SSH（Secure Shell）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
	PuTTY v0.6
	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「SSH」について説明します。

１．２　SSH について

SSH（Secure Shell）とは、暗号化や認証の技術を利用して安全に遠隔地にあるコンピュータを制御するために Telnet の代用として設計された暗号化プロトコルです。

SSH を使うことで、TCP プロトコルの接続要求に認証の処理が追加されることから、TCP 接続の安全性が確保されます。

サポートしているバージョンは、SSH2 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 1 つ（T2S）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	-	50000

Table 1.3-2　ネットワークの設定値

２．SSH の設定

２．１　SSH 機能設定

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

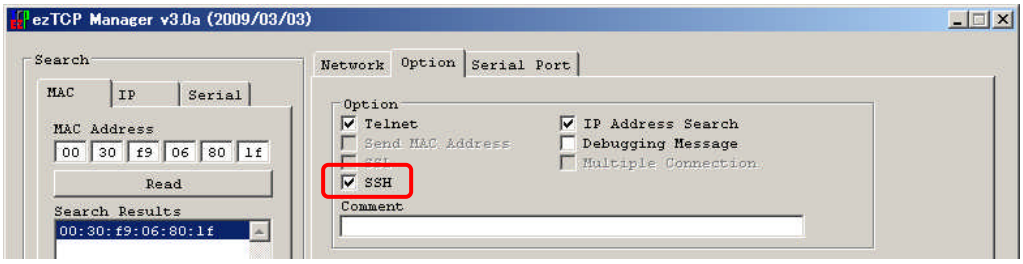

Fig 2.1-1 SSH 設定画面

チェック後、本体を SSH に対応したサーバとして動作させるのに必要な鍵とログイン ID 及び Password を作成した後に、SSH 通信が行なえます。
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　鍵(公開鍵･秘密鍵)とログイン ID 及び Password の作成

SSH 機能を使用する場合には、鍵(公開鍵･秘密鍵)とログイン ID 及び Password が必要となります。
本項では、鍵(公開鍵･秘密鍵)とログイン ID 及び Password の作成方法について説明します。

鍵(公開鍵･秘密鍵)とログイン ID 及び Password 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	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
DSA KEY	dsa keygen	DSA KEY 作成
	dsa key	作成した DSA KEY の確認
ID/Password	ssh id	ログイン ID と Password の設定
設定保存	ssh save aa55cc33	作成した鍵とログイン ID 及び Password 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、ログイン ID 及び Password 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。

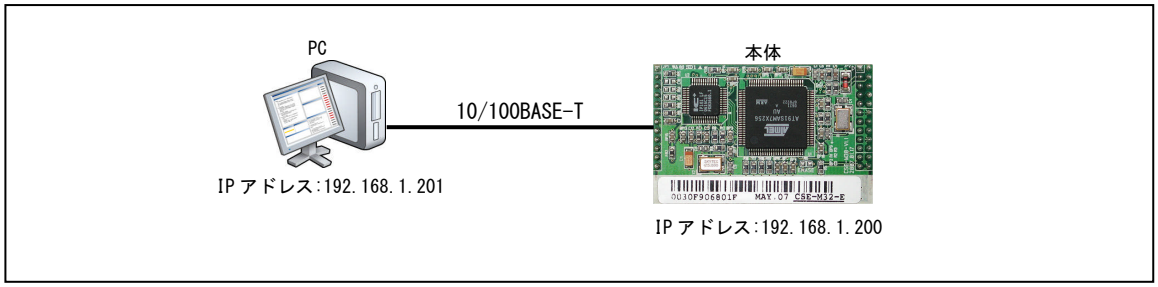

Fig 2.2-1　本体の接続(公開鍵･秘密鍵と証明書作成時)

② 本体の設定

ezManager にて OPTION タブ内の[OPTION]欄にある[telnet]と[ssh]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>は使用者 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 DSA KEY(公開鍵･秘密鍵)を作成

