

Renesas R5F565NE(CK-RX65N)用サンプル

(e2studio RX65N_gnu_dhcp_tcp_aes_gt202_uselib)の説明

(e2studio Version:2024-04 / Azure RTOS Version 6.2.1 rel-rx-2.0.0)

1. Sample の免責について

- Sample に関する Tel/Fax でのご質問に関してはお受けできません。ただし、メールでのご質問に関してはお答えするよう努力はしますが、都合によりお答えできない場合もありますので予めご了承願います。
- Sample ソフトの不具合が発見された場合の対応義務はありません。また、この関連ソフトの使用方法に関する質問の回答義務もありませんので承知の上ご利用下さい。
- Sample ソフトは、無保証で提供されているものであり、その適用可能性も含めて、いかなる保証も行いません。また、本ソフトウェアの利用により直接的または間接的に生じたいかなる損害に関しても、その責任を負わないものとします。

2. サンプルのプロジェクト名

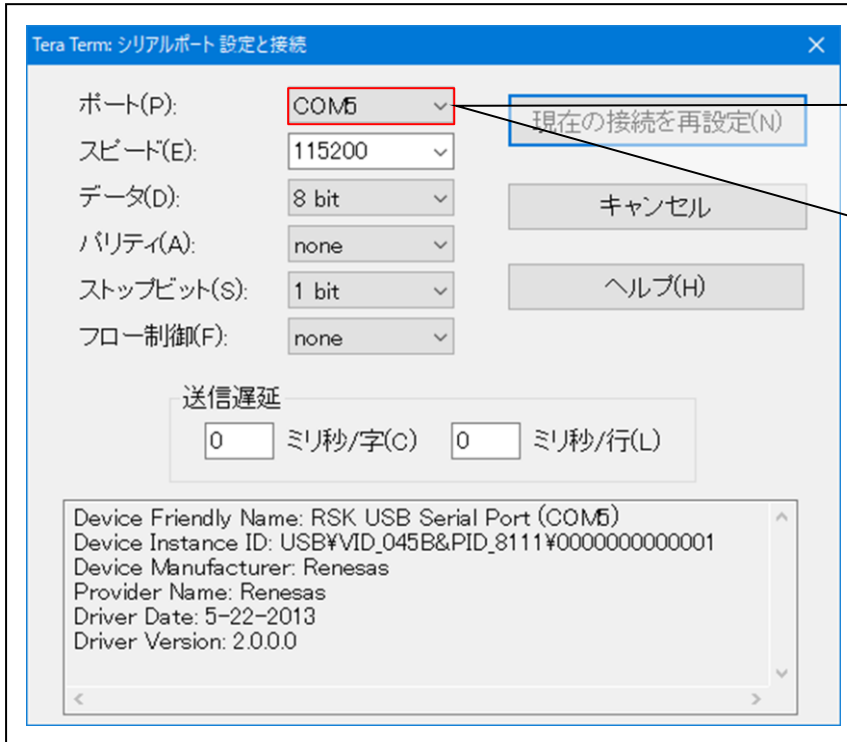
ワークスペース名	概要	プロジェクト名
Azure_sample_gnu_wifi_CK	無線 WiFi-module(GT202-QCA4002)を使用した DHCP と TCP 通信のサンプル セキュリティ API Crypto ドライバー AES-CBC を使用したサンプル (暗号・復号)	RX65N_gnu_dhcp_tcp_aes_gt202_uselib Azure RTOS モードで動作 NetX DHCP Client (dhcp_client) TCP 通信(Client) (nx_tcp_socket_.....) 暗号・復号(AES-CBC) (NX_CRYPT0_ENCRYPT) (NX_CRYPT0_DECRYPT)

統合開発環境
Renesas e2studio(Version 2024-04)
Azure RTOS (Version 6.2.1 rel-rx 2.0.0)
GCC for Renesas RX(Version 8.3.0.202305)

ハード環境
CK-RX65N (ルネサス製)

