



## Tectia SSH 6.6.7 および Tectia Quantum SSH 6.6.7 に対応されている各種アルゴリズム一覧

### Ciphers

以下の暗号化アルゴリズムがサポートされています（デフォルトでは太字の暗号が許可されています）。

- AES-128-CBC
- **AES-128-CTR**
- AES-192-CBC
- **AES-192-CTR**
- AES-256-CBC
- **AES-256-CTR**
- **CryptiCore (Tectia)**
- 3DES
- SEED (Tectia)
- Arcfour
- Blowfish
- Twofish
- Twofish-128
- Twofish-192
- Twofish-256
- **AEAD\_AES\_128\_GCM**
- **AEAD\_AES\_256\_GCM**
- **AES256-GCM (OpenSSH)**
- **AES128-GCM (OpenSSH)**

以下の Ciphers は FIPS モードで動作できません。

- CryptiCore (Tectia)
- Arcfour
- Blowfish
- Twofish
- Twofish-128
- Twofish-192
- Twofish-256
- SEED (Tectia)

### MACs

以下の MAC アルゴリズムがサポートされています（デフォルトでは太字の MAC が許可されています）。

- **CryptiCore (Tectia)**
- **HMAC-SHA2-256**
- **HMAC-SHA256-2 (Tectia)**
- HMAC-SHA224 (Tectia)
- HMAC-SHA256 (Tectia/0ld)
- HMAC-SHA384 (Tectia)
- **HMAC-SHA2-512**
- **HMAC-SHA512 (Tectia)**
- HMAC-SHA2-256-ETM (OpenSSH)
- HMAC-SHA2-512-ETM (OpenSSH)
- HMAC-SHA1-96
- **HMAC-SHA1**
- HMAC-SHA1-96
- HMAC-SHA1-ETM (OpenSSH)
- HMAC-SHA1-96-ETM (OpenSSH)
- HMAC-MD5
- HMAC-MD5-96
- HMAC-MD5-ETM (OpenSSH)
- HMAC-MD5-96-ETM (OpenSSH)

以下の MACs は FIPS モードで動作できません。

- CryptiCore (Tectia)
- HMAC-MD5
- HMAC-MD5-96
- HMAC-MD5-96-ETM (OpenSSH)
- HMAC-MD5-ETM (OpenSSH)
- HMAC-SHA-1-96
- HMAC-SHA1-96-ETM (OpenSSH)
- HMAC-SHA224 (Tectia)
- HMAC-SHA256 (Tectia/0ld)
- HMAC-SHA256-2 (Tectia)
- HMAC-SHA384 (Tectia)
- HMAC-SHA512 (Tectia)



## Host key and Public Key Signature algorithms

以下の鍵署名アルゴリズムがサポートされています（デフォルトでは太字のホスト鍵アルゴリズムが許可されています）。

- **rsa-sha2-512**
- **rsa-sha2-256**
- ssh-dss
- ssh-rsa
- ssh-rsa-cert-v01 (OpenSSH)
- ssh-dss-cert-v01 (OpenSSH)
- ssh-dss-sha224 (Tectia)
- ssh-dss-sha256 (Tectia)
- ssh-dss-sha384 (Tectia)
- ssh-dss-sha512 (Tectia)
- ssh-rsa-sha224 (Tectia)
- **ssh-rsa-sha256 (Tectia)**
- ssh-rsa-sha384 (Tectia)
- ssh-rsa-sha512 (Tectia)
- **rsa-sha2-256-cert-v01 (OpenSSH)**
- **rsa-sha2-512-cert-v01 (OpenSSH)**
- x509v3-ssh-dss
- x509v3-ssh-rsa
- **x509v3-rsa2048-sha256**
- x509v3-sign-dss
- x509v3-sign-rsa
- x509v3-sign-dss-sha224 (Tectia)
- x509v3-sign-dss-sha256 (Tectia)
- x509v3-sign-dss-sha384 (Tectia)
- x509v3-sign-dss-sha512 (Tectia)
- x509v3-sign-rsa-sha224 (Tectia)
- **x509v3-sign-rsa-sha256 (Tectia)**
- x509v3-sign-rsa-sha384 (Tectia)
- x509v3-sign-rsa-sha512 (Tectia)
- **ecdsa-sha2-nistp256**
- **ecdsa-sha2-nistp384**
- **ecdsa-sha2-nistp521**
- **ecdsa-sha2-nistp256-cert-v01 (OpenSSH)**
- **ecdsa-sha2-nistp384-cert-v01 (OpenSSH)**
- **ecdsa-sha2-nistp521-cert-v01 (OpenSSH)**
- x509v3-ecdsa-sha2-nistp256
- x509v3-ecdsa-sha2-nistp384
- x509v3-ecdsa-sha2-nistp521
- **ssh-ed25519**
- **ssh-ed25519-cert-v01 (OpenSSH)**

以下の Host key algorithms は FIPS モードで動作できません。

- ssh-dss
- ssh-rsa
- ssh-dss-cert-v01 (OpenSSH)
- ssh-rsa-cert-v01 (OpenSSH)
- x509v3-ssh-dss
- x509v3-ssh-rsa
- x509v3-sign-dss
- x509v3-sign-rsa

## KEXs

以下の KEX アルゴリズムがサポートされています（デフォルトでは太字の KEX が許可されています）。

- DH-Group1-SHA1
- DH-Group14-SHA1
- DH-Group14-SHA224 (Tectia)
- **DH-Group14-SHA256**
- **DH-Group14-SHA256 (Tectia)**
- DH-Group15-SHA256 (Tectia)
- DH-Group15-SHA384 (Tectia)
- DH-Group16-SHA384 (Tectia)
- **DH-Group16-SHA512**
- DH-Group16-SHA512 (Tectia)
- **DH-Group18-SHA512**
- DH-Group18-SHA512 (Tectia)
- **DH-GEX-SHA256**
- DH-GEX-SHA1
- DH-GEX-SHA224 (Tectia)
- DH-GEX-SHA384 (Tectia)
- DH-GEX-SHA512 (Tectia)
- ECDH-NISTP256



- ECDH-NISTP384
- ECDH-NISTP521

- Curve25519-sha256
- Curve25519-sha256 (libssh)

以下の KEX は、Tectia Quantum 版でのみサポートされています (デフォルトでは太字の KEX が許可されています)。

- PQC: **mlkem1024nistp384-sha384** (Tectia)
- PQC: **mlkem768nistp256-sha256** (Tectia)
- PQC: **mlkem768x25519-sha256** (Tectia)
- PQC: **ecdh-nistp521-kyber1024-sha512** (Tectia)
- PQC: **curve448-kyber1024-sha512** (Tectia)
- PQC: **curve25519-frodoKem1344-sha512** (Tectia)
- PQC: **sntrup761x25519-sha512** (OpenSSH)

以下の KEX は FIPS モードで動作できません。

- DH-Group1-SHA1
- DH-GEX-SHA1
- DH-GEX-SHA224 (Tectia)
- DH-GEX-SHA-256
- DH-SHA-384 (Tectia)
- DH-SHA-512 (Tectia)