次に、DSA KEY を作成します。『dsa keygen』を実行して、DSA KEY を作成してください。

```
lsh>dsa keygen
generating fips186 dsa key...done
verifying...done
lsh>
```

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

```
lsh>dsa key
DSA public prime P: 1024 bits
  + e2:18:9f:b9:ea:48:04:b8:5d:ce:94:d2:fb:08:f5:50
  + 8c:52:0b:7d:dc:ee:50:90:49:09:e9:a9:3c:1d:ae:b6
... 中略
  + d6:8f:0a:a7:b9:f1:d9:cf:15:61:5d:c7:c4:fc:d7:8c
  + 4a:f0:94:a3:99:49:9d:76:41:c9:96:fb:50:11:31:d3
lsh>
```

⑦　ログイン ID と Password を設定

ログイン ID と Password を設定します。『ssh id』を実行して、ログイン ID と Password を設定してください。
入力した Password は「*」で表示されます。
username：ログイン ID を入力してください。
password：Password を入力してください。
retype　：再度 Password を入力してください。

```
lsh>ssh id
username: eztcp
password: ********
  retype: ********
ID update ok.
lsh>
```

なお、ログイン ID と Password を忘れた際は、再度『ssh id』を入力することで、ログイン ID と Password(「*」で表示されます)の確認、または新しいログイン ID と Password を設定することができます。
username が表示された時、Enter キーを押すと現在のログイン ID と Password の確認となります。
username が表示された時、新たに設定するログイン ID を入力すると、新しい ID と Password に変更することができます。
なお、変更を行った場合には、『ssh save aa55cc33』を入力して、本体に保存してください。

```
lsh>ssh id
eztcp : ********
username:
```

⑧　鍵とログイン ID 及び Password を本体に保存

SSH を動作させるために、RSA KEY と DSA KYE 及びログイン ID と Password を本体に保存します。
『ssh save aa55cc33』を入力して、保存してください。

```
lsh>ssh save aa55cc33
save key...RSA DSA SSH_ID SSH_MSG ok
lsh>
```

２．３　注意事項

SSH は、データ通信を暗号化しセキュリティ性を向上させる便利な機能ですが、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 SSH に対応している必要があります

本体側のみ SSH 機能を使用した場合は正しいデータ通信が行われません。

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

(2)TCP 通信モード T2S(TCP)でのみ使用することができます。

ezManager にて SSH 機能の使用を選択すると、通信モードは T2S に固定されます。

通信モードとして ATC、COD 及び U2S が選択されている状態で、SSH 機能の使用を選択すると、通信モードは T2S に変更されます。

(3)SSL 機能と併用して使用することはできません

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「SSL」とは排他利用となります。

ezManager にて SSH 機能の使用を選択すると、SSL 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 SSH 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。

３．動作確認

本体と PuTTY を使用して、SSH の動作確認方法を解説します。

３．１　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 PuTTY 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。

＊　動作確認を行うためには、SSH クライアントソフト「PuTTY」が必要となります。
お手数ですがお客様にてご用意ください。

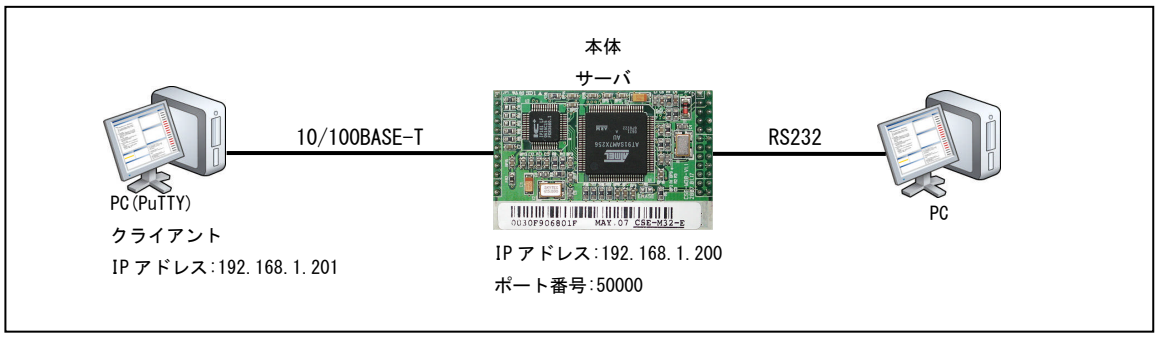

Fig 3.1-1　本体の接続図

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	
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