3. Tera Term Pro のインストール

- ① 「teraterm-4.106.exe」 を検索してダウンロードする。
- ② PC にインストールし実行する
- ③ シリアルポートの設定



COM 番号は、
PC 側でシリアル通信可能な
番号を指定する。

115200BPS

8bit

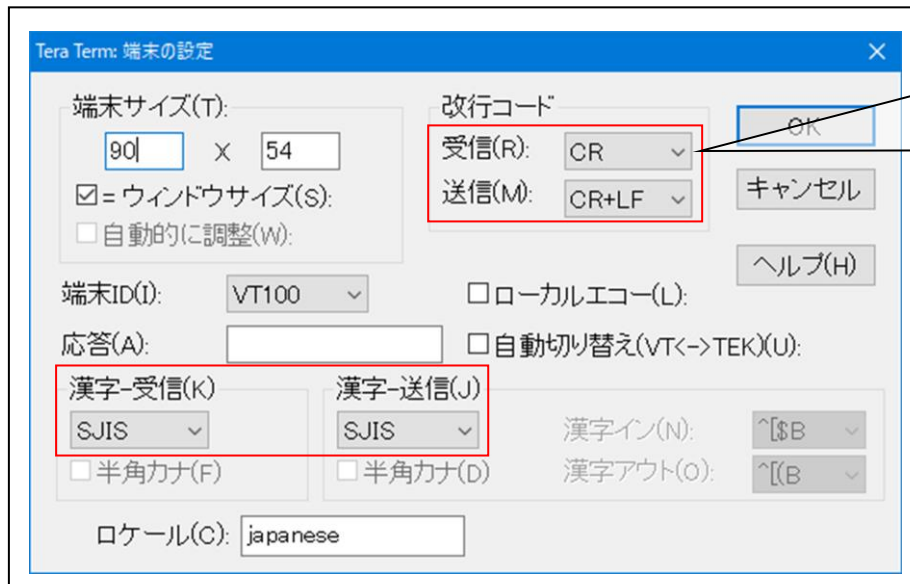
none

1bit

none

の仕様にする。

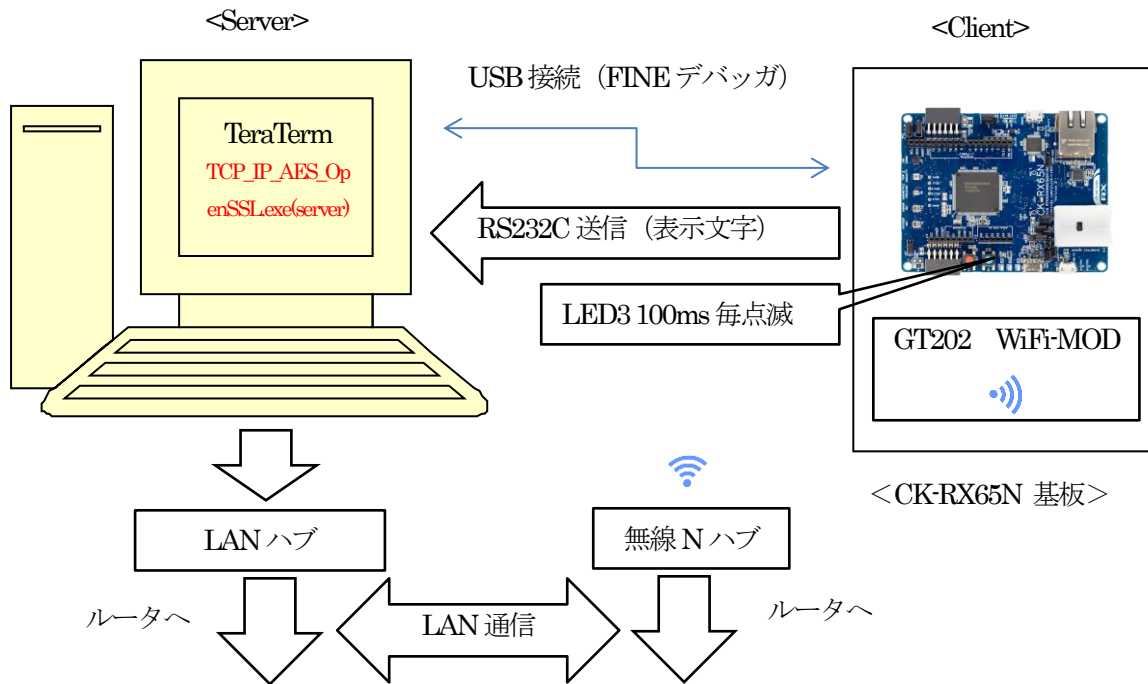
④ 端末の設定



USB シリアルコンバータ
ータ使用時に CR コードが
カットされる設定の場合は、
受信 : LF にして下さい。

赤枠の設定にする。

4. 動作構成

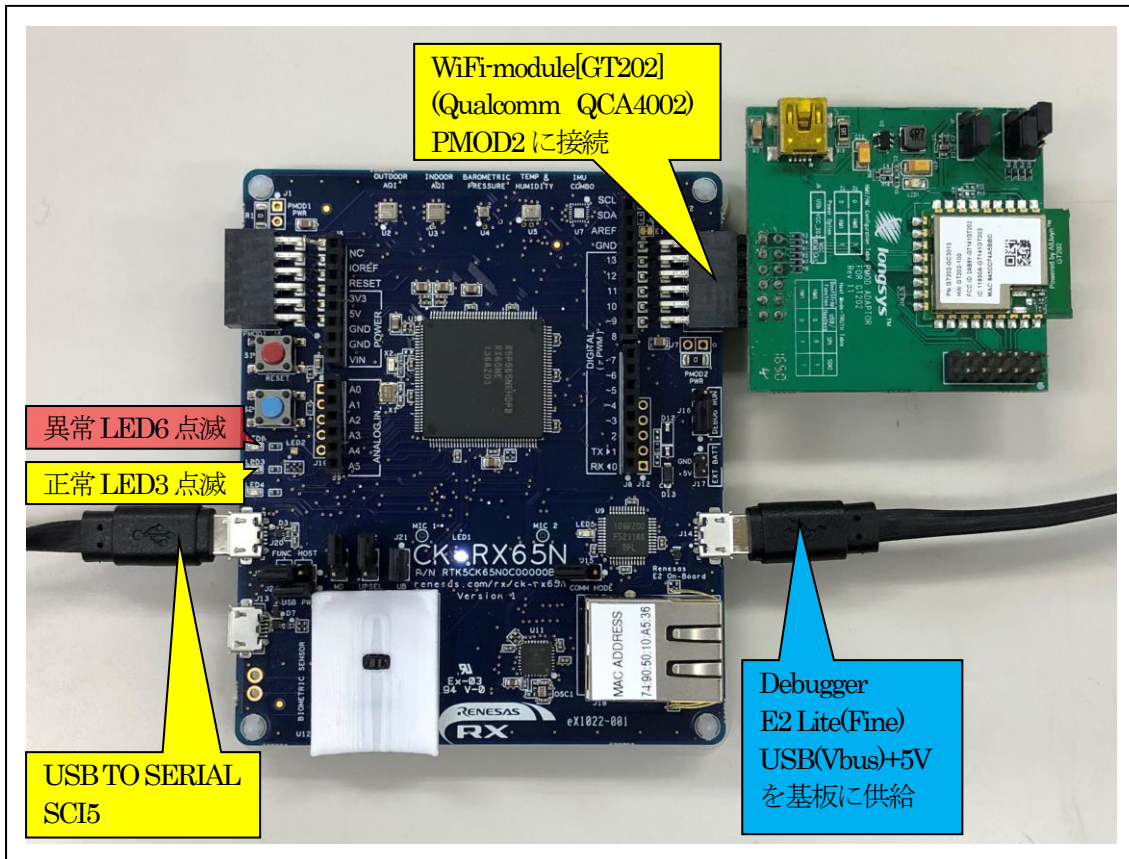


<TCP_IP_AES_OpenSSL.exe>
【Plain mode】
 1. 平文を受信する。
 2. 受信した平文をそのまま送信する。

【AES-CBC mode】
 1. 暗号文を受信する。
 2. 受信した暗号文を復号して表示する。
 3. 復号文を暗号化した文章を送信する。

<RX65N_gnu_dhcp_tcp_aes_gt202_uselib>
【Plain mode】
 1. 平文を送信する。
 2. 受信した平文を TeraTerm に表示する。

【AES-CBC mode】
 1. AES(CBC)暗号化した文章を送信する。
 2. 受信した暗号文を復号して TeraTerm に表示する。



ジャンパ		備考
J2	ショート	Current Measurement point for MCU
J15	オープン	Select debugger comms mode
J16	1-2ショート	DEBUG
J21	ショート	Enable USB boot mode
J22	オープン	Select USB boot mode power supply method
J11	オープン	Configures the MCU for normal boot mode

5. 「RX65N_gnu_dhcp_tcp_aes_gt202_uselib」 サンプルの説明

5-1. フォルダ構成とファイル名【<ホルダ名>を示す】

<Azure_sample_gnu_wifi_CK>		
<rx_gnu_filex_lib>	AzureRTOS FileX ライブラリ作成用ホルダ	
<rx_gnu_netxduo_addons_lib>	AzureRTOS NetX Duo Addons ライブラリ作成用ホルダ	
<rx_gnu_netxduo_lib>	AzureRTOS NetX Duo ライブラリ作成用ホルダ	
<rx_gnu_threadx_lib>	AzureRTOS ThredX ライブラリ作成用ホルダ	
<RX65N_gnu_dhcp_tcp_aes_gt202_uselib>	DHCP / TCP 通信 / AES-CBC(暗号・復号) サンプルプロジェクト	
<HardwareDebug>	RX65N_gnu_dhcp_tcp_g t202_uselib.elf	ELF ファイル、JTAG で使用
	RX65N_gnu_dhcp_tcp_a es_gt202_uselib.map	MAP ファイル、アドレス情報
	RX65N_gnu_dhcp_tcp_a es_gt202_uselib.mot	モトローラーHEX ファイル
	その他	自動生成ファイル
<lib>	<filex>	FileX (全Cソースはビルド除外)
	<netxduo>	NetX Duo (全Cソースはビルド除外)
	<netxduo_addons>	NetX Duo Addons (全Cソースはビルド除外)
	<threadx>	ThreadX (全Cソースはビルド除外)
	librx_gnu_filex_lib.a	FileX ライブラリ
	librx_gnu_netxduo_addo ns_lib.a	NetX Duo Addons ライブラリ
	librx_gnu_netxduo_lib.a	NetX ライブラリ
	ibrx_gnu_threadx_lib.a	ThredX ライブラリ
<src>	<Azure_aes>	AES-CBC
	aes.c aes.h	暗号・復号処理のソース
	<driver>	
	<r_irq_rx>	FSP IRQ ドライバ (変更)
	<r_sci_rx>	FSP SPI ドライバ (変更)
	<rtos_config>	スマートコンフィグレータにより作成
	<rtos_skeleton>	
	dhcp_fixed_entry.c	DHCP スレッド処理のソース
	tcp_aes_thread_entry.c	TCP スレッド処理のソース
	<smc_gen>	スマートコンフィグレータにより作成
	<wifi_gt202>	GT202 用ドライバソース一式
	demo_printf.c	コンソール入出力処理のソース
	demo_printf.h	demo_printf.c のヘッダー
	hardware_setup.c	周辺 I/O デバイス初期化ソース

	hardware_setup.h	hardware_setup.c のヘッダー
	sample_netx_duo_ping.c	NetX 等初期化サンプルソース
	sf_wifi_nsal_api.c	NetX WiFi-API ソース
	sf_wifi_nsal_api.h	sf_wifi_nsal_api.c のヘッダ
	linker_script.ld	リンカスクリプトファイル
RX65N_gnu_dhcp_tcp_aes_gt20 2_uselib.scfg	スマートコンフィグレータの管理ファイル	
その他	自動生成ファイル	

5-2. Macro Defines の説明

Macro Name	値	説明
A_PRINTF_ENABLED	0	処理進行内容の表示を無効にする
	1	処理進行内容の表示を有効にする
NX_ENABLE_DHCP	0	DHCP Client Disable ◎ソースコードに直接 IP アドレスを記述 sample_netx_duo_ping.c : <pre> status = nx_ip_create(&g_ip0, "NetX IP Instance 0", #if (NX_ENABLE_DHCP == 1) IP_ADDRESS(0,0,0,0), IP_ADDRESS(255,255,255,0), #else IP_ADDRESS(192,168,21,54), //固定 IP アドレス IP_ADDRESS(255,255,255,0), //サブネットマスク #endif &g_pool0, nsal_netx_driver, (UCHAR*)ip_thread_stack, sizeof(ip_thread_stack), 1); </pre>
	1	DHCP Client Enable
TX_INCLUDE_USER_DEFINE_FILE		「tx_user.h」を有効にする
NX_INCLUDE_USER_DEFINE_FILE		「nx_user.h」を有効にする
FX_INCLUDE_USER_DEFINE_FILE		「fx_user.h」を有効にする
NXD_MQTT_CLOUD_ENABLE		MQTT メッセージングプロトコルを有効にする
NX_SECURE_ENABLE		MQTT クライアントは TLS サポート付きで構築される
NX_ENABLE_EXTENDED_NOTIFY_SUPPORT		多くのコールバックフックを有効にする
NX_ENABLE_IP_PACKET_FILTER		IP パケットを有効にする
FLATCC_NO_ASSERT		FLATCC をアサートしない
NX_AZURE_IOT_LOG_LEVEL	0	NX_AZURE ログ関数を使用しない
	1	LogError(...)を使用する
	2	LogError(...)/LogInfo(...)を使用する
	3	LogError(...)/LogInfo(...)/LogDebug(...)を使用する

5-3. サンプルの動作説明（基板側 CK-RX65N）

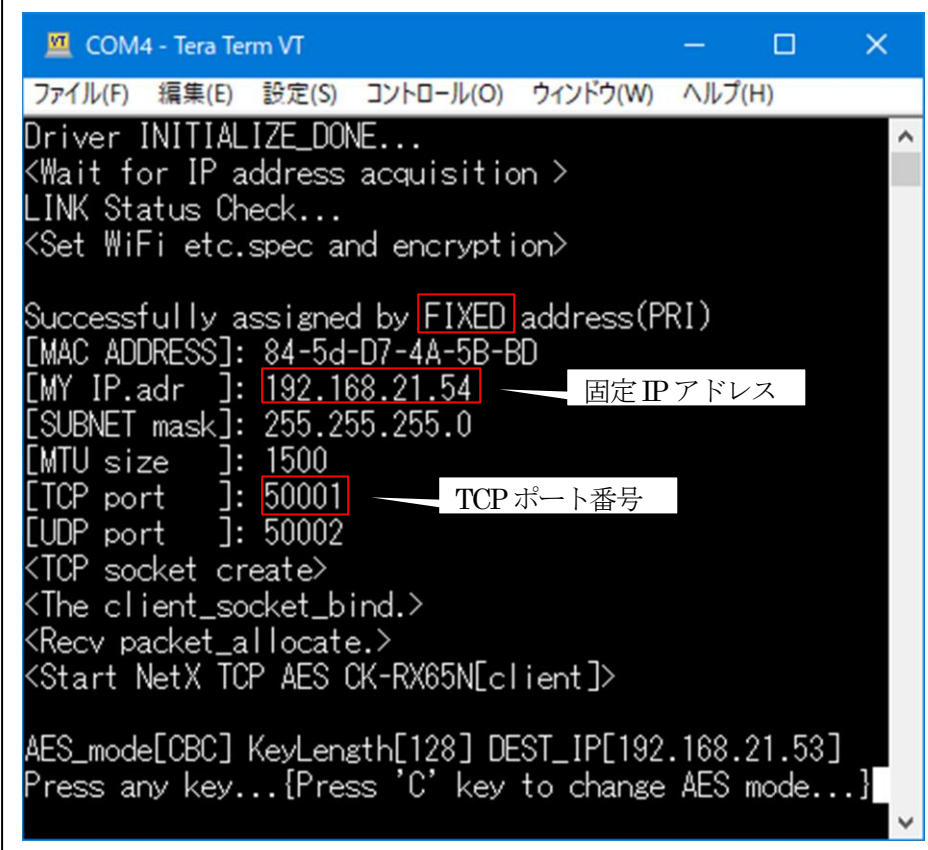
1) DHCP 無効時 (NX_ENABLE_DHCP=0)

