SSL(Secure Socket Layer)機能使用方法

第１版　２００９年６月２５日

対応製品

本アプリケーションノートは、弊社取り扱いの次の ezTCP 製品に対応しています。

弊社対応 ezTCP 製品：CSE-M32

動作確認

本アプリケーションノートは、弊社取り扱いの以下の機器、ソフトウェアにて動作確認を行っています。

動作確認を行った機器、ソフトウェア

OS	WindowsXP SP3
ハードウェア	CSE-M32
ソフトウェア	ezManager v3.0a
	TCP-VSP for ezTCP v1.20
	コマンドプロンプト
	ハイパーターミナル v5.1

■本製品の内容及び仕様は予告なしに変更されることがありますのでご了承ください。

目　次

１．概要

１．１　概要

本製品では多様なネットワーク環境下での利用を考慮して、様々なセキュリティ機能が用意されています。
本アプリケーションノートは、それらセキュリティ機能の一つである「SSL」について説明します。

１．２　SSL について

SSL（Secure Socket Layer）とは暗号化プロトコルの一つで、データ通信の安全性を確保するための技術です。

通常、ネットワークでのデータ通信は、平文(暗号化されていない文)でやり取りされており、通信をキャプチャすることで容易に通信内容を確認することが可能です。
SSL を使用することで通信内容が暗号化され、通信内容を把握することが困難になります。

SSL(Secure Socket Layer)は、Netscape 社によって開発され、後に IETF(Internet Engineering TaskForce)によって TLS(Transport Layer Security)という名称で標準化されました。
本製品でサポートしているバージョンは SSL3.0/TLS1.0 になり、4 つの通信モード（T2S/COD/ATC/U2S）のうち、TCP プロトコルの 3 つ（T2S/COD/ATC）で使用することが可能です。

１．３　使用環境について

本アプリケーションノートは、下表に示すシリアルの設定値とネットワークの設定値を使用して説明しますが、これらの設定値はお客様の使用環境に合わせて変更してください。

	PC	本体
通信速度	38400	38400
データ長	8	8
ストップビット	1	1
パリティ	NONE	NONE
フロー制御	NONE	NONE

Table 1.3-1　シリアルの設定値

	PC	本体
IP アドレス	192.168.1.201	192.168.1.200
サブネットマスク	255.255.255.0	255.255.255.0
ポート番号	51000	50000

Table 1.3-2　ネットワークの設定値

２．SSL の設定

２．１　SSL 機能設定

SSL 機能を使用する際は、ezManager のオプションタブ内の[Option]欄にある SSL のチェックボックスをチェックします。

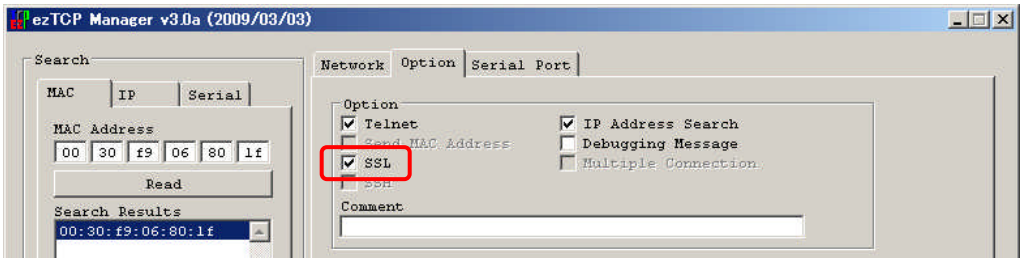

Fig 2.1-1 SSL 設定画面

これで SSL 機能が使用可能になりますが、本体をサーバモードで動作させる際には、次項「2.2　公開鍵･秘密鍵と証明書の作成」の操作が必要になります。
その際、telnet による接続を行いますので、[Option]欄にある Telnet のチェックボックスをチェックしてください。

２．２　公開鍵･秘密鍵と証明書の作成

SSL 機能をサーバモードで動作させる場合には、公開鍵･秘密鍵と証明書が必要になります。
本項では、これら公開鍵･秘密鍵と証明書の作成方法について説明します。

公開鍵･秘密鍵と証明書作成時に使用するコマンドを以下に示します。

項目	コマンド	説明
RSA KEY（公開鍵・秘密鍵）	rsa keygen <key length>	RSA KEY 作成　keylength は 512/768/1024 から指定
	rsa key	作成した RSA KEY の確認
	rsa test	作成した RSA KEY のテスト
証明書	cert new	作成した RSA KEY から証明書を作成
	cert view	作成した証明書を確認
設定保存	ssl save aa55cc33	作成した鍵と証明書を本体に保存