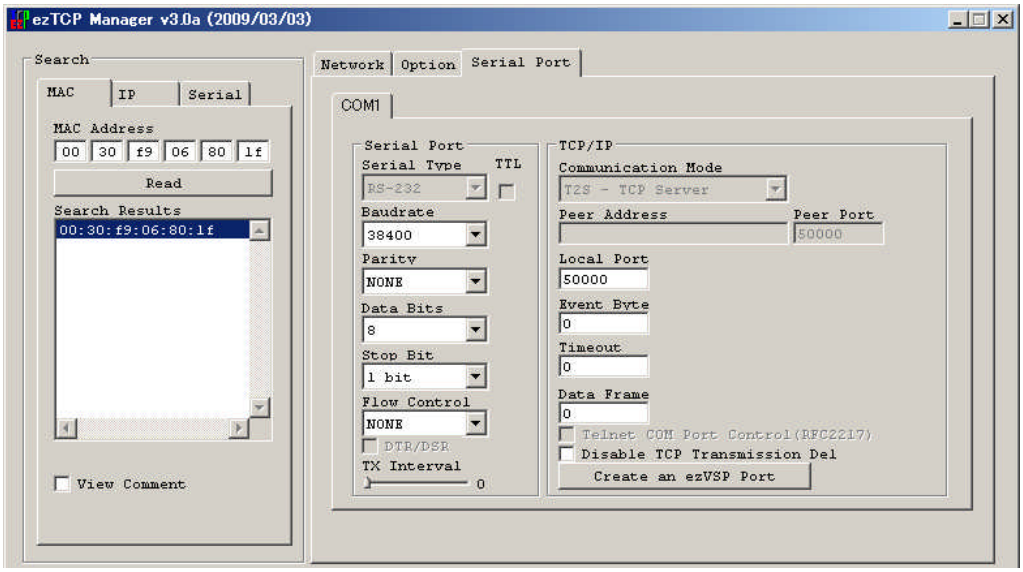

Fig 3.1-2　本体の設定

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。

「SSH STATUS」が、「N/A」になっていることを確認してください。

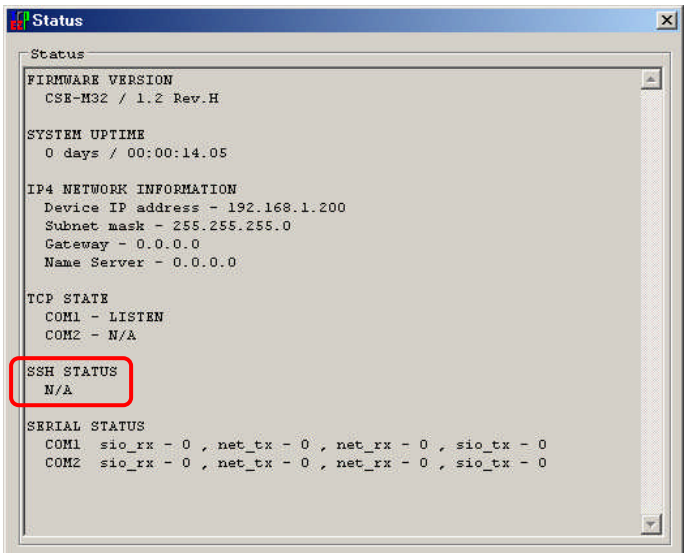

Fig 3.1-3　SSH 接続前 Status 画面

③ PuTTY の設定

PuTTY の設定を行います。

「Session」-[Specify the destination you want to connect to]にある「Host Name(or IP adress)」と「Port」にそれぞれ本体の Local IP Address と Local Port を入力してください。