<DHCP FIXED Thread>

Term 画面

- < 1 > 「"Driver INITIALIZE_DONE..."」
- < 2 > 「"<Wait for IP address acquisition>..."」
- < 3 > 「"LINK Status Check..."」
- < 4 > 「"<Set Wi Fi ect.spec and emryption>"」

<成功画面>IP アドレス確立により、基板上の LED3（緑色）を 100msec 毎に点滅



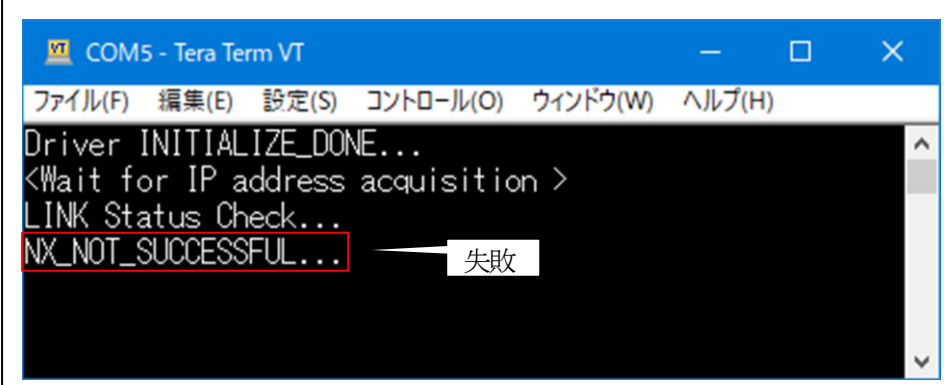
```

COM4 - Tera Term VT
ファイル(F) 編集(E) 設定(S) コントロール(O) ウィンドウ(W) ヘルプ(H)
Driver INITIALIZE_DONE...
<Wait for IP address acquisition >
LINK Status Check...
<Set Wi Fi ect.spec and emryption>

Successfully assigned by FIXED address(PRI)
[MAC ADDRESS]: 84-5d-D7-4A-5B-BD
[MY IP,adr ]: 192.168.21.54 ← 固定 IP アドレス
[SUBNET mask]: 255.255.255.0
[MTU size ]: 1500
[TCP port ]: 50001 ← TCP ポート番号
[UDP port ]: 50002
<TCP socket create>
<The client_socket_bind.>
<Recv packet_allocate.>
<Start NetX TCP AES CK-RX65N[client]>

AES_mode[CBC] KeyLength[128] DEST_IP[192.168.21.53]
Press any key...[Press 'C' key to change AES mode...]
  
```

<失敗画面>IP アドレス未確立により、基板上の LED6（赤色）を 100msec 毎に点滅



```

COM5 - Tera Term VT
ファイル(F) 編集(E) 設定(S) コントロール(O) ウィンドウ(W) ヘルプ(H)
Driver INITIALIZE_DONE...
<Wait for IP address acquisition >
LINK Status Check...
NX_NOT_SUCCESSFUL... ← 失敗
  
```

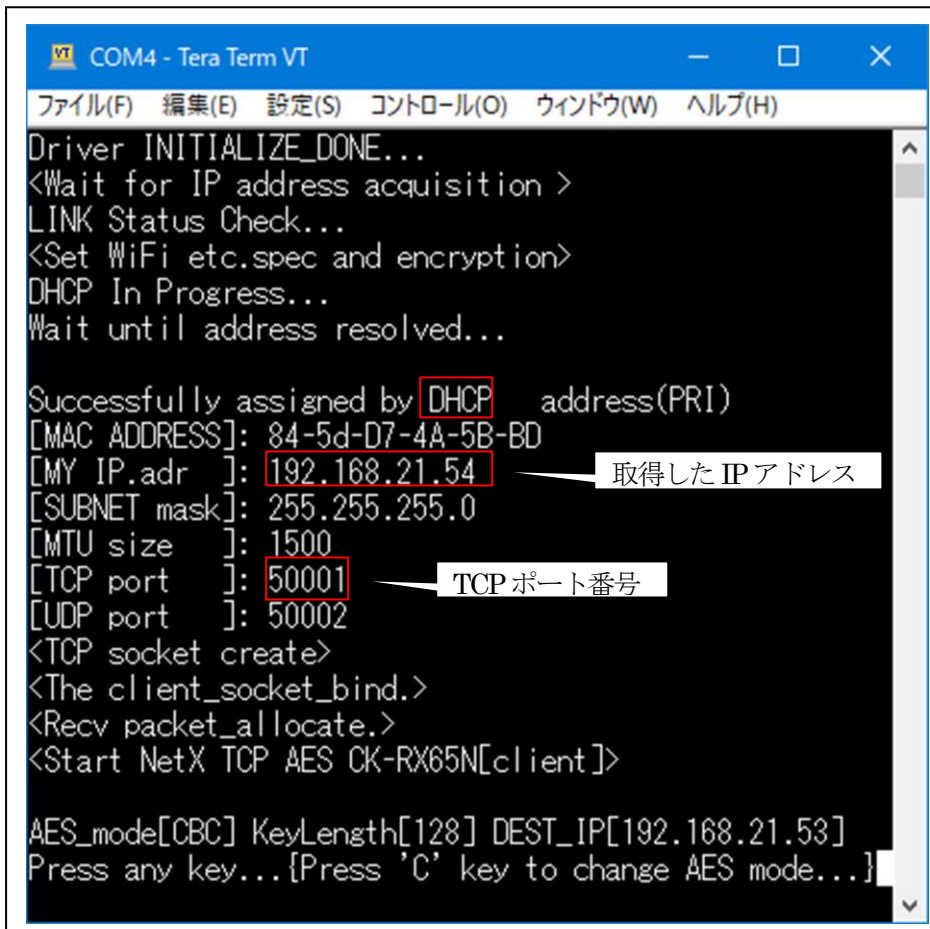

2) DHCP 有効時 (NX_ENABLE_DHCP=1)

<DHCP FIXED Thread>

Term 画面

- < 1 > ["Driver INITIALIZE_DONE..."]
- < 2 > ["<Wait for IP address acquisition>.."]
- < 3 > ["LINK Status Check..."]
- < 4 > ["<Set Wi Fi ect.spec and emryption>"]
- < 5 > ["DHCP In Progress..."]
- < 6 > ["Wait until address resolved..."]

<成功画面>IP アドレス確立により、基板上の LED3 (緑色) を 100msec 毎に点滅



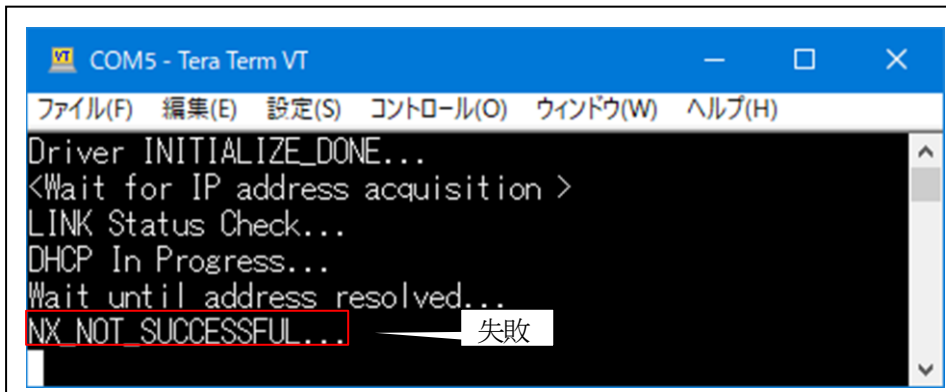
```

COM4 - Tera Term VT
ファイル(F) 編集(E) 設定(S) コントロール(O) ウィンドウ(W) ヘルプ(H)
Driver INITIALIZE_DONE...
<Wait for IP address acquisition >
LINK Status Check...
<Set Wi Fi ect.spec and emryption>
DHCP In Progress...
Wait until address resolved...

Successfully assigned by DHCP address(PRI)
[MAC ADDRESS]: 84-5d-D7-4A-5B-BD
[MY IP.adr ]: 192.168.21.54
[SUBNET mask]: 255.255.255.0
[MTU size ]: 1500
[TCP port ]: 50001
[UDP port ]: 50002
<TCP socket create>
<The client_socket_bind.>
<Recv packet_allocate.>
<Start NetX TCP AES CK-RX65N[client]>

AES_mode[CBC] KeyLength[128] DEST_IP[192.168.21.53]
Press any key...[Press 'C' key to change AES mode...]
  
