

# **SKSTACK-IP**

## **(Single-hop Edition)**

### **SK コマンド**

### **リファレンスマニュアル**

TESSERA TECHNOLOGY INC

Document Version: 1.2.1a  
Published Date: 4<sup>th</sup> July 2016

改版履歴

日付	版	変更内容
2014 年 4 月 19 日	初版	
2014 年 5 月 24 日	1.2.1	SKSEND, SKSENDTO コマンドの入力、応答内容の誤記修正 PaC 再認証開始のタイミングを変更
2016 年 7 月 4 日	1.2.1a	Wi-SUN ルート B の接続例を追記 SKLL64 コマンド追記 周波数とチャンネル番号の対応表を追記 RSSI の計算方法を追記

## Contents

1. Document Overview .....	5
1.1 SK コマンド .....	5
1.2 シリアル通信設定 .....	5
2. SK コマンド チュートリアル .....	6
2.1 初期設定 .....	6
2.2 設定の確認 .....	6
2.3 コーディネータの起動 .....	6
2.4 コーディネータの検索 .....	7
2.5 相手に UDP でデータを送る .....	8
2.6 TCP 通信 .....	8
2.7 TCP による通信 .....	9
2.8 コネクションの切断 .....	9
2.9 認証と暗号化 .....	10
2.10 Wi-SUN B ルート接続例 .....	11
3. 仮想レジスタ .....	13
3.1 仮想レジスタ .....	13
4. コマンドリファレンス .....	15
4.1 SKSREG .....	16
4.2 SKINFO .....	17
4.3 SKSTART .....	18
4.4 SKJOIN .....	19
4.5 SKREJOIN .....	21
4.6 SKTERM .....	22
4.7 SKSENDTO .....	23
4.8 SKCONNECT .....	25
4.9 SKSEND .....	26
4.10 SKCLOSE .....	28
4.11 SKPING .....	29
4.12 SKSCAN .....	30
4.13 SKREGDEV .....	31
4.14 SKRMDEV .....	32
4.15 SKSETKEY .....	33
4.16 SKRMKEY .....	34

4.17	SKSECENABLE.....	35
4.18	SKSETPSK.....	36
4.19	SKSETPWD .....	37
4.20	SKSETRBID.....	38
4.21	SKADDNBR .....	39
4.22	SKUDPPORT .....	40
4.23	SKTCPPORT .....	41
4.24	SKSAVE.....	42
4.25	SKLOAD.....	43
4.26	SKERASE .....	44
4.27	SKVER.....	45
4.28	SKRESET.....	46
4.29	SKTABLE .....	47
4.30	SKLL64.....	48
5.	イベント .....	49
5.1	ERXUDP.....	49
5.2	ERXTCP.....	49
5.3	EPONG .....	50
5.4	ETCP.....	50
5.5	EADDR.....	50
5.6	ENEIGHBOR .....	51
5.7	EPANDESC .....	51
5.8	EEDSCAN.....	51
5.9	EHANDLE .....	52
5.10	EVENT.....	53
6.	ポート番号 .....	55
6.1	UDP ポート .....	55
6.2	TCP ポート .....	55
7.	TCP タイムアウト時間 .....	56
8.	周波数とチャンネル番号.....	57
9.	エラーコード.....	58
10.	スタック仕様.....	59
10.1	準拠規格.....	59
11.	無線仕様.....	59
11.1	ARIB T108 仕様.....	59

12.	MAC 仕様 .....	60
12.1	IEEE 802.15.4 .....	60
13.	6LowPAN 仕様 .....	61
13.1	6LowPAN .....	61
14.	IP 仕様 .....	62
14.1	IP .....	62
14.2	TCP .....	62
14.3	UDP .....	62
15.	注意事項 .....	63
15.1	変更 .....	63

## 1. Document Overview

本ドキュメントは SKSTACK-IP (Single-hop Edition )用 SK コマンドの使い方を記述した文書です。

### 1.1 SK コマンド

SK コマンドは先頭が”SK”で始まる短いコマンドの集合です。パラメータ設定、UDP データ送受信、TCP 通信制御など SKSTACK-IP の主要機能が SK コマンドを介して実行できます。コマンドは ASCII 文字で指定し、コマンド引数の区切りにはホワイトスペースを使います。

また仮想レジスタと呼ばれるパラメータ指定用の変数が用意されており、対応するレジスタに適切な値を設定することで、プロトコルの挙動を調整、変更することができます。

### 1.2 シリアル通信設定

項目名	設定値
ボーレート	115.2kbps
キャラクタ長	8 ビット
ストップ・ビット	1 ビット
パリティ	なし
フロー制御	なし
改行コード	CRLF
ローカルエコー	必要なし

## 2. SK コマンド チュートリアル

2 台の端末で通信を行う SK コマンドの実行例を以下に紹介します。(コマンド表記中のホワイトスペースを「`_`」で示してあります)

### 2.1 初期設定

事前に個別設定すべき項目は MAC アドレス (IEEE 64 bit アドレス) です。以下のように指定します。(製品によっては予め設定されています)