[Connection type:]は、「SSH」を選択してください。

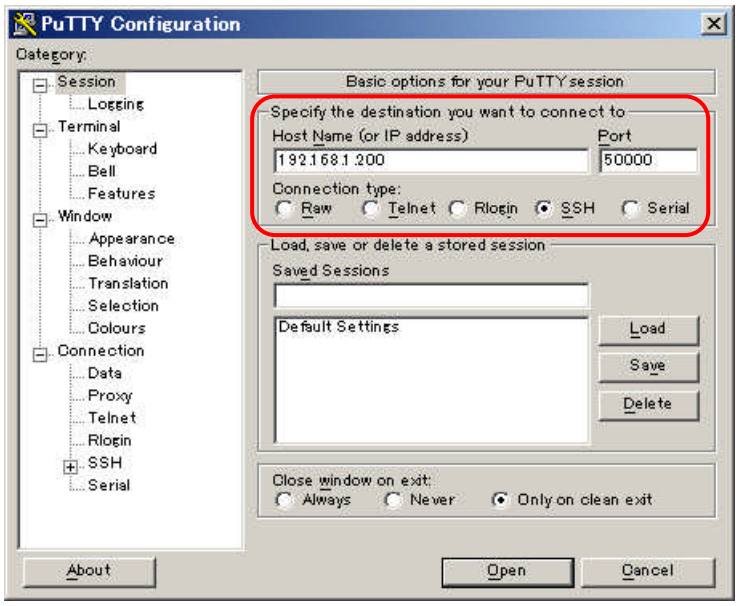

Fig 3.1-4　PuTTY 設定画面

設定が終わりましたら、「Open」を押してください。

③　サーバに接続

サーバに接続しますと、下図のような警告メッセージが表示されます。(2 回目以降の接続では表示されません)
「はい(Y)」を押してください。

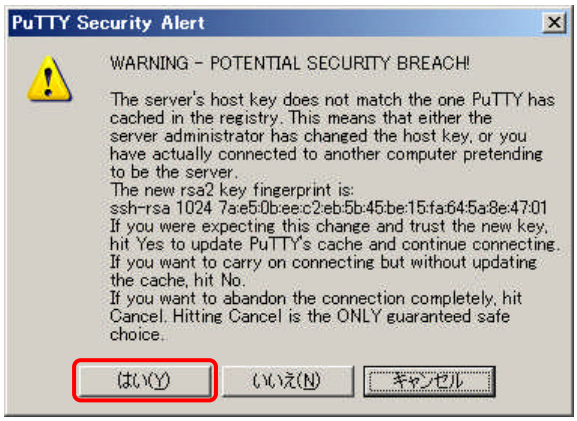

Fig 3.1-5　警告メッセージ

④　ログイン ID と Password を入力

PuTTY のターミナルウィンドウが開き、ログイン ID と Password を要求してきますので、設定したログイン ID と Password を入力してください。Password は入力しても表示されません。

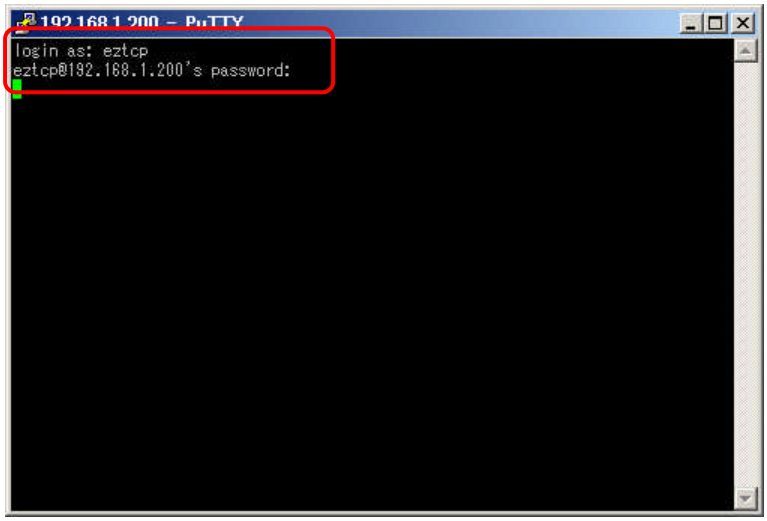

Fig 3.1-6　PuTTY ターミナルウィンドウ

⑤接続を確認

SSH 機能を使用して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 SATE と SSH 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