```

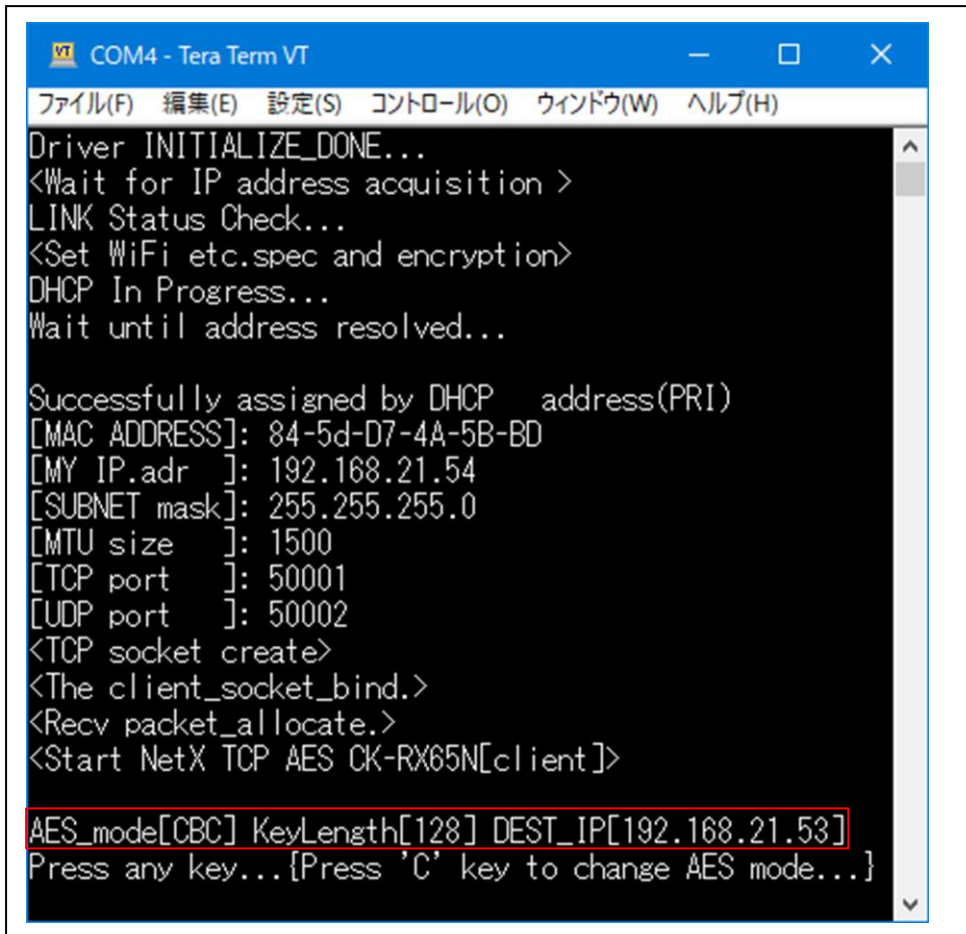
<失敗画面>IP アドレス未確立により、基板上の LED6 (赤色) を 100msec 毎に点滅



```

COM5 - Tera Term VT
ファイル(F) 編集(E) 設定(S) コントロール(O) ウィンドウ(W) ヘルプ(H)
Driver INITIALIZE_DONE...
<Wait for IP address acquisition >
LINK Status Check...
DHCP In Progress...
Wait until address resolved...
NX NOT SUCCESSFUL...
  
```

3) TCP/IP 送受信
 <TCPAES Thread>



```

COM4 - Tera Term VT
ファイル(F) 編集(E) 設定(S) コントロール(O) ウィンドウ(W) ヘルプ(H)
Driver INITIALIZE_DONE...
<Wait for IP address acquisition >
LINK Status Check...
<Set WiFi etc.spec and encryption>
DHCP In Progress...
Wait until address resolved...

Successfully assigned by DHCP address(PRI)
[MAC ADDRESS]: 84-5d-D7-4A-5B-BD
[MY IP.adr ]: 192.168.21.54
[SUBNET mask]: 255.255.255.0
[MTU size ]: 1500
[TCP port ]: 50001
[UDP port ]: 50002
<TCP socket create>
<The client_socket_bind.>
<Recv packet_allocate.>
<Start NetX TCP AES CK-RX65N[client]>

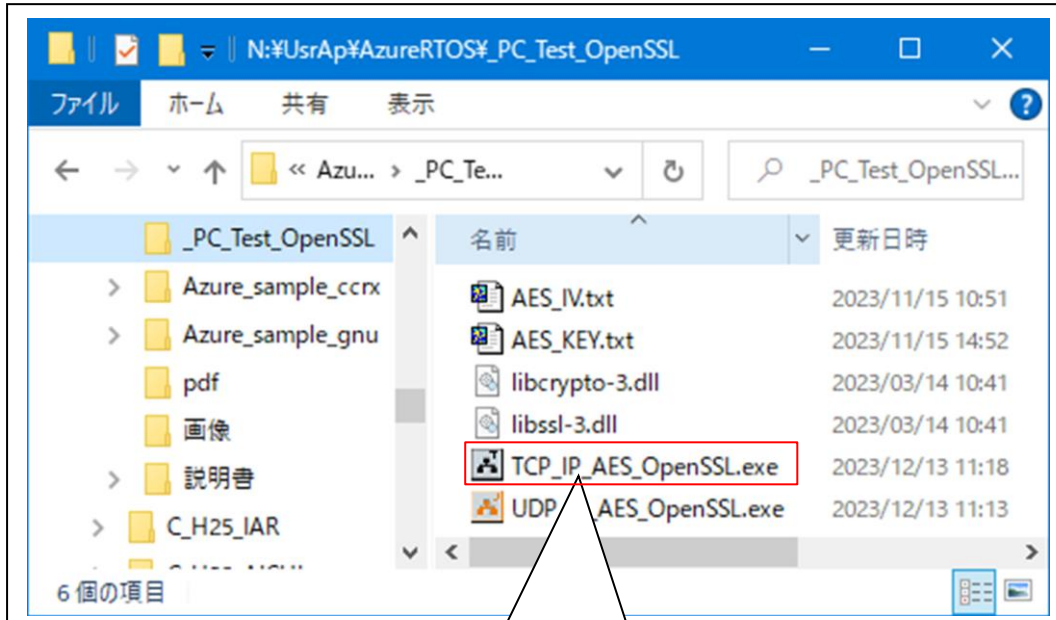
AES_mode[CBC] KeyLength[128] DEST_IP[192.168.21.53]
Press any key...{Press 'C' key to change AES mode...}
  
```

表示項目	表示内容	説明
AES_mode[x]	PLAIN CBC	送受信モードの指定 ◎変数のフラグにより指定 aes.c : int AES_crypto_mode; 0 : PLAIN // 平文モード 1 : CBC // AES-CBC モード暗号・復号
KeyLength[x]	128 192 256	AES-CBC モード時の Key ビット長の指定 ◎変数の数値により指定 aes.c : int AES_crypto_bit; 128 : Key ビット長が 128bit 192 : Key ビット長が 192bit 256 : Key ビット長が 256bit
DEST_IP[xxx.xxxx.xxxx.xxxx]	固定	送信先(PC 側)IP アドレス ◎define にて指定 tcp_aes_thread_entry.c : #define DEST_IP IP_ADDRESS(192,168,xx,xx)

5-4. Windows PC側のテストプログラムで動作確認 (PLAIN (平文) モード)

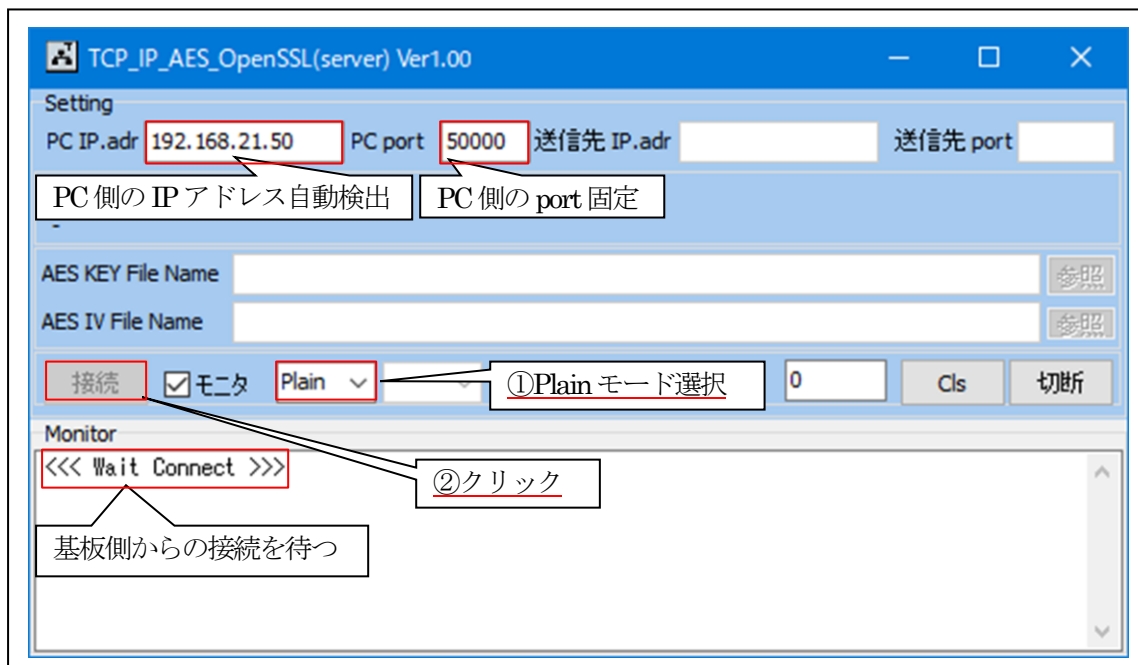
- 1) 「TCP_IP_AES_OpenSSL.exe」を起動する。(各モード共通)