Table 2.2-1　コマンド一覧

① 本体の接続

公開鍵･秘密鍵と証明書を作成するため本体と PC を下図のように接続してください。

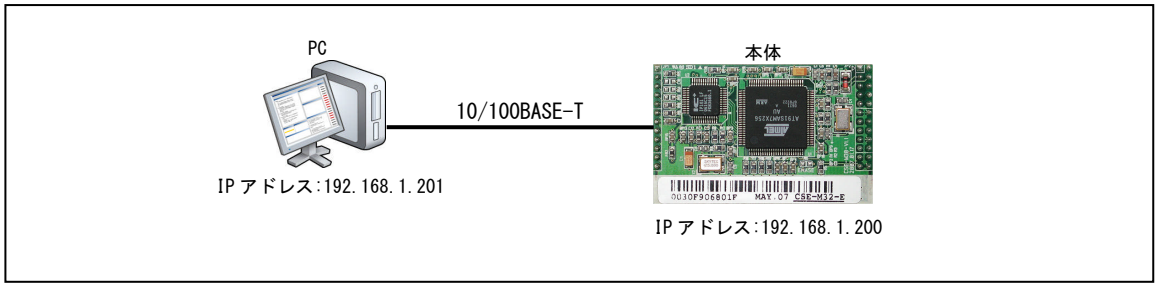

Fig 2.2-1　本体の接続(公開鍵･秘密鍵と証明書作成時)

② 本体の設定

ezManager にて OPTION タブ内の[OPTION]欄にある[telnet]と[ssl]のチェックボックスがチェックされているか確認します。

③ Telnet 接続

本体(IP アドレス 192.168.1.200、ポート 23)にコマンドプロンプトを使用して、telnet 接続します。

なお、WindowsVista のコマンドプロンプトで Telnet コマンドを使用するには、Telnet クライアントをインストールしている必要があります。

```
C:¥Documents and Settings¥user>telnet 192.168.1.200
```

＊ C:¥Documents and Settings¥user>は使用する PC によって異なります。

接続すると下記の文字が表示されます。

```
CSE-M32 Management Console v1.2E Sollae Systems
lsh>
```

④ RSA KEY(公開鍵･秘密鍵)を作成

本製品は 512 と 768 及び 1024byte の RSA KEY をサポートしています。RSA KEY を大きくするほど、より安全に通信が行えますが、作成時間は長くなります。

1024byte の鍵を作成する場合には、約 1 分程度の時間が必要です。

RSA KEY を作成するため『rsa keygen<key length>』を実行してください。

RSA KEY の値は、作成する度に異なります。

```
lsh>rsa keygen 1024
average 50sec required to find two 512bits prime numbers, please wait..
rsa: find 512bits random prime p..1 2 5 7 10 11 16 22 23 25 28 35 38 43 46 61 67 68 71 77 80 85 88 91 92
98 100 101 103 110 115 122 128 131 137 140 145 148 158 161 172 173 191 197
... 中略
3 224 227 233 241 244 251 263 274 281 283 296 314 317 322 326 329 found
rsa: RSA key pair(public/private key) generated.
rsa: key validation OK
lsh>
```

鍵が作成されると『RSA key pair(public/private key) generated.』と『key validation OK』が表示されますのでご確認ください。

⑤ RSA KEY のテスト

『rsa test』を入力して、RSA KEY が正常に作成されたことをご確認ください。

```
lsh>rsa test
* random plain text encrypt/decrypt test *
rsa: key validation OK
public key encryption... done
private key decryption... done
verify ok
private key encryption... done
public key decryption... done
verify ok
```

『rsa key』を入力して、RSA KEY の内容を確認することができます。

```
lsh>rsa key
RSA public modulus: 1024 bits
  + f2:c5:d0:38:0e:67:36:00:22:41:32:98:9f:8e:1e:d8
  + 55:4c:88:f9:53:21:f6:b5:09:5d:0e:ed:5a:b8:72:31
... 中略
  + 30:9d:9d:b3:0a:14:cc:85:4f:a5:ef:25:34:a4:3c:fa
  + e7:c2:db:5f:49:5c:30:2e:69:76:4a:dd:30:82:20:9f
RSA public exponent: 24 bits
  + 01:00:01
lsh>
```

⑥ 証明書の作成

次に、証明書を作成します。『cert new』を実行して、証明書を作成してください。

証明書には、信頼された第三者機関の認証局(CA)から発行され有効性が保障されている公認証明書と、認証局を使用せず発行者自身が署名した自己署名証明書の 2 種類があります。

今回作成する証明書は、自己署名証明書です。

証明書には、IP アドレス情報が含まれておりますので、本体の IP アドレスが変更された時には証明書を新たに作成してください。

```
lsh>cert new
generating self-signed host certificate...694 done
-----BEGIN CERTIFICATE-----
MIICsjCCAhugAwIBAgIBATANBgkqhkiG9w0BAQQFADCBlTELMAkGA1UEBhMCS1Ix
EDAOBgNVBAgTB0luY2hlb24xDjAMBgNVBAcTBU5hbUd1MRcwFQYDVQQKEw5Tb2xs
... 中略
rhQmvletPXGRnxs4xU4gpLeB8zzWHitcsAgPbf8Ex4ae5LyBZVUCldymbpeKHfqe
7XdQ5Ki3sAm2OSO18bzPKj6NUZGt1A==
-----END CERTIFICATE-----
lsh>
```