端末 1 :

```
SKSREG _S1_ 12345678ABCDEF01
```

端末 1 の 64 bit アドレスを 0x 12345678ABCDEF01 に設定。

端末 2 :

```
SKSREG _S1_ 12345678ABCDEF02
```

端末 2 の 64 bit アドレスを 0x 12345678ABCDEF02 に設定。

### 2.2 設定の確認

SKINFO コマンドで現在の設定を確認します。以下のように表示されることを確認してください。

端末 1 :

```
EINFO _FE80:0000:0000:0000:1034:5678:ABCD:EF01_ 12345678ABCDEF01_ 21_FF  
FF_FFFE
```

端末 2 :

```
EINFO _FE80:0000:0000:0000:1034:5678:ABCD:EF02_ 12345678ABCDEF02_ 21_FF  
FF_FFFE
```

2.1 で指定した 64 bit アドレスから IPv6 リンクローカルアドレスが生成され、自端末用のアドレスとして設定されているのが確認できます。以後、このリンクローカルアドレスを使用します。

### 2.3 コーディネータの起動

端末 1 をコーディネータとして利用します。このため、まず ED スキャンで各チャンネルの電波状態を把握します。

SKSCAN\_0\_0\_FFFFFFFF\_4

得られた結果から最適と思われるチャンネルを選択し設定します。PAN ID は 0xFFFF 以外の値を選択して設定します。PAN ID の重複を確認するためアクティブスキャンを行って周囲の PAN を検索しても良いです。

端末 1: Ch33 (922.5 MHz)を選択

SKSREG\_S2\_21

端末 1: PAN ID 0x8888 を選択

SKSREG\_S3\_8888

最後に S15 レジスタを 1 にしてコーディネータとして起動します。

SKSREG\_S15\_1

## 2.4 コーディネータの検索

コーディネータと通信したいデバイスは、アクティブスキャンを使ってコーディネータを検索します。

端末 2:

SKSCAN\_2\_0\_FFFFFFFF\_6

以下の結果が得られます。

EVENT 20

EPANDESC

Channel:33

Channel Page:09

Pan ID:8888

Addr:12345678abcdef01

LQI:50

Pair ID:CCDDEEFF



mode=2 で拡張アクティブスキャンを行うと、自端末と同じ Pairing ID を設定しているコーディネータのみが応答します。周囲に複数のコーディネータが存在する場合、EPANDESC イベントが複数回、通知されることがあります。その中から通信したい相手を選択し、そのチャンネルと PAN ID を同じ値に設定します。

端末 2:  
SKSREG \_S2\_21

端末 2:  
SKSREG \_S3\_8888

## 2.5 相手に UDP でデータを送る

UDP でデータを送るには SKSENDTO コマンドを使います。

端末 2 上で :  
SKSENDTO \_1\_  
FE80:0000:0000:0000:1034:5678:ABCD:EF01\_0E1A\_0\_0005\_12345  
(実際には 1 行です。データ部の”12345”はエコーバックされません)

端末 1 のポート 3610 番(0xE1A)宛てに、5 バイトのデータを UDP データグラムで送信します。

端末 1 :  
ERXUDP \_FE80:0000:0000:0000:1034:5678:ABCD:EF02\_  
FE80:0000:0000:0000:1034:5678:ABCD:EF01\_0E1A\_0E1A\_12345678ABCDEF02\_0  
005\_3132333435  
(実際には 1 行です)

(IP パケット送信に先立って、MAC アドレス解決のためにアドレス要請が実行される場合があります。)

## 2.6 TCP 通信

次に TCP でデータ通信してみます。まずコネクションの確立を行います。

端末 1 :

```
SKCONNECT _FE8000000000000010345678ABCDEF02 _0E1A _0E1A
```

端末 2 のポート 3610 番 (0x0E1A) に接続要求を出します。接続に成功すると両端末で以下のようにイベントが表示されるはずです。

端末 1 :

```
ETCP _01 _01 _FE80:0000:0000:0000:1034:5678:ABCD:EF02 _0E1A _0E1A
```

端末 2 :

```
ETCP _01 _01 _FE80:0000:0000:0000:1034:5678:ABCD:EF01 _0E1A _0E1A
```

接続に成功し、そのコネクションのハンドル番号が 1 であることを示します。

## 2.7 TCP による通信

データを送る場合は SKSEND コマンドを使います。

端末 1 :

```
SKSEND _1 _0005 _12345
```

端末 2 では以下のように表示されます。

```
ERXTCP _FE80:0000:0000:0000:1034:5678:ABCD:EF01 _0E1A _0E1A  
_0005 _3132333435
```

また端末 1 では送信成功を通知するイベントが発生します。

端末 1 :

```
ETCP _05 _01
```

TCP コネクションは双方向なので、端末 2 側で同様に「SKSEND 1 0005 12345」コマンドを発行すると、端末 1 がデータを受信します。

コネクション確立後の TCP 通信では、相手先の Ipv6 アドレスを指定する必要はありません。コネクションのハンドル番号で通信可能です。

## 2.8 コネクションの切断

どちらかの端末で SKCLOSE を発行すると TCP コネクションが切断され、ハンドル番号が

開放されます。

端末 1 :

SKCLOSE\_1

端末 1, 2 両方で、コネクション切断のイベント通知が発生します。

ETCP\_03\_01

以後、ハンドル番号 1 によるデータ通信はエラーとなります。

## 2.9 認証と暗号化

PANA 認証による接続と暗号化通信を利用するには、コーディネータ起動前にまず PSK を設定します。

端末 1 :

SKSETPSK\_10\_000102030405060708090a0b0c0d0e0f

その後、「コーディネータの起動」にしたがってチャンネル、PAN ID を決定後、最後に SKSTART コマンドを発行します。(S15 レジスタは自動的に 1 になります)。

デバイスも同様に PSK を設定します。

端末 2 :