プログラム場所【¥_PC_Test_OpenSSL】 サンプルの解凍ホルダ



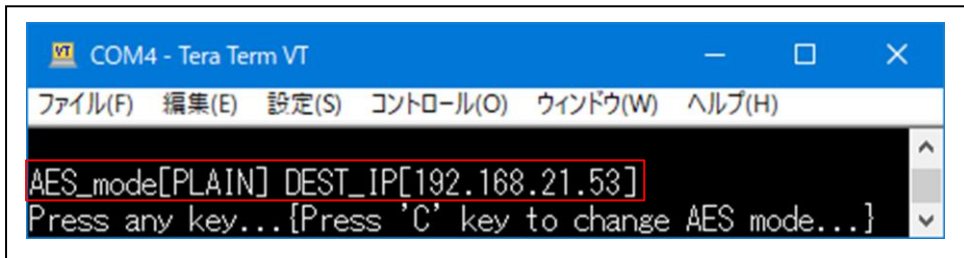
「TCP_IP_AES_OpenSSL.exe」を起動

- 2) 「TCP_IP_AES_OpenSSL」の各項目を設定して「基板」側からの「接続」を待つ。



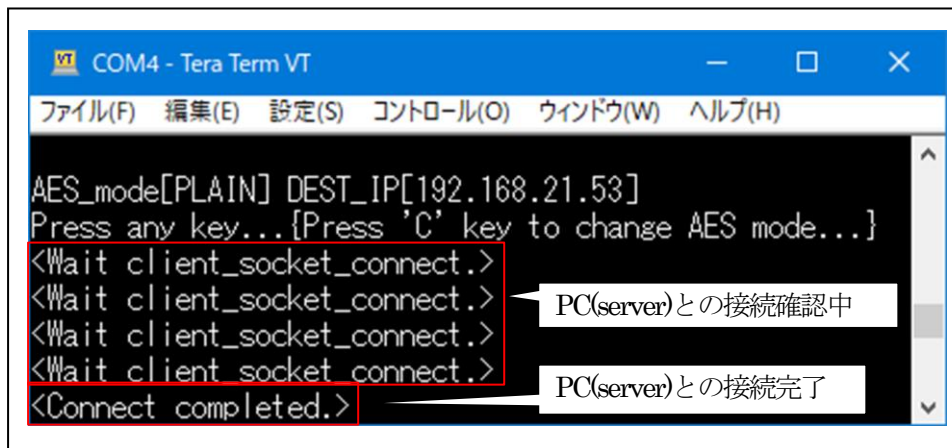
3) 基板側の各項目の確認と設定。

表示項目	説明
AES_mode[PLAIN]	送受信モードの指定 ◎変数のフラグにより指定 aes.c : int AES_crypto_mode = PLAIN; //0=PLAIN
DEST_IP[192.168.21.53]	送信先(PC側)IPアドレス ◎defineにて指定 tcp_aes_thread_entry.c : #define DEST_IP IP_ADDRESS(192,168,21,53)



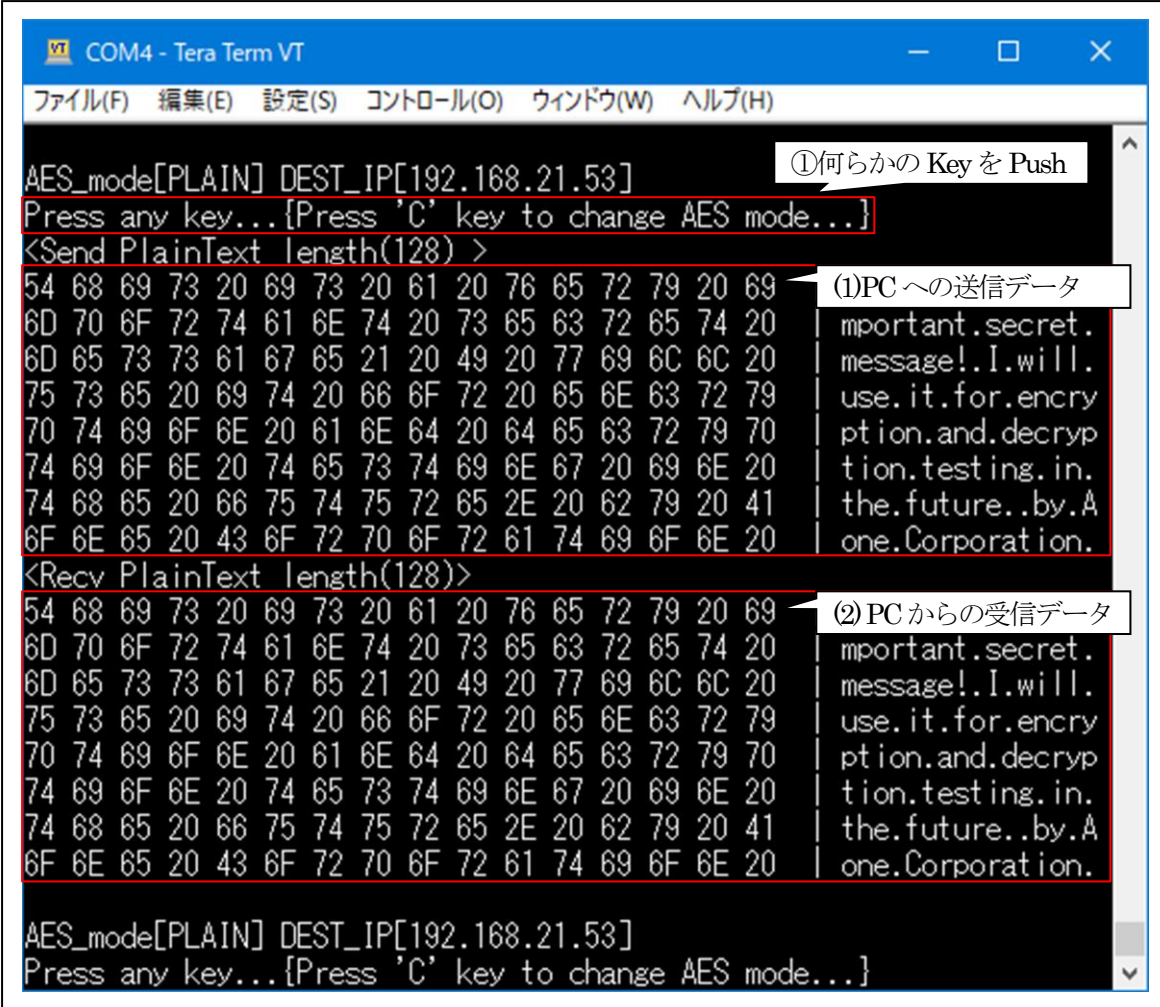
4) 基板側から PC(server)側へ平文テキストを送信する。

① disconnection の場合は、PC(server)との Connection 処理を実行



☆接続が失敗した場合は「Ctrl+C」Key-Push で中断する。

②接続完了後、「基板」側から PC(server)側へ平文テキストを送受信する



```

COM4 - Tera Term VT
ファイル(F) 編集(E) 設定(S) コントロール(O) ウインドウ(W) ヘルプ(H)
AES_mode[PLAIN] DEST_IP[192.168.21.53]
Press any key...{Press 'C' key to change AES mode...}
<Send PlainText length(128) >
54 68 69 73 20 69 73 20 61 20 76 65 72 79 20 69
6D 70 6F 72 74 61 6E 74 20 73 65 63 72 65 74 20
6D 65 73 73 61 67 65 21 20 49 20 77 69 6C 6C 20
75 73 65 20 69 74 20 66 6F 72 20 65 6E 63 72 79
70 74 69 6F 6E 20 61 6E 64 20 64 65 63 72 79 70
74 69 6F 6E 20 74 65 73 74 69 6E 67 20 69 6E 20
74 68 65 20 66 75 74 75 72 65 2E 20 62 79 20 41
6F 6E 65 20 43 6F 72 70 6F 72 61 74 69 6F 6E 20
important.secret.
message!.I.will.
use.it.for.ency
ption.and.decry
tion.testing.in.
the.future..by.A
one.Corporation.
<Recv PlainText length(128)>
54 68 69 73 20 69 73 20 61 20 76 65 72 79 20 69
6D 70 6F 72 74 61 6E 74 20 73 65 63 72 65 74 20
6D 65 73 73 61 67 65 21 20 49 20 77 69 6C 6C 20
75 73 65 20 69 74 20 66 6F 72 20 65 6E 63 72 79
70 74 69 6F 6E 20 61 6E 64 20 64 65 63 72 79 70
74 69 6F 6E 20 74 65 73 74 69 6E 67 20 69 6E 20
74 68 65 20 66 75 74 75 72 65 2E 20 62 79 20 41
6F 6E 65 20 43 6F 72 70 6F 72 61 74 69 6F 6E 20
important.secret.
message!.I.will.
use.it.for.ency
ption.and.decry
tion.testing.in.
the.future..by.A
one.Corporation.
AES_mode[PLAIN] DEST_IP[192.168.21.53]
Press any key...{Press 'C' key to change AES mode...}
  
