

SSH FIDO2

Zumpyx

2026-06-09

~/ssh/config
SSH FIDO2 conf.d
ControlMaster

1. 環境構築

SSH FIDO2

```
# 環境構築
mkdir -p ~/.ssh/conf.d ~/.ssh/keys ~/.ssh/controlmasters
touch ~/.ssh/config

# 権限設定
chmod 700 ~/.ssh/conf.d ~/.ssh/keys ~/.ssh/controlmasters
chmod 600 ~/.ssh/config
```

2. FIDO2 vs U2F

U2F (FIDO2 / U2F)

Prod Bastion FIDO2

```
cd ~/.ssh/keys

# FIDO2 Ed25519
# -0 resident:
# -0 verify-required: PIN
ssh-keygen -t ed25519-sk \
  -0 resident \
  -0 verify-required \
  -0 application="ssh:Cloudhost-Sens-2026" \
```

```
-C "Cloudhost-Sens-2026" \  
-f id_ed25519_sk_sens
```

Ed25519 (Ed25519)

Dev Ed25519 RSA

```
# Ed25519  
ssh-keygen -t ed25519 \  
-O application="ssh:Standard-2026" \  
-C "Standard-2026" \  
-f id_ed25519_std  
  
# Passphrase  
ssh-keygen -p -f ~/.ssh/keys/id_ed25519_std
```

3. SSH

Include

~/.ssh/config

```
# macOS UserKeychain  
IgnoreUnknown UserKeychain  
  
#  
Include ~/.ssh/conf.d/*.conf
```

~/.ssh/conf.d/10-sensitive.conf

Bastion/Prod

```
# 10-sensitive.conf  
Host bastion prod core-* sensitive  
# Agent  
IdentitiesOnly yes  
IdentityFile ~/.ssh/keys/id_ed25519_sk_sens1  
IdentityFile ~/.ssh/keys/id_ed25519_sk_sens2  
  
# SSH Agent  
IdentityAgent none  
AddKeysToAgent no  
ForwardAgent no  
  
StrictHostKeyChecking yes
```

```
PasswordAuthentication no
LogLevel VERBOSE
```

XXXXXXXXXX ~/.ssh/conf.d/20-access.conf

XXXXXXXXXXXXXXXXXXXXX Socks5 XXXXXXXXXXXXXXXX

```
# 20-access.conf
```

```
Host core-kali
  HostName 52.52.50.188
  User kali
  Port 22
  PubkeyAuthentication yes
  IdentitiesOnly yes
  IdentityFile ~/.ssh/keys/id_ed25519_sk_sens1
```

```
Host test-vm-kali
  HostName 192.168.56.129
  User kali
  Port 22
  IdentitiesOnly yes
  IdentityFile ~/.ssh/keys/id_ed25519_std
  IdentityFile ~/.ssh/keys/id_ed25519_standard
  DynamicForward 1080 # XXXXX Socks5 XXXXXX
  PasswordAuthentication no
```

```
Host commando-win
  HostName 192.168.95.155
  User admin
  Port 22
  IdentitiesOnly yes
  IdentityFile ~/.ssh/keys/id_ed25519_std
  IdentityFile ~/.ssh/keys/id_ed25519_standard
```

XXXXXXXXXX ~/.ssh/conf.d/90-defaults.conf

XXXXXXXXXXXXXXXXXX ControlMasterXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX TCP X
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

```
# 90-defaults.conf
```

```
Host *
  # XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
  ServerAliveInterval 30
  ServerAliveCountMax 3
  TCPKeepAlive yes

  # XXXXXX
```

```

IdentitiesOnly yes
ForwardAgent no
AddKeysToAgent no
HashKnownHosts yes

# 禁用 TCP 监听
ControlMaster auto
ControlPath ~/.ssh/controlmasters/%C
ControlPersist 10m

# 禁用 ASCII 艺术图 MITM 攻击
VisualHostKey yes

```

4. 配置 SSH

配置 SSH 配置文件

```

~/.ssh/conf.d/ 目录下创建 dotfiles 文件
keys/ 目录下创建 .gitignore 文件

```

配置 SSH

- 配置 SSH 配置文件 Bilibili 密钥 - 配置 SSH 密钥 Fido2 SSH-Agent SSH 密钥