SKSETPSK\_10\_000102030405060708090a0b0c0d0e0f

その後、アクティブスキャンで接続先のコーディネータを確定したら、SKJOIN コマンドで接続を開始します。

端末 2 :

0x12345678abcdef01 のコーディネータへ接続する

SKJOIN\_FE80:0000:0000:0000:1034:5678:ABCD:EF01

SKJOIN コマンドを発行すると PANA 認証が進行します。その間、ポート 716 番の UDP データが ERXUDP イベントで通知されます。

接続に成功すると EVENT 25 が発生し接続相手が通知されます。

端末 2 :

EVENT 25 FE80:0000:0000:0000:1034:5678:ABCD:EF01

端末 1 :

EVENT 25 FE80:0000:0000:0000:1034:5678:ABCD:EF02

この時点で相手方との暗号化通信が有効になります。

端末 2 :

暗号オプション=1 で UDP を送信

SKSENDTO 1 FE80:0000:0000:0000:1034:5678:ABCD:EF01 0E1A 1 0001 1

端末 1 :

受信した UDP が暗号化されている(<SECURED>引数 = 1)ことが分かります。

ERXUDP FE80:0000:0000:0000:1034:5678:ABCD:EF02

FE80:0000:0000:0000:1034:5678:ABCD:EF01 0E1A 0E1A 12345678ABCDEF02 1 0001 31

一方で接続に失敗すると接続元で EVENT 24 が発生します。PSK が異なっている、PAN ID が一致していないので通信が失敗しているなどの要因で接続は失敗します。

## 2.10 Wi-SUN B ルート接続例

※端末を一度接続しなおしてから実行してください。

スマートメータ側(親機:PAA)設定と起動

SKSREG S2 29 ; チャンネル設定

SKSREG S3 8888 ; PAN ID 設定

SKSETPWD C 0123456789AB ; パスワード設定

SKSETRBID 00112233445566778899AABBCCDD00FF ; Rout-B ID 設定

SKSTART ; PAA 動作開始

デバイス側(子機:PaC)の設定と起動

SKSETPWD C 0123456789AB ; パスワード設定

SKSETRBID 00112233445566778899AABBCCDD00FF ; Rout-B ID 設定

SKSCAN \_2\_ FFFFFFFF \_6 ; アクティブスキャン実行  
見つけた親機のチャンネルと PAN ID を合わせる。

SKSREG \_S2\_ 29

SKSREG \_S3\_ 8888

見つけた親機の MAC アドレスを IPv6 アドレスに変換

SKLL64 \_12345678ABCDEF01

FE80:0000:0000:0000:1034:5678:ABCD:EF01

SKJOIN \_FE80:0000:0000:0000:1034:5678:ABCD:EF01 ; PAA 接続シーケンス開始

EVENT 25 が発生すれば、接続完了。EVENT 24 なら失敗

(動作状態 get コマンド例)

SKSENDTO \_1\_ FE80:0000:0000:0000:1034:5678:ABCD:EF01 \_0E1A\_ 1\_

000E\_ (\$10 \$81 \$00\$01 \$05\$FF\$01 \$02\$88\$01 \$62 \$01 \$80 \$00)

(カッコ内はバイナリデータ)

### 3. 仮想レジスタ

仮想レジスタは SKSTACK-IP のパラメータを指定するための変数です。SKSREG コマンドで設定と読取が行えます。

#### 3.1 仮想レジスタ

レ ジ ス タ 番 号	内 容	属 性	初 期 値	値 域	保 存
S01	自端末の IEEE 64bit (MAC アドレス) このレジスタを設定するとプロトコル・スタックが一度、リセットされます。	R/W		0x0 - 0xFFFFFFFF FFFFFFFF FF	○
S02	自端末が使用する周波数の論理チャンネル番号	R/W	33	33 - 60	○
S03	自端末の PAN ID	R/W	0xFFFF	0x0 - 0xFFFF	○
S07	MAC 層セキュリティのフレームカウンタ 自端末のフレームカウンタを読み出します。	R	0	0-0xFFFF FFFF	×
S0A	Pairing ID  拡張ビーコン要求に設定する Pairing ID を設定します。ここで指定した Pairing ID と一致した端末が拡張ビーコンを応答します。 指定した値が 8 文字に足りない場合は残りをスペースで埋めます。 SKSETRBID コマンドで Route B ID を設定した場合は、その末尾 8 バイトが自動的に本レジスタの内容に変更されます。	R/W	CCDDEEFF	ASCII 8 文 字	×
S15	ビーコン応答の制御フラグ  0: ビーコンリクエストに応答しません。 1: ビーコンリクエストに応答します。  1 に設定するとコーディネータとして動作を開始すると共にビーコン要求への応答を開始します。0 にするとコーディネータとしての動作を解除し、RFD として動作します。	R/W	0	0 or 1	×
S16	PANA セッションライフタイム  PAA ではライフタイムが経過してもセッションが更新されない場合は、接続相手を切断します。  PaC ではライフタイムが近づくとき自動的に再認証を実行してセッションを更新します。	R/W	900 (秒)	60-0xFFFF FFFF	×
S17	自動再認証フラグ	R/W	1	0 or 1	×