証明書が作成されると『-----END CERTIFICATE-----』が表示されますのでご確認ください

⑦　作成した証明書の確認

『cert view』を入力して、作成した証明書をご確認ください。

```
lsh>cert view
ssl: + Issuer
ssl: +   country / KR
ssl: +   state or province / Incheon
ssl: +   locality / NamGu
ssl: +   organization / Sollae Systems
ssl: +   organizationUnit / Research
ssl: +   common / 192.168.1.200
ssl: +   email / support@eztcp.com
ssl: + Validity
ssl: +   notAfter  500101000000Z
ssl: +   notBefore 491231235959Z
ssl: + Subject
ssl: +   country / KR
ssl: +   state or province / Incheon
ssl: +   locality / NamGu
ssl: +   organization / Sollae Systems
ssl: +   organizationUnit / Research
ssl: +   common / 192.168.1.200
ssl: +   email / support@eztcp.com
ssl: + Public key OID: 1.2.840.113549.1.1.1. PKCS #1 RSA
ssl: + Extension OID: 2.5.29.19.
ssl: +   30:03:01:01:ff
ssl: + Signature Algorithm OID: 1.2.840.113549.1.1.4. md5WithRSAEncryption
lsh>
```

IP アドレス部分が『common / 192.168.1.200』となっていることをご確認ください。

⑧　RSA KEY と証明書を本体に保存

SSL を動作させるために、RSA KEY と証明書を本体に保存します。『ssl save aa55cc33』を入力して、保存してください。

```
lsh>ssl save aa55cc33
save key...RSA CERT_host ok
lsh>
```

