# Tectia Client/Server で対応されている各種アルゴリズム一覧

## Ciphers

以下の暗号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
- Arcfour
- Blowfish
- Twofish
- Twofish-128
- Twofish-192
- Twofish-256

FIPS モードで動作する暗号は 3DES、CBC モード及び CTR モードの AES-128、AES-192、及び AES-256 です。

## MACs

以下の MAC 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）。

- **HMAC-SHA1**
- **HMAC-SHA1-96**
- **HMAC-SHA256**
- **HMAC-SHA256-2 (Tectia/Old)**
- **HMAC-SHA224 (Tectia)**
- **HMAC-SHA256 (Tectia)**
- **HMAC-SHA384 (Tectia)**
- **HMAC-SHA512**
- **HMAC-SHA512 (Tectia)**
- **CryptiCore (Tectia)**
- HMAC-MD5
- HMAC-MD5-96

上記各アルゴリズムの全ての HMAC-SHA （HMAC-SHA1 及び HMAC-SHA2 共）が FIPS モードで動作します。

## Host key algorithms

以下のホスト鍵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）。

- **ssh-dss**
- **ssh-rsa**
- 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)
- **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
- x509v3-ecdsa-sha2-nistp256
- x509v3-ecdsa-sha2-nistp384
- x509v3-ecdsa-sha2-nistp521

## KEXs

以下のホスト KEX 方式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 (Tectia)**
- DH-Group15-SHA256 (Tectia)
- DH-Group15-SHA384 (Tectia)
- DH-Group16-SHA384 (Tectia)
- DH-Group16-SHA512 (Tectia)
- 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

Windows 上ではサポートされている全ての KEX が FIPS モードで動作します。
FIPS 認証の暗号ライブラリの詳細に付いては Cryptographic library の項を参照して下さい。