge.example.com.crt -noout | openssl md5
```

? (stdin)= [ ]

/etc/certs/hoge.example.com.crt???SSL????????????

- ?????????????????

```
openssl pkey -pubout -in /etc/private/hoge.example.com.key | openssl md5
```

? (stdin)= [ ]

/etc/private/hoge.example.com.key???SSL????????????

????????????????????????????2????????????????????

## 2a.???????????????? (????????????)

????????????????

- ?????????????????

```
openssl x509 -issuer_hash -noout -in /etc/certs/hoge.example.com.crt
```

/etc/certs/hoge.example.com.crt???SSL????????????

- ?????????????????

```
openssl x509 -subject_hash -noout -in /etc/certs/hoge.sample.com.CA.crt
```

/etc/certs/hoge.sample.com.CA.crt????SSL????????????????

??2????????????????????????????????????????

## 2b.???????????????? (????????????????)

Let's Encrypt????????????????????

- ?????????????????

```
openssl x509 -issuer_hash -noout -in /etc/certs/hoge.example.com.crt
```

- ?????????????????

```
sed -n -e'1d' -e'/BEGIN/, $p' /etc/certs/hoge.example.com.crt | openssl x509 -subject_hash -noout
```

??2????????????????????????????????????????

SSL??

# SSL??????????

????????????????????????????

## ?????SSL????????????????

```
openssl x509 -noout -dates -subject -in /etc/certs/hoge.sample.com.crt
```

/etc/certs/hoge.sample.com.crt????????????????

### ??????

```
notBefore=Jan 26 06:01:26 2023 GMT
notAfter=Feb 22 14:59:00 2024 GMT
subject= /C=JP/ST=Kuken-Island/L=Rasen-Boden/O=Atelier-of-Ryza/CN=atelier.reisalin.com
```

????CSR????CN????????????