	<p>PANA セッションのライフタイムが経過した際の再認証 (PaC) または切断 (PAA) 処理を抑制します。</p> <p>0: 再認証、切断を自動では実行しません。 1 (初期値): 再認証、切断を自動で実行します。</p>				
SA0	<p>MAC 層ブロードキャストに対するセキュリティ制御</p> <p>0: MAC 層ブロードキャスト (= すなわち IP マルチキャスト) 宛て IP パケットを暗号化しません 1: すべての IP マルチキャストを暗号化します</p> <p>PANA 認証を行い暗号通信が有効の場合、本レジスタは 1 (初期値) の必要があります。PANA 認証を行わず、非暗号通信でマルチキャストを送信したい場合は 0 を設定します。</p>	R/W	1	0 or 1	×
SA2	<p>送信出力</p> <p>無線送信出力の減衰量を調整します。 0x00: 減衰なし 0x1A: 減衰最大</p>	R/W	0	0x00 - 0x1A	○
SFB	<p>送信時間制限中フラグ</p> <p>送信総和時間の上限に達して送信制限中の場合に 1 になります</p>	R	0	0 or 1	×
SFD	<p>無線送信の積算時間 (単位ミリ秒)</p> <p>実際に無線区間に送出されたデータの積算時間をミリ秒で保持します。</p>	R	0	0x0 - 0xFFFFFFFF FFFFFFFF FF	×
SFE	<p>エコーバックフラグ</p> <p>0: コマンド入力のエコーバックをしない 1: エコーバックあり</p>	R/W	1	0 or 1	×
SFF	<p>オートロード</p> <p>SKSAVE コマンドで保存した内容を、電源投入時に自動的にロードして設定します。</p> <p>0: オートロード無効 1: オートロード有効</p>	R/W	0	0 or 1	○

R: Read Only , R/W: Read and Write enable

## 4. コマンドリファレンス

### ● SK コマンドフォーマット

1つのSKコマンドは改行(<CRLF>)で区切られた1行の文である必要があります。SKコマンドの引数はスペース' 'で区切って指定します。このリファレンスマニュアルでは、改行は<CRLF>、区切りのスペースは'+'記号で示してあります。

またコマンド引数の数値は以下の形式で指定する必要があります。

1. ON/OFFを表すフラグは、1または0で指定します。
2. 8, 16, 32ビットの整数は、それぞれ2桁, 4桁, 8桁の16進数で指定します
3. 指定した16進数が必要桁数に満たない場合は、上位を0で埋めて解釈します。(15を指定する場合、'0F'もしくは'F'と指定。10は、'000A'または'A'と指定)。
4. CHAR型はASCII文字で指定します。ASCII文字は制御文字を除いた0x20-0x7eまでの値を取ります。
5. IPv6アドレスは、コロン区切り(FE80:0000:0000:0000:1034:5678:ABCD:EF01)、コロン無し(FE800000000000000010345678ABCDEF01)どちらの形式でも受け付けます。

### ● イベントフォーマット

SKコマンドを実行した結果としてイベントが発生することがあります。イベントはアルファベットの'E'の後にイベント名が続き、SKコマンドと同様に改行までが1つの文となります。数値は16進数で表現され、パラメータがある場合はスペースで区切られます。



#### 4.1 SKSREG

仮想レジスタの内容を表示・設定します。

<SREG>に続けて<VAL>を指定すると値の設定、<VAL>を指定しないとそのレジスタの現在値を表示します。値の場合は ESREG イベントで通知されます。

Input		Response
SKSREG+ <SREG>+ <VAL><CRLF>	→	
	←	ESREG+<VAL><CRLF>
	←	OK<CRLF>
Input Parameters		
Name	Type	Description
<SREG>	SREG 番号	アルファベット 's' で始まるレジスタ番号を16進数で指定します。
<VAL>	可変	レジスタに設定する値 設定値域はレジスタ番号に依存します。
Response Parameters		
Name	Type	Description
<VAL>	可変	レジスタの現在値

## 4.2 SKINFO

現在の主要な通信設定値を表示します。

Input		Response
SKINFO <CRLF>	→	
	←	EINFO+ <IPADDR>+ <ADDR64>+ <CHANNEL>+ <PANID>+ <ADDR16><CRLF>
	←	OK<CRLF>

  

Input Parameters		
Name	Type	Description

  

Response Parameters		
Name	Type	Description
<IPADDR>	UINT8[16]	端末に設定されているリンクローカルアドレスを表示します
<ADDR64>	UINT8[8]	端末の IEEE 64bit MAC アドレスを表示します。
<PANID>	UINT16	現在の PAN ID を表示します。
<CHANNEL>	UINT8	現在使用している周波数の論理チャンネル番号を表示します。
<ADDR16>	UINT16	現在のショートアドレスを表示します。

### 4.3 SKSTART

端末を PAA (PANA 認証サーバ)として動作開始します。

動作開始に先立って PSK, PWD, Route-B ID 等のセキュリティ設定を済ませておく必要があります。本コマンドを発行すると自動的にコーディネータとして動作開始し S15 レジスタ値は 1 になります。またアクティブスキャンに対して自動的に応答するようになります。

本コマンド発行前に確立していた PANA セッションはクリアされます。

コマンド例：

Password = "0123456789AB", RouteB ID = "00112233445566778899AABBCCDDEEFF",  
PAN ID = 0x8888、29 チャンネルで PAA を起動する場合

**SKSREG S1 12345678abcdef01**

**SKSREG S2 29**

**SKSREG S3 8888**

**SKSETPWD C 0123456789AB**

**SKSETRBID 00112233445566778899AABBCCDDEEFF**

**SKSTART**

Input		Response
SKSTART <CRLF>	→	
	←	OK<CRLF>
Input Parameters		
Name	Type	Description
Response Parameters		
Name	Type	Description