```

☆受信処理が失敗した場合は「Ctrl+C」Key-Push で中断する。

5) 基板側の原文保存場所 (各モード共通)

モジュール名	変数名
tcp_aes_thread_entry.c	static UCHAR *src_str={ //テスト用原文 "This is a very important secret message!" "I will use it for encryption and decryption testing" "in the future. by Aone Corporation" };

6) 「TCP_IP_AES_OpenSSL」側の送受信を確認する。

The screenshot shows the 'TCP_IP_AES_OpenSSL(server) Ver1.10' application. The 'Setting' section includes PC IP address (192.168.21.53), PC port (50000), and a 'モニタ' (Monitor) checkbox which is checked. The 'Monitor' window displays the following log:

```

<<< Wait Connect >>>
接続しました。          接続完了
<<< Wait Receive data[1] >>>
-(1)Receive plain data from client
54 68 69 73 20 69 73 20 61 20 76 65 72 79 20 69  This.is.a.very.i
6D 70 6F 72 74 61 6E 74 20 73 65 63 72 65 74 20  mportant.secret.
6D 65 73 73 61 67 65 21 20 49 20 77 69 6C 6C 20  message!.I.will.
75 73 65 20 69 74 20 66 6F 72 20 65 6E 63 72 79  use.it.for.ency
70 74 69 6F 6E 20 61 6E 64 20 64 65 63 72 79 70  ption.and.decry
74 69 6F 6E 20 74 65 73 74 69 6E 67 20 69 6E 20  tion.testing.in.
74 68 65 20 66 75 74 75 72 65 2E 20 62 79 20 41  the.future..by.A
6F 6E 65 20 43 6F 72 70 6F 72 61 74 69 6F 6E 20  one.Corporation.
-(2)Send plain data to client
54 68 69 73 20 69 73 20 61 20 76 65 72 79 20 69  This.is.a.very.i
6D 70 6F 72 74 61 6E 74 20 73 65 63 72 65 74 20  mportant.secret.
6D 65 73 73 61 67 65 21 20 49 20 77 69 6C 6C 20  message!.I.will.
75 73 65 20 69 74 20 66 6F 72 20 65 6E 63 72 79  use.it.for.ency
70 74 69 6F 6E 20 61 6E 64 20 64 65 63 72 79 70  ption.and.decry
74 69 6F 6E 20 74 65 73 74 69 6E 67 20 69 6E 20  tion.testing.in.
74 68 65 20 66 75 74 75 72 65 2E 20 62 79 20 41  the.future..by.A
6F 6E 65 20 43 6F 72 70 6F 72 61 74 69 6F 6E 20  one.Corporation.
<<< Wait Receive data[2] >>>

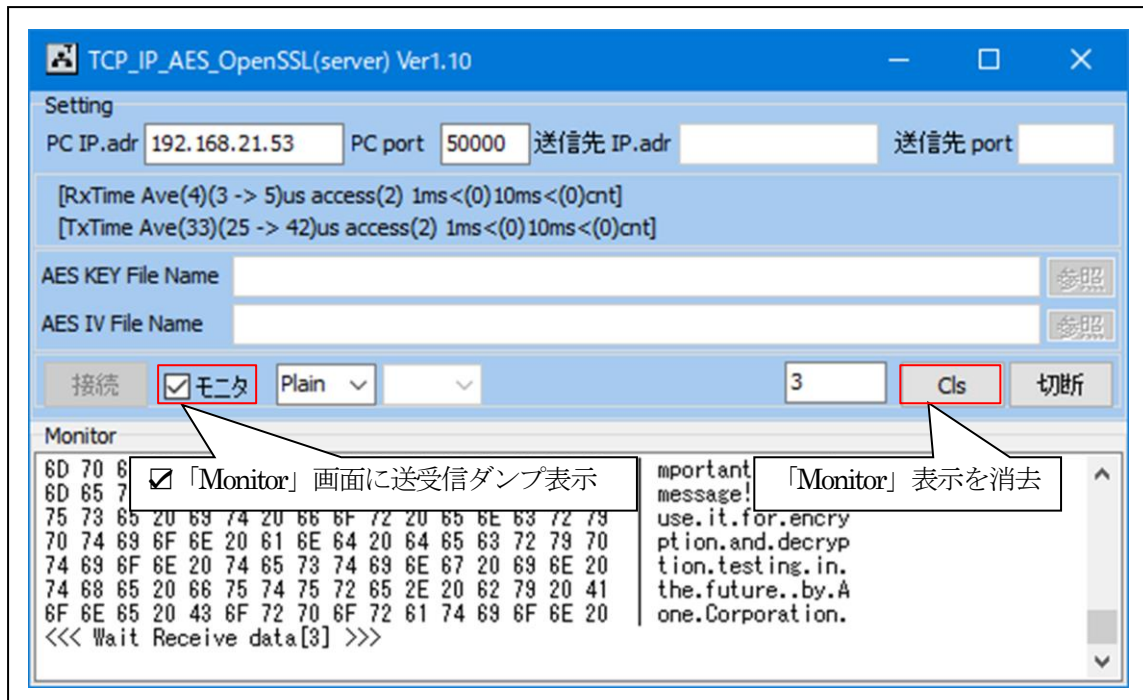
```

Annotations in the image:

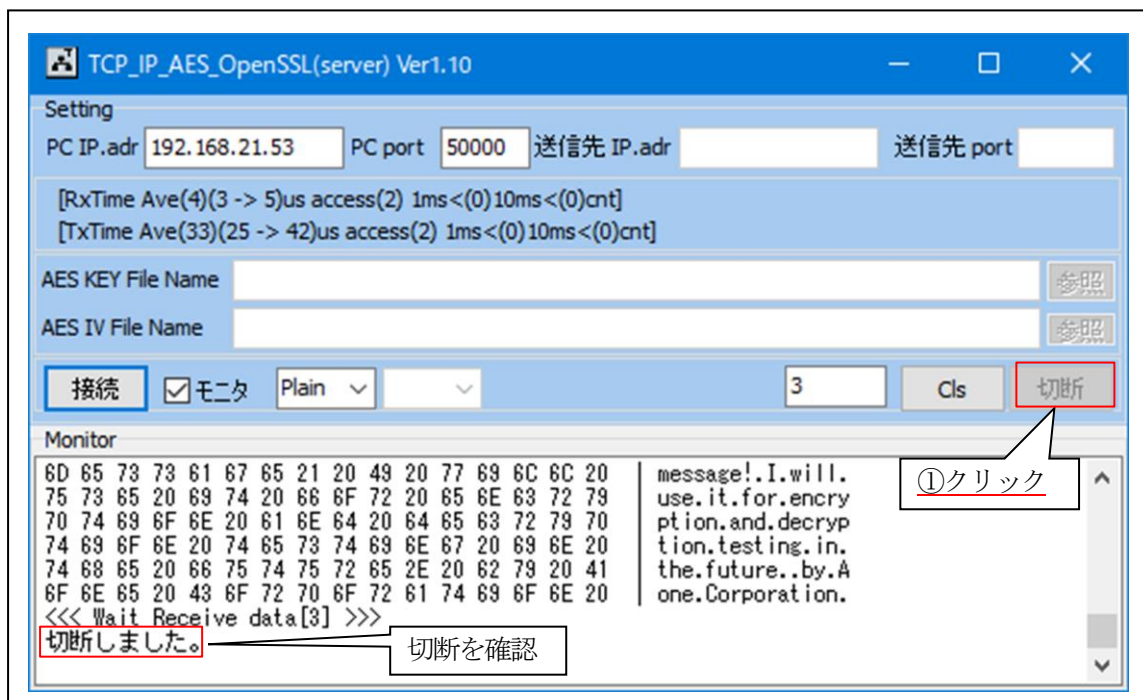
- A box labeled '接続完了' (Connection completed) points to the '接続しました。' (Connected) message.
- A box labeled '(1) 「基板」側からの受信データ' (Received data from the board) points to the first block of hex and ASCII data.
- A box labeled '(2) 「基板」側への送信データ' (Transmitted data to the board) points to the second block of hex and ASCII data.