２．３　注意事項

SSL は、データ通信を暗号化しセキュリティ性を向上させる為に有効な機能ですが、本製品で使用する上では次の点にご注意ください。

(1)IP 通信相手は SSL に対応している必要があります

本体側のみ SSL 機能を使用している場合は正しいデータ通信が行われません。

SSL 機能を使用する場合には、TCP 接続先／元も SSL に対応している必要があります。

(2)UDP 通信モード U2S(UDP)では使用することができません

ezManager にて SSL 機能の使用を選択している状態で、通信モードとして U2S を選択するとエラーダイアログが表示されます。

すでに通信モードとして U2S が選択された状態で、SSL 機能の使用を選択すると、通信モードが T2S に変更されます。

(3)SSH 機能と併用して使用することができません

本製品でサポートされているもう一つのセキュリティ設定「SSH」とは排他利用となります。

ezManager にて SSL 機能の使用を選択すると、SSH 機能の使用選択ができなくなります。

(4)Telnet COM Port Control(RFC2217)機能と併用して使用することができません

本製品でサポートされている通信機能の追加オプション「Telnet COM Port Control(RFC2217)」とは排他利用となります。

ezManager にて SSL 機能の使用を選択すると、Telnet COM Port Control(RFC2217)の使用選択ができなくなります。

(5)使用できるシリアルポート数と通信速度が制限されます

SSL 機能を使用すると、複数のシリアルポートを有する本製品では、COM1 以外のシリアルポートは使用できなくなります。

また、COM1 のシリアル通信速度は最大 115,200bps までに制限されます。

３．動作確認

本体と付属ソフトウェアを使用して、TCP プロトコルのサーバ／クライアントそれぞれにおける動作確認方法を解説します。

３．１　サーバモードでの動作確認

本体をサーバモード(T2S)で動作させ、クライアントには TCP-VSP for ezTCP を使用します。
それぞれの機器の接続は下図のように構成します。

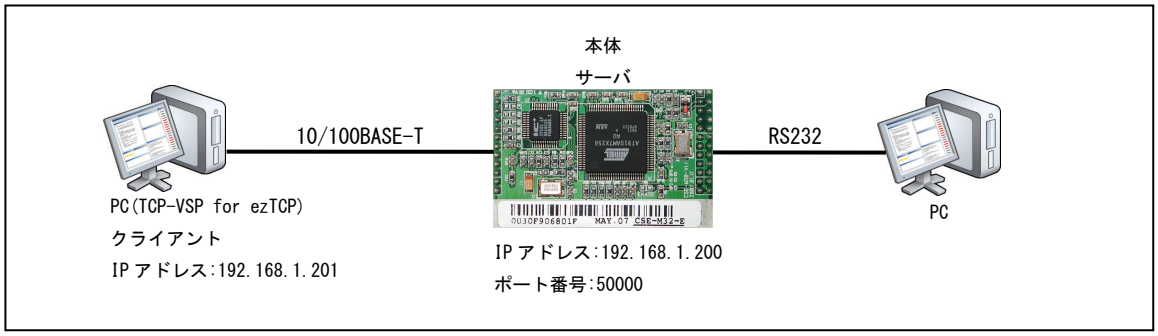

Fig 3.1-1　サーバモードでの動作確認構成

① 本体の設定

ezManager を使って本体を次のように設定し、[Write]ボタンを押して本体に書き込んでください。

Serial Port	
Baudrate	38400
Parity	NONE
Data Bits	8
Stop Bit	1
Flow Control	NONE

Table 3.1-1　シリアルポートの設定値

TCP/IP	
Communication Mode	T2S-TCP Server
Local Port	50000
Event Byte	0
Timeout	0
Data Frame	0