#### 4.4 SKJOIN

指定した<IPADDR>に対して PaC（PANA 認証クライアント）として PANA 接続シーケンスを開始します。

SKJOIN 発行前に PSK, PWD, Route-B ID 等のセキュリティ設定を施しておく必要があります。

接続先は SKSTART コマンドで PAA として動作開始している必要があります。

接続の結果はイベントで通知されます。

PANA 接続シーケンスは PaC が PAA に対してのみ開始できます。

接続元（PaC）：

接続が完了すると、指定した<IPADDR>に対するセキュリティ設定が有効になり、以後の通信でデータが暗号化されます。

接続先（PAA）：

接続先はコーディネータとして動作開始している必要があります。

PSK から生成した暗号キーを自動的に配布します。相手からの接続が完了すると接続元に対するセキュリティ設定が有効になり、以後の通信でデータが暗号化されます。1つのデバイスとの接続が成立すると、他デバイスからの新規の接続を受け付けなくなります。

コマンド例：

Password = "0123456789AB", RouteB ID = "00112233445566778899AABBCCDDEEFF",  
PAN ID = 0x8888、29 チャンネルで 0x12345678abcdef01 の PAA へ接続する場合

SKSREG S1 12345678abcdef02

SKSREG S2 29

SKSREG S3 8888

SKSETPWD C 0123456789AB

SKSETRBID 00112233445566778899AABBCCDDEEFF

SKJOIN FE80:0000:0000:0000:1034:5678:ABCD:EF01

Input		Response
SKJOIN+ <IPADDR><CRLF>	→	
	←	OK<CRLF>
	←	

Input Parameters		
Name	Type	Description
<IPADDR>	UINT8[16]	接続先 IP アドレス
Response Parameters		
Name	Type	Description

#### 4.5 SKREJOIN

現在接続中の相手に対して再認証シーケンスを開始します。

再認証シーケンスの前に SKJOIN による接続が成功している必要があり、接続していないと ER10 になります。

再認証に成功すると、暗号キーと PANA セッション期限が更新されます。

PaC は、PAA が指定したセッションのライフタイムの 80%が経過した時点で、自動的に再認証シーケンスを実行します。このため SKREJOIN コマンドは基本的に発行する必要がありませんが、任意のタイミングで再認証したい場合には本コマンドを使います。

PAA は、セッションが更新されずにライフタイムが過ぎるとセッション終了要請を自動的に発行します。

Input		Response
SKREJOIN<CRLF>	→	
	←	OK<CRLF> FAIL ER10<CRLF>
	←	

  

Input Parameters		
Name	Type	Description

  

Response Parameters		
Name	Type	Description

#### 4.6 SKTERM

現在確立している PANA セッションの終了を要請します。

SKTERM は PAA、PaC どちらからでも実行できます。接続が確立していない状態でコマンドを発行すると ER10 になります。

セッションの終了に成功すると暗号通信は解除されます。

また PAA は他デバイスからの新しい接続を受け入れることができるようになります。

セッションの終了要請に対して相手から応答がなく EVENT 28 が発生した場合、セッションは終了扱いとなります。

Input		Response
SKTERM<CRLF>	→	
	←	OK<CRLF> FAIL ER10<CRLF>
	←	

  

Input Parameters		
Name	Type	Description

  

Response Parameters		
Name	Type	Description

#### 4.7 SKSENDTO

指定した宛先に UDP でデータを送信します。

SKSENDTO コマンドは以下の形式で正確に指定する必要があります。

- 1) アドレスは必ずコロン表記で指定してください。
- 2) ポート番号は必ず 4 文字指定してください。
- 3) データ長は必ず 4 文字指定してください。
- 4) セキュリティフラグは 1 文字で指定してください。
- 5) データは入力した内容がそのまま忠実にバイトデータとして扱われます。スペース、改行もそのままデータとして扱われます。
- 6) データは、データ長で指定したバイト数、必ず入力してください。サイズが足りないと、指定したバイト数揃うまでコマンド受け付け状態から抜けません。
- 7) データ部の入力のエコーバックされません。

正しい例：

SKSENDTO 1 2001:BEEF:0000:0000:0000:00FF:FE00:0003 0E1A 1 0005 01234

("01234"は画面にエコーバックされません)

ターミナルソフトで入力した場合、5 バイトで 0x30, 0x31, 0x32, 0x33, 0x34 が送信されます。  
受信側では、受信データの 16 進数 ASCII 表現で表示されます。

相手側に伝わる送信元ポート番号は、<HANDLE>で指定した UDP ハンドルの待受ポート番号となります。未使用のハンドルを指定すると ER10 になります。

Input		Response
SKSENDTO+ <HANDLE>+ <IPADDR>+ <PORT>+ <SEC> + <DATALEN>+ <DATA>	→	
	←	<CRLF>OK<CRLF>



Input Parameters		
Name	Type	Description
<HANDLE>	UINT8	送信元 UDP ハンドル
<IPADDR>	UINT8[16]	宛先 IPv6 アドレス
<PORT>	UINT16	宛先ポート番号
<SEC>	UINT8	<p>暗号化オプション 0: 必ず平文で送信</p> <p>1: SKSECENABLE コマンドで送信先がセキュリティ有効で登録されている場合、暗号化して送ります。登録されていない場合、または、暗号化無しで登録されている場合、データは送信されません。</p> <p>2: SKSECENABLE コマンドで送信先がセキュリティ有効で登録されている場合、暗号化して送ります。登録されていない場合、または、暗号化無しで登録されている場合、データは平文で送信されます。</p>
<DATALEN>	UINT16	送信データ長
<DATA>	CHAR[ ]	送信データ
Response Parameters		
Name	Type	Description