☆受信データをそのまま送信します。(ループバック)

7) 「TCP_IP_AES_OpenSSL」 その他の操作 (各モード共通)

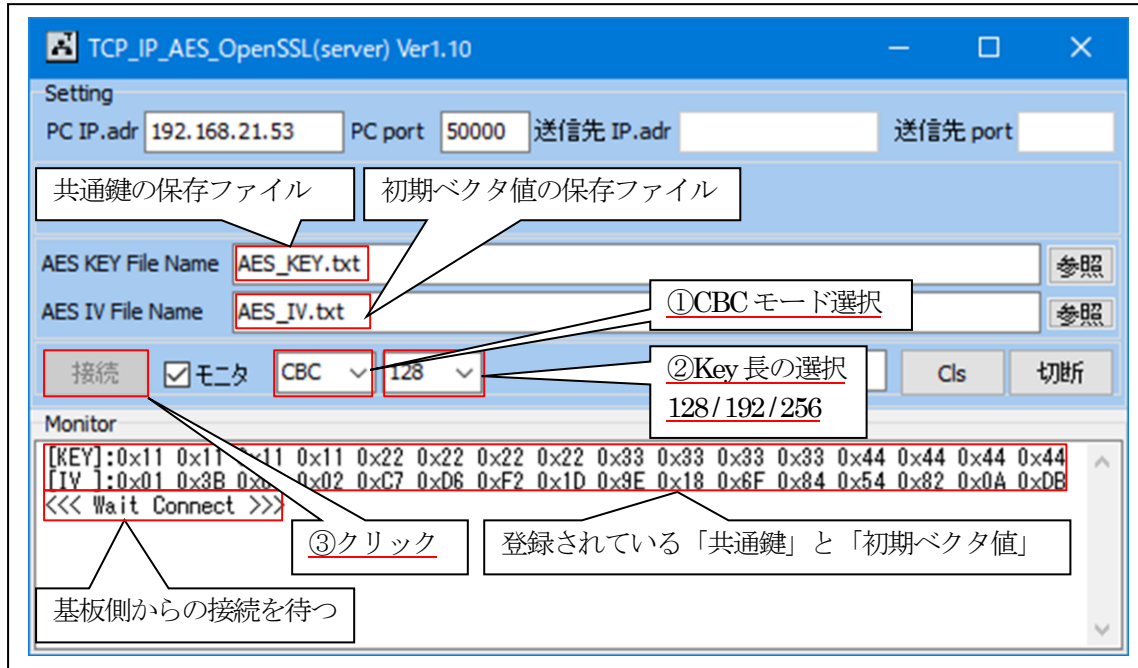


8) TCP_IP-Portを「切断」する。(各モード共通)



5-5. Windows PC 側のテスト用プログラムで動作確認 (AES-CBC モード)

- 1) 「TCP_IP_AES_OpenSSL.exe」を起動する。
- 2) 「TCP_IP_AES_OpenSSL」の各項目を設定して「基板」側からの「接続」を待つ。



3) 「AES_KEY.txt」「AES_IV.txt」の説明

```

「AES_KEY.txt」共通鍵テキストファイル
// default aes_common_key 共通鍵 128bit | 192bit | 256bit
// コメント行は、//のみの使用にしてください。
0x11,0x11,0x11,0x11,0x22,0x22,0x22,0x22,0x33,0x33,0x33,0x33,0x44,0x44,0x44,0x44, // 128bit
0x55,0x55,0x55,0x55,0x66,0x66,0x66,0x66, // ↑ + 192bit
0x77,0x77,0x77,0x77,0x88,0x88,0x88,0x88, // ↑ + 256bit
  
```

☆共通鍵を変更する場合は、基板側と同等の鍵を適当なエディタで変更する。

```

「AES_IV.txt」初期ベクタ値テキストファイル
// default aes_initial_vect 初期化ベクタ
// コメント行は、//のみの使用にしてください。
0x01,0x3B,0x01,0x02,0xC7,0xD6,0xF2,0x1D,0x9E,0x18,0x6F,0x84,0x54,0x82,0x0A,0xDB
  
```

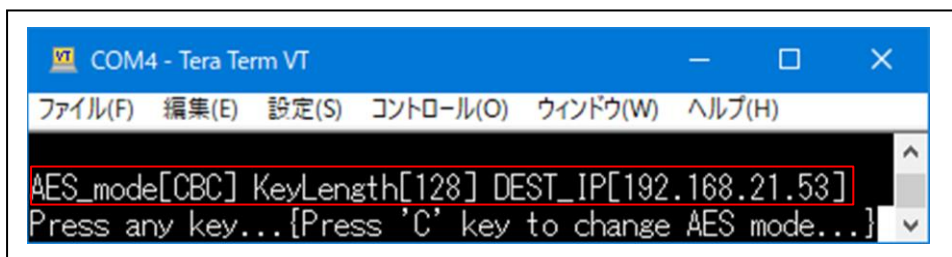
☆初期ベクタ値を変更する場合は、基板側と同等の初期ベクタ値を適当なエディタで変更する。

4) 基板側の各項目の確認と設定。

表示項目	説明
AES_mode[CBC]	送受信モードの指定 ◎変数のフラグにより指定 aes.c : int AES_crypto_mode = CBC; // 1=CBC
KeyLength[128]	AES-CBC モード時の Key ビット時の指定 ◎変数の数値により指定 aes.c : int AES_crypto_bit = 128;
DEST_IP[192.168.21.53]	送信先(PC 側)IP アドレス ◎define にて指定 tcp_aes_thread_entry.c : #define DEST_IP IP_ADDRESS(192,168,21,53)

共通鍵データの保存モジュールと変数 [aes.c]
<pre>uint8_t AES_key[32] = { // default aes_common_key 共通鍵 128bit 192bit 256bit 0x11,0x11,0x11,0x11,0x22,0x22,0x22,0x22,0x33,0x33,0x33,0x33,0x44,0x44,0x44,0x44, // 128bit 0x55,0x55,0x55,0x55,0x66,0x66,0x66,0x66, // ↑ + 192bit 0x77,0x77,0x77,0x77,0x88,0x88,0x88,0x88, // ↑ + 256bit };</pre>

初期ベクタ値データの保存モジュールと変数 [aes.c]
<pre>uint8_t AES_iv[16] = { // default aes_initial_vect 初期化ベクタ 0x01,0x3B,0x01,0x02,0xC7,0xD6,0xF2,0x1D,0x9E,0x18,0x6F,0x84,0x54,0x82,0x0A,0xDB };</pre>



5) 基板側から PC(server) 側へ CBC 暗号テキストを送信する。

COM5 - Tera Term VT

ファイル(F) 編集(E) 設定(S) コントロール(O) ウィンドウ(W) ヘルプ(H)

AES_mode[**CBC**] KeyLength[128] DEST_IP[192.168.21.5] ①何らかの Key を Push
 Press any key...[Press 'C' key to change AES mode...]

<PlainText length(128) >

54 68 69 73 20 69 73 20 61 20 76 65 72 79 20 69
 6D 70 6F 72 74 61 6E 74 20 73 65 63 72 65 74 20
 6D 65 73 73 61 67 65 21 20 49 20 77 69 6C 6C 20
 75 73 65 20 69 74 20 66 6F 72 20 65 6E 63 72 79
 70 74 69 6F 6E 20 61 6E 64 20 64 65 63 72 79 70
 74 69 6F 6E 20 74 65 73 74 69 6E 67 20 69 6E 20
 74 68 65 20 66 75 74 75 72 65 2E 20 62 79 20 41
 6F 6E 65 20 43 6F 72 70 6F 72 61 74 69 6F 6E 20
 message...it will
 use.it.for.ency
 ption.and.decry
 ption.testing.in
 the.future..by.A
 one.Corporation.

<Send EncryptText length(128)>

44 50 E8 F0 DA 72 DE 0D 8E D4 8F 1D B3 04 73 C0
 29 30 C8 09 06 DE 48 C2 90 52 08 49 8B 69 63 E1
 64 32 1C 1D C1 8D 80 18 17 45 61 B7 3B B2 25 11
 36 6A 2A CB 36 25 FD 42 07 66 45 31 D2 DF 74 3E
 E4 44 F8 65 49 72 88 B5 30 ED 13 FD 8B A3 06 43
 17 E0 26 1F 9E C5 24 FD 88 18 69 0A 27 89 A7 78
 30 8D 5D B0 0F C9 A1 B2 68 81 40 A8 8C 27 F2 B0
 13 5D 17 A6 FE 18 DA 13 8F 91 7D 06 53 3A 33 BA
 0]~ノ。ih.@i.'-
 .]ヲ。レ...}S:30

<Recv EncryptText length(128)>

44 50 E8 F0 DA 72 DE 0D 8E D4 8F 1D B3 04 73 C0
 29 30 C8 09 06 DE 48 C2 90 52 08 49 8B 69 63 E1
 64 32 1C 1D C1 8D 80 18 17 45 61 B7 3B B2 25 11
 36 6A 2A CB 36 25 FD 42 07 66 45 31 D2 DF 74 3E
 E4 44 F8 65 49 72 88 B5 30 ED 13 FD 8B A3 06 43
 17 E0 26 1F 9E C5 24 FD 88 18 69 0A 27 89 A7 78
 30 8D 5D B0 0F C9 A1 B2 68 81 40 A8 8C 27 F2 B0
 13 5D 17 A6 EE 18 DA 13 8F 91 7D 06 53 3A 33 BA
 0]~ノ。ih.@i.'-
 .]ヲ。レ...}S:30

<DecryptText length(128) >

54 68 69 73 20 69 73 20 61 20 76 65 72 79 20 69
 6D 70 6F 72 74 61 6E 74 20 73 65 63 72 65 74 20
 6D 65 73 73 61 67 65 21 20 49 20 77 69 6C 6C 20
 75 73 65 20 69 74 20 66 6F 72 20 65 6E 63 72 79
 70 74 69 6F 6E 20 61 6E 64 20 64 65 63 72 79 70
 74 69 6F 6E 20 74 65 73 74 69 6E 67 20 69 6E 20
 74 68 65 20 66 75 74 75 72 65 2E 20 62 79 20 41
 6F 6E 65 20 43 6F 72 70 6F 72 61 74 69 6F 6E 20
 ption.and.decry
 ption.testing.in
 the.future..by.A
 one.Corporation.

