Tectia Client/Server 6.5.1 および 6.5.2 で対応されている各種アルゴリズム一覧

Ciphers

以下の暗号化方式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)
- chacha20-poly1305 (OpenSSH)
- idea-CBC
- rijndael-CBC (Tectia)
- cast128-CBC

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

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）。

- **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)**

KEXs

以下の 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**
- **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)**

curve25519-sha256 (libssh) は、どのプラットフォームでも FIPS モードでサポートされていません。
その他のサポートされる KEX は、Linux、Windows、Solaris、HPUX Itanium 上で FIPS モードで動作することができます。

ただし、HP-UX PA-RISC と IBM AIX では、OpenSSL 暗号ライブラリバージョン 0.9.8 の問題により、以下の KEX は FIPS モードで動作できません。

- DH-Group15-SHA256 (Tectia)
- DH-Group15-SHA384 (Tectia)
- ECDH-NISTP256
- ECDH-NISTP384
- ECDH-NISTP521