#### 4.8 SKCONNECT

指定した宛先に TCP の接続要求を発行します。

相手側は指定したポートで TCP の接続待ち受けを開始している必要があります。

接続処理の結果は ETCP イベントで通知されます。接続に成功した場合、ETCP イベントでコネクションに対応するハンドル番号が通知されます。以後、データ送信や切断処理はこのハンドル番号を指定します。

同じ<LPORT>と<RPORT>の組み合わせで E すでに何らかの宛先と接続が確立している場合、ER10 エラーとなります。このため<LPORT>は 0 以外のランダムな数値を指定することを推奨します。( <LPORT>は自端末の待受ポート番号である必要はありません)

接続処理の実行途中に本コマンドが発行されると ER10 エラーとなります。

Input		Response
SKCONNECT+ <IPADDR>+ <RPORT>+ <LPORT><CRLF>	→	
	←	OK<CRLF>

  

Input Parameters		
Name	Type	Description
<IPADDR>	UINT8[16]	接続先 IPv6 アドレス
<RPORT>	UINT16	接続先ポート番号 値域:1-65534
<LPORT>	UINT16	接続元ポート番号 値域:1-65534

  

Response Parameters		
Name	Type	Description

#### 4.9 SKSEND

指定したハンドル番号に対応する TCP コネクションを介して接続相手にデータを送信します。

送信処理の結果は ETCP イベントで通知されます。

すでにデータが送信中の場合、本コマンドを発行すると FAIL ER10 になります。

SKSEND は以下の形式で正確に指定する必要があります。

- 1) アドレスは必ずコロン表記で指定してください。
- 2) ポート番号は必ず 4 文字指定してください。
- 3) データ長は必ず 4 文字指定してください。
- 4) データは入力した内容がそのまま忠実にバイトデータとして扱われます。  
スペース、改行もそのままデータとして扱われます。
- 5) データは、データ長で指定したバイト数、必ず入力してください。サイズが足りないと、指定したバイト数揃うまでコマンド受け付け状態から抜けません。
- 6) データ部の入力のエコーバックされません。

正しい例：

SKSEND 1 0005 01234

(“01234”は画面にエコーバックされません)

ターミナルソフトで入力した場合、5 バイトで 0x30, 0x31, 0x32, 0x33, 0x34 が送信されます。

受信側では、受信データの 16 進数 ASCII 表現で表示されます。

Input		Response
SKSEND+ <HANDLE>+ <DATALEN>+ <DATA>	→	
	←	<CRLF>OK<CRLF>

Input Parameters		
Name	Type	Description
<HANDLE>	UINT8	ハンドル番号 SKCONNECT で接続を確立した際に受け取ったハンドル番号を指定します。
<DATALEN>	UINT16	送信データ長
<DATA>	CHAR[ ]	送信データ
Response Parameters		
Name	Type	Description

#### 4.10 SKCLOSE

指定したハンドルに対応する TCP コネクションの切断要求を発行します。

切断処理の結果は ETCP イベントで通知されます。

すでに切断初折が実行中の場合、本コマンドを発行すると FAIL ER10 になります。

Input		Response
SKCLOSE + <HANDLE><CRLF>	→	
	←	OK<CRLF>
Input Parameters		
Name	Type	Description
<HANDLE>	UINT8	ハンドル番号 SKCONNECT で接続を確立した際に受け取ったハンドル番号を指定します。
Response Parameters		
Name	Type	Description

#### 4.11 SKPING

指定した IPv6 宛てに ICMP Echo request を送信します。

Echo reply を受信すると EPONG イベントで通知されます。

送信先 IP がネイバーキャッシュにない場合、ICMP の送信は保留されアドレス要請が発行されます。その後アドレス解決に成功すると自動的に ICMP は再送されます。

Input		Response
SKPING + <IPADDR><CRLF>	→	
	←	OK<CRLF>
Input Parameters		
Name	Type	Description
<IPADDR>	UINT8[16]	Ping 送信先の IPv6 アドレス
Response Parameters		
Name	Type	Description

#### 4.12 SKSCAN

指定したチャンネルに対してアクティブスキャンまたは ED スキャンを実行します。

アクティブスキャンは、PAN を発見する度に EPANDESC イベントが発生して内容が通知されます。その後、指定したすべてのチャンネルのスキャンが完了すると EVENT イベントが 0x1E コードで発生して終了を通知します。

ED スキャンは、スキャンが完了した時点で EEDSCAN イベントが発生します。

MODE に 2 を指定すると、拡張ビーコン要求の Payload IE に Pairing Sub-ID が付与されます。Pairing 値(8 バイト)は S0A で設定します。

Pairing ID が付与された拡張ビーコン要求を受信したコーディネータは、同じ Pairing 値が設定されている場合に、拡張ビーコンを応答します。

MODE に 3 を指定すると、拡張ビーコン要求に Information Element を含めません。コーディネータは拡張ビーコンを応答します。

Input		Response
SKSCAN + <MODE>+ <CHANNEL_MASK>+ <DURATION><CRLF>	→	
	←	OK<CRLF>

  