SSH STATUS 項目　　：State - 6

：KEY - DH_GRPUP2, RSA

：Cipher - AES256, HMAC_SHA1

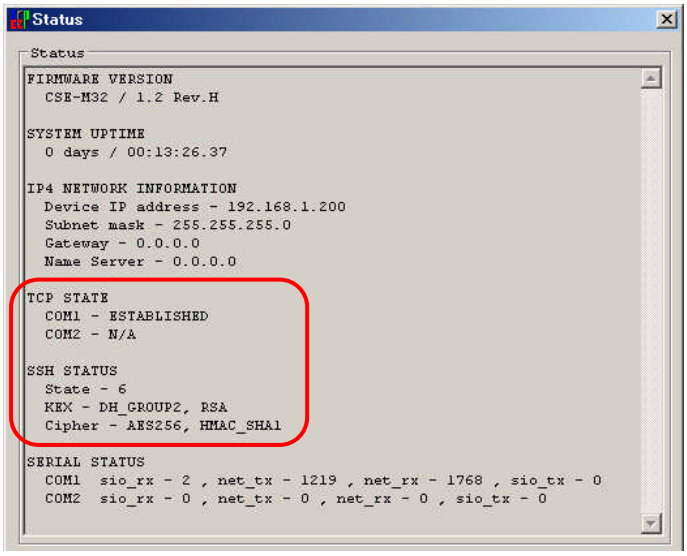

Fig 3.1-7　SSH 接続後 Status 画面

⑥データ通信の確認

SSH 接続後、データ通信が可能かどうか確認します。

本体のシリアルポートと接続した PC 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。

ポートの設定	値
ビット/秒	38400
データビット	8
パリティ	なし
ストップビット	1
フロー制御	なし

Table 3.1-3　ポートの設定

シリアルポート側のターミナルからデータ「123」を送信し PuTTY のターミナルに「123」が表示され、PuTTY のターミナルからデータ「abc」を送信し、シリアルポート側のターミナルに「abc」が表示されれば OK です。

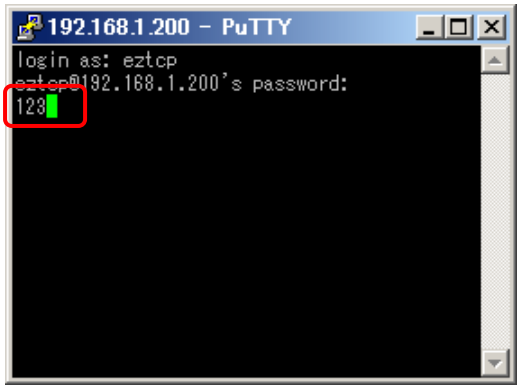

Fig 3.1-8　PuTTY 側で受信

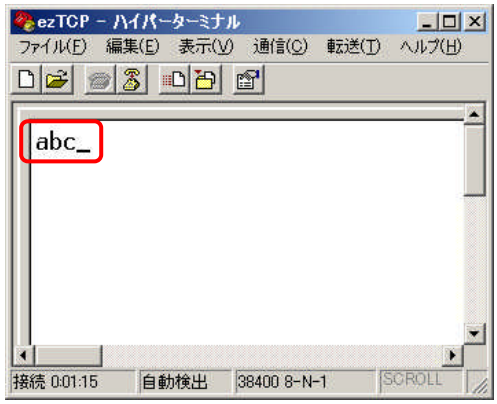

Fig 3.1-9　シリアルポート側で受信

上の画像は、PuTTY 側から本体側に文字データ「abc」を送信し、本体側から PuTTY 側に文字データ「123」を送信した時の画像です。

「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