Table 3.1-2　ネットワークの設定値

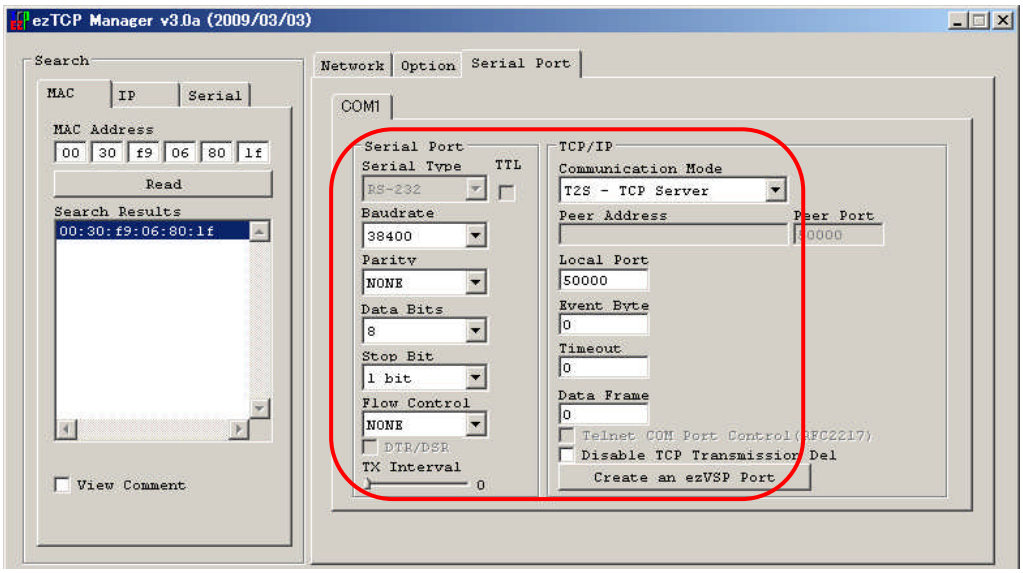

Fig 3.1-2　本体の設定

② 本体のステータスを確認

ezManager の[Status]ボタンを押してステータスの確認をします。

「SSL STATUS」が、「N/A」になっていることを確認してください。

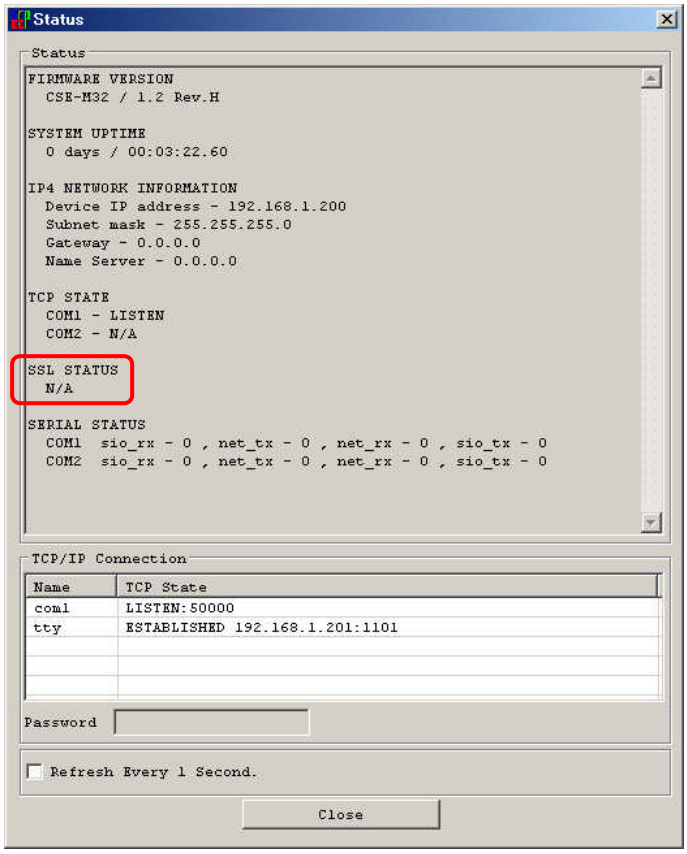

Fig 3.1-3　サーバモードで SSL 接続前 Status 画面

③ 仮想 COM ポートの作成

TCP-VSP for ezTCP を起動後、メイン画面にある[VSP Add]ボタンを押して、仮想 COM ポートを作成します。

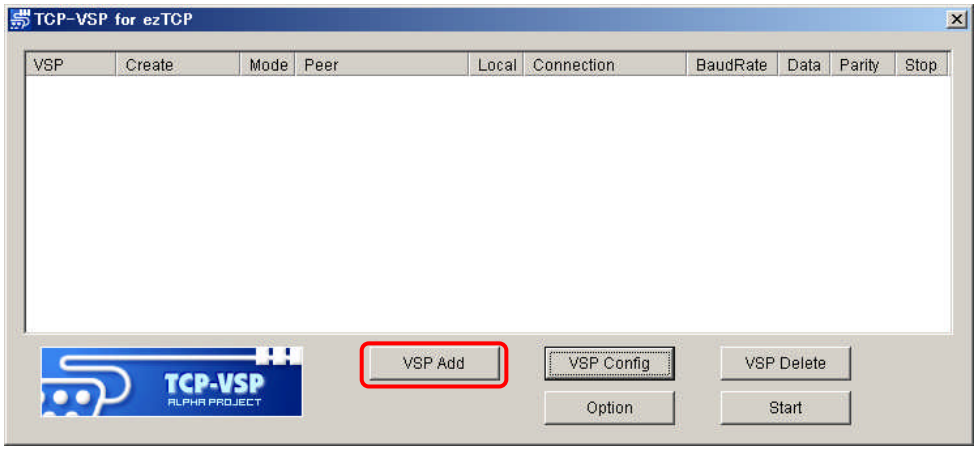

Fig 3.1-4　TCP-VSP for ezTCP メイン画面

④　作成する仮想 COM ポートの設定

ADD 画面が表示されますので、仮想 COM ポート作成に必要な情報の入力と、[SSL/TLS Enable]のチェックボックスにチェックを入れてください

各項目の詳しい説明は、「TCP-VSP 取扱説明書」をご覧ください。

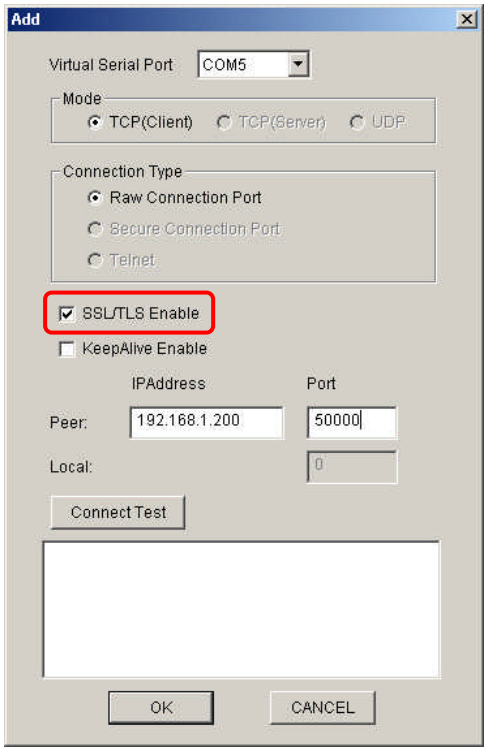

Fig 3.1-5　仮想 COM ポート設定画面

VirtualSerialPort	作成する仮想 COM ポートを選択
Mode	TCP (Client)
ConnectionType	RawConnectionPort
SSL/TLS Enable	ON
IP Address	192.168.1.200
Port	50000