Input Parameters		
Name	Type	Description
<MODE>	UINT8	0:ED スキャン 2:アクティブスキャン(IE あり) 3:アクティブスキャン(IE なし)
<CHANNEL_MASK>	UINT32	スキャンするチャンネルをビットマップフラグで指定します。 最下位ビットがチャンネル 33 に対応します。
<DURATION>	UINT8	各チャンネルのスキャン時間を指定します。 スキャン時間は以下の式で計算されます。 $0.01 \text{ sec} * (2^{\text{<DURATION>} + 1})$ 値域:0-14  Duration=6 以上を推奨します

  

Response Parameters		
Name	Type	Description

#### 4.13 SKREGDEV

セキュリティを適用するため、指定した IP アドレスを端末に登録します。  
登録数が上限の場合、FAIL ER10 が戻ります。

Input		Response
SKREGDEV+ <ADDR> <CRLF>	→	
	←	OK<CRLF>
Input Parameters		
Name	Type	Description
<IPADDR>	UINT8[16]	登録対象となる IPv6 アドレス
Response Parameters		
Name	Type	Description



#### 4.14 SKRMDEV

指定した IP アドレスのエントリーをネイバーテーブル、ネイバーキャッシュから強制的に削除します。

Input		Response
SKRMDEV+ <TARGET><CRLF>	→	
	←	OK<CRLF>
Input Parameters		
Name	Type	Description
<TARGET>	UINT8[16]	削除したいエントリーの IPv6 アドレス
Response Parameters		
Name	Type	Description

#### 4.15 SKSETKEY

指定されたキーインデックスに対する暗号キー(128bit)を、MAC 層セキュリティコンポーネントに登録します。

本コマンドでキーを設定後、SKSECENABLE コマンドで対象デバイスのセキュリティ設定を有効にすることで、以後、そのデバイスに対するユニキャストが MAC 層で暗号化されます。

指定したキーの桁が 16 バイト (ASCII 32 文字) より多い場合、ER06 になります。  
桁が 16 バイトより少ない場合、キーの内容が不定になり、OK または FAIL どちらになるか不定です。必ず 32 文字を指定してください。

暗号キーの登録容量を超えている場合、FAIL ER10 になります。指定したキーインデックスに既存の設定がある場合、新しい設定で上書き登録されます。

登録に成功するとカレントキーインデックスが指定した<INDEX>に切り替わります。

Input		Response
SKSETKEY+ <INDEX>+ <KEY><CRLF>	→	
	←	OK<CRLF>

  

Input Parameters		
Name	Type	Description
<INDEX>	UINT8	キーインデックス
<KEY>	UINT8[16]	128bit NWK 暗号キー

  

Response Parameters		
Name	Type	Description

#### 4.16 SKRMKEY

指定されたキーインデックスに対する暗号キー(128bit)を、MAC 層セキュリティコンポーネントから削除します。

指定したキーインデックスが登録されていない場合、FAIL ER10 になります。

Input		Response
SKRMKEY+ <INDEX><CRLF>	→	
	←	OK<CRLF>

  

Input Parameters		
Name	Type	Description
<INDEX>	UINT8	削除対象のキーインデックス

  

Response Parameters		
Name	Type	Description

#### 4.17 SKSECENABLE

指定した IP アドレスに対する MAC 層セキュリティの有効・無効を指定します。

指定する IPADDR は、事前に SKREGDEV コマンドで登録されている必要があります。登録されていない IP アドレスを指定すると FAIL ER10 になります。

<MODE> が 1 の場合、指定した <IPADDR> に対する <MACADDR> 情報が更新されます。  
<MODE>=1 で登録に成功した場合、この <MACADDR> に対応する MAC 層フレームカウンタが 0 で初期化されます。

<MODE> が 0 の場合、セキュリティの適用が無効になるだけで、<MACADDR> 情報は更新されません（値は無視されます）。

本コマンドによるセキュリティ設定は送信時に適用されるものです。受信時は、受信した MAC フレームの内容により必要な復号化が行われます。

Input		Response
SKSECENABLE+ <MODE>+ <IPADDR>+ <MACADDR><CRLF>	→	
	←	OK<CRLF>
Input Parameters		
Name	Type	Description
<MODE>	UINT16	0:セキュリティ無効 1:セキュリティ適用
<IPADDR>	UINT8[16]	セキュリティを適用する対象の IPv6 アドレス
<MACADDR>	UINT8[16]	対象 IPv6 アドレスに対応する 64bit アドレス
Response Parameters		
Name	Type	Description

#### 4.18 SKSETPSK

PANA 認証に用いる PSK を登録します。

すでに PSK が登録されている場合は新しい値で上書きされます。

<KEY>のバイト列は ASCII 2 文字で 1 バイトの HEX 表現で指定します。そのため<LEN>で指定する PSK 長の 2 倍の文字入力が必要です。

PSK を変更するには、SKRESET でリセットした後、再度、SKSETPSK コマンドを発行する必要があります。

\*) PSK は 16 バイトの必要があります。そのため LEN は 0x10 以外で FAIL ER06 になります。また<KEY>が 32 文字（16 バイト）に足りない場合は、不足分が不定値になります。

Input		Response
SKSETPSK+ <LEN>+ <KEY><CRLF>	→	
	←	OK<CRLF>
Input Parameters		
Name	Type	Description
<LEN>	UINT8	PSK のバイト長
<KEY>	UINT8[32]	PSK バイト列
Response Parameters		
Name	Type	Description

#### 4.19 SKSETPWD

PWD で指定したパスワードから PSK を生成して登録します。

SKSETPSK による設定よりも本コマンドが優先され、PSK は本コマンドの内容で上書きされます。

\* ) <PWD>の文字数が指定した<LEN>に足りない場合、不足分は不定値になります。

Input		Response
SKSETPWD+ <LEN>+ <PWD><CRLF>	→	
	←	OK<CRLF>
Input Parameters		
Name	Type	Description
<LEN>	UINT8	1-32
<PWD>	CHAR[ ]	ASCII 文字
Response Parameters		
Name	Type	Description