①基板側に保存してある原文のダンプ表示

②原文を暗号化してPC(server)側に送信した暗号文のダンプ表示

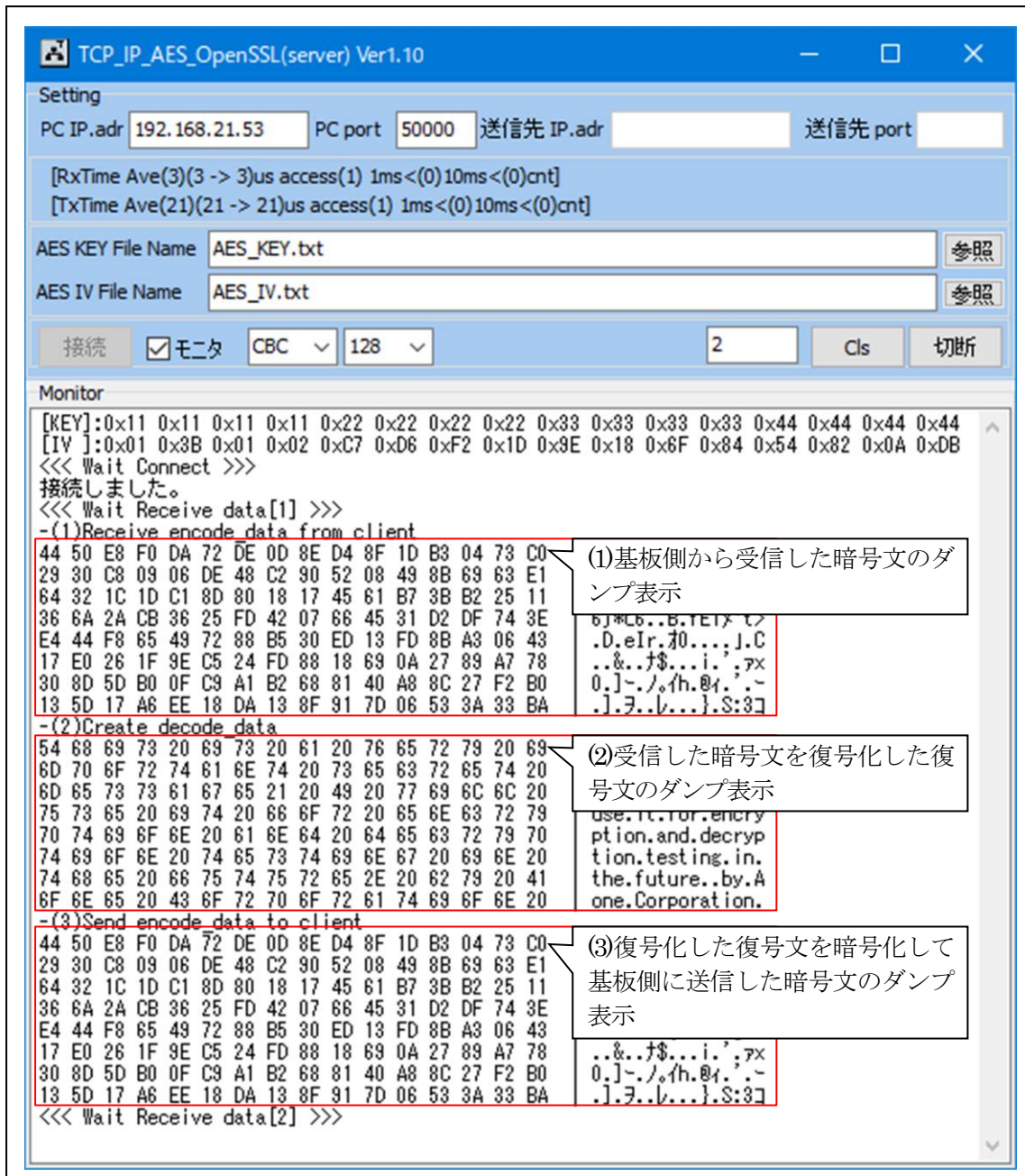
③PC(server)が受信した暗号文を復号した文章をPC(server)側で暗号化した暗号文を受信したダンプ表示

④受信したPC(server)からの暗号文を復号化した複合文のダンプ表示

☆受信処理が失敗した場合は「**Ctrl+C**」Key-Push で中断する。

- ① 「(1)PlainText」と「(4)DecryptText」が同等の場合、基板側と PC 側が同等な復号処理（デコード）であることの実証になる。
- ② 「(2)Send EncryptText」と「(3)Recv EncryptText」が同等の場合、基板側と PC 側が同等な暗号処理（エンコード）であることの実証になる。

6) 「TCP_IP_AES_OpenSSL」側の送受信を確認する。



Setting

PC IP.adr 192.168.21.53 PC port 50000 送信先 IP.adr 送信先 port

[RxTime Ave(3)(3 -> 3)us access(1) 1ms<(0)10ms<(0)cnt]
[TxTime Ave(21)(21 -> 21)us access(1) 1ms<(0)10ms<(0)cnt]

AES KEY File Name AES_KEY.txt 参照
AES IV File Name AES_IV.txt 参照

接続 モニタ CBC 128 2 Cls 切断

Monitor

[KEY]:0x11 0x11 0x11 0x11 0x22 0x22 0x22 0x22 0x33 0x33 0x33 0x33 0x44 0x44 0x44 0x44
[IV]:0x01 0x3B 0x01 0x02 0xC7 0xD6 0xF2 0x1D 0x9E 0x18 0x6F 0x84 0x54 0x82 0x0A 0xDB
<<< Wait Connect >>>
接続しました。
<<< Wait Receive data[1] >>>
-(1)Receive encode data from client

44 50 E8 F0 DA 72 DE 0D 8E D4 8F 1D B3 04 73 C0
29 30 C8 09 06 DE 48 C2 90 52 08 49 8B 69 63 E1
64 32 1C 1D C1 8D 80 18 17 45 61 B7 3B B2 25 11
36 6A 2A CB 36 25 FD 42 07 66 45 31 D2 DF 74 3E
E4 44 F8 65 49 72 88 B5 30 ED 13 FD 8B A3 06 43
17 E0 26 1F 9E C5 24 FD 88 18 69 0A 27 89 A7 78
30 8D 5D B0 0F C9 A1 B2 68 81 40 A8 8C 27 F2 B0
13 5D 17 A6 EE 18 DA 13 8F 91 7D 06 53 3A 33 BA

(1)基板側から受信した暗号文のダンプ表示

6] *C6..B.TE] *C
.D.e]r. *0...].C
..&.. *\$...i.' *x
0.]-. /..h. *4.'.-
.]. *..b...}.S: *3]

-(2)Create decode data

54 68 69 73 20 69 73 20 61 20 76 65 72 79 20 69
6D 70 6F 72 74 61 6E 74 20 73 65 63 72 65 74 20
6D 65 73 73 61 67 65 21 20 49 20 77 69 6C 6C 20
75 73 65 20 69 74 20 66 6F 72 20 65 6E 63 72 79
70 74 69 6F 6E 20 61 6E 64 20 64 65 63 72 79 70
74 69 6F 6E 20 74 65 73 74 69 6E 67 20 69 6E 20
74 68 65 20 66 75 74 75 72 65 2E 20 62 79 20 41
6F 6E 65 20 43 6F 72 70 6F 72 61 74 69 6F 6E 20

(2)受信した暗号文を復号化した復号文のダンプ表示

use. r. r. for. encry
ption. and. decryp
tion. testing. in.
the. future. by. A
one. Corporation.

-(3)Send encode data to client

44 50 E8 F0 DA 72 DE 0D 8E D4 8F 1D B3 04 73 C0
29 30 C8 09 06 DE 48 C2 90 52 08 49 8B 69 63 E1
64 32 1C 1D C1 8D 80 18 17 45 61 B7 3B B2 25 11
36 6A 2A CB 36 25 FD 42 07 66 45 31 D2 DF 74 3E
E4 44 F8 65 49 72 88 B5 30 ED 13 FD 8B A3 06 43
17 E0 26 1F 9E C5 24 FD 88 18 69 0A 27 89 A7 78
30 8D 5D B0 0F C9 A1 B2 68 81 40 A8 8C 27 F2 B0
13 5D 17 A6 EE 18 DA 13 8F 91 7D 06 53 3A 33 BA

(3)復号化した復号文を暗号化して基板側に送信した暗号文のダンプ表示

..&.. *\$...i.' *x
0.]-. /..h. *4.'.-
.]. *..b...}.S: *3]

<<< Wait Receive data[2] >>>

- ① 「(1)Receive encode_data from client」と「(3)Send encode_data to client」が同等の場合、基板側とPC側が同等な暗号処理（エンコード）であることの実証になる。
- ② 「(2)Create decode_data」と「基板」側の「(4)DecryptText」が同等の場合、基板側とPC側が同等な復号処理（デコード）であることの実証になる。

6. 注意事項

- 本文書の著作権は、エーワン（株）が保有します。
- 本文書を無断での転載は一切禁止します。
- 本文書に記載されている内容についての質問やサポートはお受けすることが出来ません。
- 本文章に関して、ルネサス エレクトロニクス社への問い合わせは御遠慮願います。
- 本文書の内容に従い、使用した結果、損害が発生しても、弊社では一切の責任を負わないものとします。
- 本文書の内容に関して、万全を期して作成しましたが、ご不審な点、誤りなどの点がありましたら弊社までご連絡ください幸いです。
- 本文書の内容は、予告なしに変更されることがあります。

7. 商標

- e2studio・RX65N は、ルネサス エレクトロニクス株式会社の登録商標または商品名称です。
- CK-RX65N は、ルネサス エレクトロニクス株式会社の商品名です。
- 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。

8. 参考文献

- 「RX65N ユーザーズマニュアル ハードウェア編」 ルネサス エレクトロニクス株式会社
- 「e2studio ユーザーズマニュアル 入門ガイド」 ルネサス エレクトロニクス株式会社
- 「AzureRTOS」 マイクロソフト株式会社
- ルネサス エレクトロニクス株式会社提供のサンプル集
- その他

〒486-0852

愛知県春日井市下市場町 6-9-20

エーワン株式会社

<https://www.aone.co.jp>