Table 3.1-3　仮想 COM ポート設定

[Connect Test]を押し、接続テストを行ってください。

この時の結果表示が、「Fig 3.1-6　**接続テスト**」のようになれば、SSL 通信での Connect Test に成功です。

失敗した場合には、アイコン及び表示文字が赤くなります。

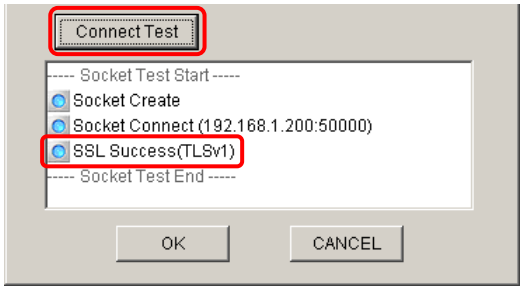

Fig 3.1-6　接続テスト

Connect Test が成功したら[OK]ボタンを押して、[VSP Add]を閉じます。

⑤　仮想 COM ポートの処理を開始

メイン画面にある仮想 COM ポートのチェックボックスが、チェックされていることを確認し、[Start]ボタンを押してください。

仮想 COM ポートの処理が開始されます。

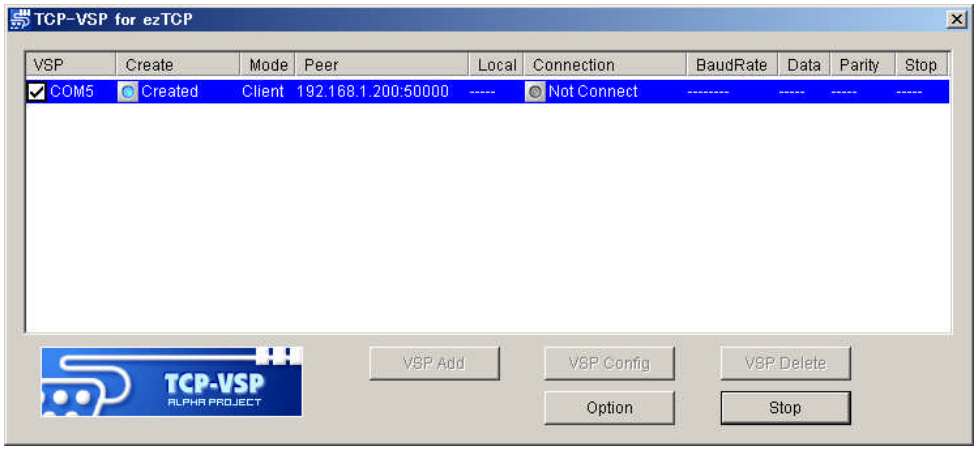

Fig 3.1-7　仮想 COM ポート処理開始

⑥　本体の COM ポートと接続した PC と仮想 COM ポートを作成した PC の通信条件を設定

各々のパソコン上で Windows 付属のハイパーターミナルを起動し、通信条件を設定します。

通信条件を下表に示します。

なお、WindowsVista にはハイパーターミナルが付属されておりませんので別途ターミナルソフトをご用意ください。

	PC(TCP-VSP for ezTCP)	本体の COM ポートと接続した PC
ビット/秒	38400	38400
データビット	8	8
パリティ	なし	なし
ストップビット	1	1
フロー制御	なし	なし

Table 3.1-4　ポートの設定

⑦　TCP 接続の確認

SSL 機能を使用して TCP 接続していることを確認します。

ezManager の[Status]ボタンを押して、TCP STATE と SSL STATUS が下記の画面のようになっていることをご確認ください。

TCP SATE　　：COM1 -　ESTABLISHED

SSL STATUS　　：State -　7

：Cipher -　RSA_AES_256_CBC_SHA

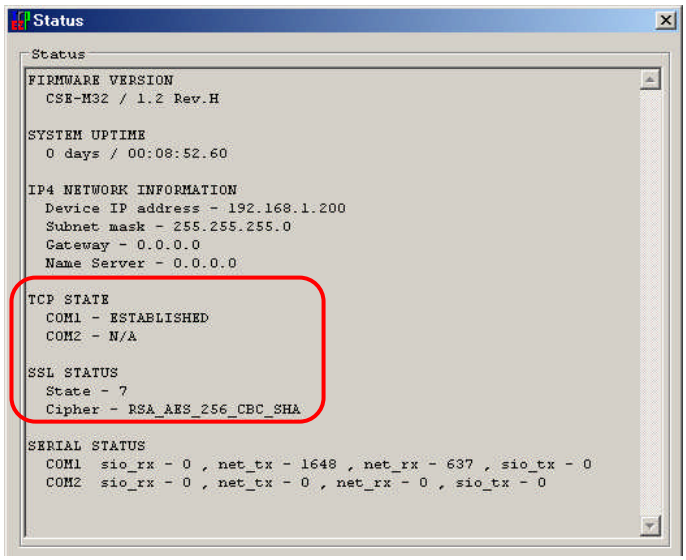

Fig 3.1-8　サーバモードで SSL 接続後 Status 画面

⑧　データ通信の確認

データ通信を行ってください。

Fig 3.1-9 本体側で受信

Fig 3.1-10 仮想 COM ポート側で受信

上の画像は、仮想 COM ポート側から本体側に文字データ「TCP-VSP」を送信し、本体側から仮想 COM ポート側に文字データ「ezTCP」を送信した時の画像です。

３．２　クライアントモードでの動作確認

本体をクライアントモード(COD)で動作させ、SSL に対応したサーバに接続し通信が行えるか確認してください。
それぞれの機器の接続は下図のように構成します。
なお、クライアントモードでの動作確認を行う場合は、SSL に対応したサーバを用意していただく必要があります。

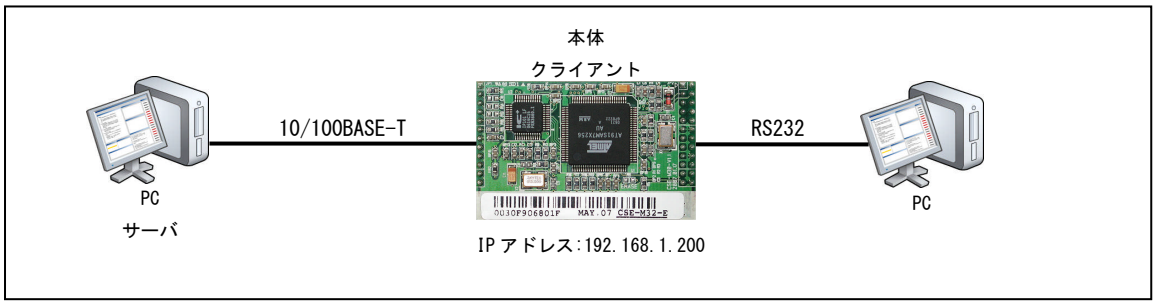

Fig 3.2-1　クライアントモードでの動作確認構成

① 本体の設定

ezManager を使って本体を次のように設定し、[Write]ボタンを押して本体に書き込んでください。

Serial Port	
Baudrate	38400
Parity	NONE
Data Bits	8
Stop Bit	1
Flow Control	NONE

Table 3.2-1　シリアルポートの設定値

TCP/IP	
Communication Mode	COD-TCP Client
Peer Address	用意したサーバの IP アドレス
Peer Port	用意したサーバのポート番号
Event Byte	0
Timeout	0
Data Frame	0

Table 3.2-2　ネットワークの設定値

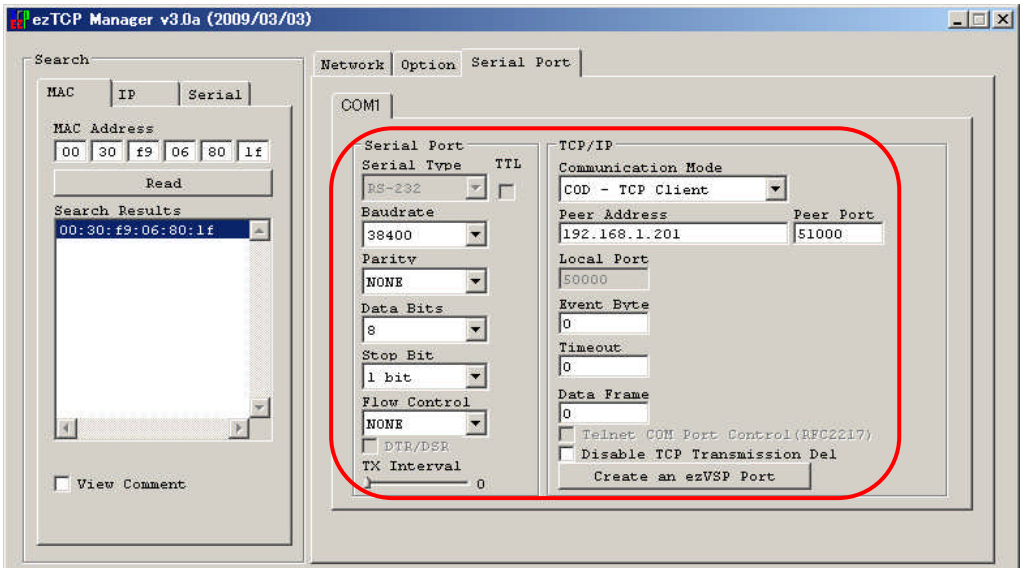

Fig 3.2-2　本体の設定

② 本体のステータスを確認

ezManager の[Status]ボタンを押してステータスの確認をします。

「SSL STATUS」が、「N/A」になっていることを確認してください。

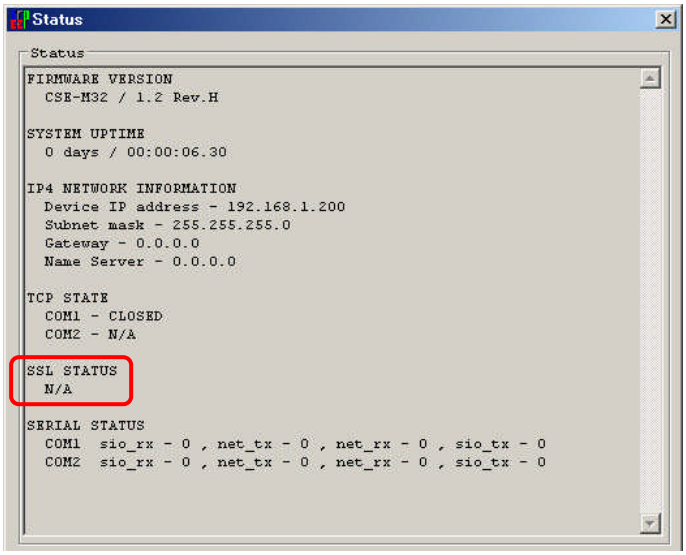

Fig 3.2-3　クライアントモードで SSL 接続前 Status 画面

③ サーバに接続

サーバへ SSL を使用して TCP 接続していることを確認します。

ezManager の[Status]ボタンを押して、TCP STATE と SSL STATUS が下記の画面のようになっていることをご確認ください。

TCP SATE　　：ESTABLISHED

SSL STATUS 項目　：State - 7

：Cipher - RSA_AES_256_CBC_SHA

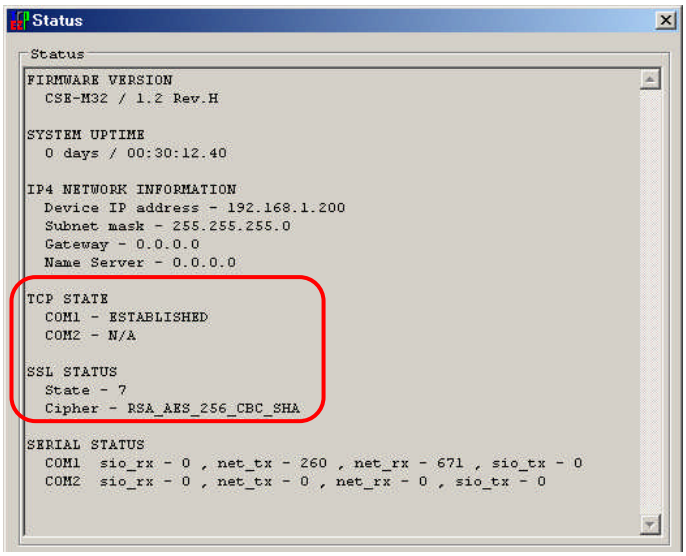

Fig 3.2-4　クライアントモードで SSL 接続後 Status 画面

④ データ通信の確認

SSL が機能している状態で正常にデータ通信が行えるか確認してください。

「TCP-VSP for ezTCP」の著作権およびサポートについて

・本製品に含まれる「TCP-VSP for ezTCP」（以下、本ソフトウェア）の著作権はアルファプロジェクトが保有しています。
　本ソフトウェアを無断で譲渡、転売、２次配布することは一切禁止いたします。
・当社は本ソフトウェアに関し、海外での保守サービス及び技術サポート等はおこなっておりません。
・本ソフトウェアの運用の結果、万が一損害が発生しても、弊社では一切責任を負いませんのでご了承ください。

「ezManager」の著作権およびサポートについて

・本製品に含まれる「ezManeger」（以下、本ソフトウェア）の著作権は SollaeSystems 社が保有しています。
　本ソフトウェアを無断で譲渡、転売、２次配布することは一切禁止いたします。
・当社は本ソフトウェアに関し、海外での保守サービス及び技術サポート等はおこなっておりません。
・本ソフトウェアの運用の結果、万が一損害が発生しても、弊社では一切責任を負いませんのでご了承ください。

ご注意

・本文書の著作権は（株）アルファプロジェクトが保有します。
・本文書の内容を無断で転載することは一切禁止します。
・本文書に記載された回路図およびサンプルプログラム等の著作権は（株）アルファプロジェクトが保有しますが、お客様のアプリケーションで使用される場合には、ご自由にご利用いただけます。
・本文書の内容は、将来予告なしに変更されることがあります。
・本文書に記載されている内容、およびサンプルプログラムについての質問等のサポートは一切受け付けておりませんのでご了承ください。
・本文書の内容については、万全を期して作成しましたが、万一不審な点、誤りなどお気付きの点がありましたら弊社までご連絡下さい。
・本文書の内容およびサンプルプログラムに基づき、アプリケーションを運用した結果、万一損害が発生しても、弊社では一切責任を負いませんのでご了承下さい。

商標について

・Windows®の正式名称は Microsoft®Windows®Operating System です。
・Microsoft、Windows は、米国 Microsoft Corporation.の米国およびその他の国における商標または登録商標です。
・Windows®Vista、Windows®XP、Windows®2000 Professional は、米国 Microsoft Corporation.の商品名称です。
　本文書では下記のように省略して記載している場合がございます。ご了承下さい。
　Windows®Vista は Windows Vista もしくは WinVista
　Windows®XP は Windows XP もしくは WinXP
　Windows®2000 Professional は Windows 2000 もしくは Win2000

・その他の会社名、製品名は、各社の登録商標または商標です。

ALPHA PROJECT Co.,LTD.
株式会社アルファプロジェクト
〒431-3114
静岡県浜松市東区積志町 834
http://www.apnet.co.jp
E-MAIL : query@apnet.co.jp