#### 4.20 SKSETRBID

指定された<ID>から各 Route-B ID を生成して設定します。

Pairing ID (SA レジスタ)として<ID>の下位 8 文字が設定されます。

\*) <ID>は ASCII 32 文字必要で、足りない場合、不足分が不定値になります。

Input		Response
SKSETRBID+ <ID> <CRLF>	→	
	←	OK<CRLF>
Input Parameters		
Name	Type	Description
<ID>	CHAR[]	32 桁の ASCII 文字
Response Parameters		
Name	Type	Description

#### 4.21 SKADDNBR

指定した IP アドレスと 64bit アドレス情報を、IP 層のネイバーキャッシュに Reachable 状態で登録します。これによってアドレス要請を省略して直接 IP パケットを出力することができます。

同じ IP アドレスがエントリーされている場合は設定が上書きされます。

ネイバーキャッシュがすでに一杯の場合は最も古いエントリーが削除され、ここで指定した IP アドレスが登録されます。

Input		Response
SKADDNBR+ <IPADDR>+ <MACADDR><CRLF>	→	
	←	OK<CRLF>
	←	
Input Parameters		
Name	Type	Description
<IPADDR>	UINT8[16]	登録する IPv6 アドレス
<MACADDR>	UINT8[8]	登録 IPv6 アドレスに対応する 64bit アドレス
Response Parameters		
Name	Type	Description



#### 4.22 SKUDPPORT

UDP の待ち受けポートを指定します。

設定したポートは、SKSAVE コマンドで保存した後、電源再投入時にオートロード機能でロードした場合に有効になります。

Input		Response
SKUDPPORT+ <HANDLE>+ <PORT><CRLF>	→	
	←	OK<CRLF>
	←	
Input Parameters		
Name	Type	Description
<HANDLE>	UINT8	対応する UDP ハンドル番号 (1-6)
<PORT>	UINT16	ハンドル番号に割り当てられる待ち受けポート番号 (0-0xFFFF) 0 を指定した場合、そのハンドルは未使用となりポートは 着信しません。また 0xFFFF は予約番号で着信しませ ん。
Response Parameters		
Name	Type	Description

#### 4.23 SKTCPPORT

TCP の待ち受けポートを指定します。

設定したポートは、SKSAVE コマンドで保存した後、電源再投入時にオートロード機能でロードした場合に有効になります。

Input		Response
SKTCPPORT+ <INDEX>+ <PORT><CRLF>	→	
	←	OK<CRLF>
	←	

  

Input Parameters		
Name	Type	Description
<INDEX>	UINT8	設定可能な4つのポートのどれを指定するかインデックス(1-4)
<PORT>	UINT16	設定する待ち受けポート番号 (0-0xFFFF) 0を指定した場合、そのハンドルは未使用となりポートは着信しません。また 0xFFFF は予約番号で着信しません。

  

Response Parameters		
Name	Type	Description

#### 4.24 SKSAVE

現在の仮想レジスタの内容を不揮発性メモリに保存します。

何らかの要因で保存に失敗した場合、FAIL ER10 エラーになります。

Input		Response
SKSAVE<CRLF>	→	
	←	OK<CRLF>
Input Parameters		
Name	Type	Description
Response Parameters		
Name	Type	Description

#### 4.25 SKLOAD

不揮発性メモリに保存されている仮想レジスタの内容をロードします。  
 何らかの要因でロードに失敗した場合、FAIL ER10 エラーになります。  
 内容が保存されていない状態でロードを実行すると L ER10 になります。

Input		Response
SKLOAD<CRLF>	→	
	←	OK<CRLF>

  

Input Parameters		
Name	Type	Description

  

Response Parameters		
Name	Type	Description

#### 4.26 SKERASE

レジスタ保存用の不揮発性メモリエリアを初期化して、未保存状態に戻します。  
本コマンドを実行後、SKLOAD コマンドを発行すると SKLOAD コマンドは ER10 エラーを返すようになります。

Input		Response
SKERASE<CRLF>	→	
	←	OK<CRLF>

  

Input Parameters		
Name	Type	Description

  

Response Parameters		
Name	Type	Description

#### 4.27 SKVER

SKSTACK IP のファームウェアバージョンを表示します。

EVER イベントが発生します。

Input		Response
SKVER<CRLF>	→	
	←	EVER + <VERSION><CRLF> OK<CRLF>
Input Parameters		
Name	Type	Description
Response Parameters		
Name	Type	Description
<VERSION>	CHAR[ ]	x.x.x 形式のバージョン番号が ASCII 文字で出力されます。

#### 4.28 SKRESET

プロトコル・スタックの内部状態を初期化します。

すべての内部変数が初期値に戻ります。

ただし 64bit アドレスだけは、S01 レジスタで設定した直近の値がそのまま再利用されます。

Input		Response
SKRESET<CRLF>	→	
	←	OK<CRLF>

##### Input Parameters

Name	Type	Description

##### Response Parameters

Name	Type	Description

#### 4.29 SKTABLE

SKSTACK IP 内の各種テーブル内容を画面表示します。

表示するテーブルに対応したイベントが発生します。

Input		Response
SKTABLE+	→	
<MODE><CRLF>	←	OK<CRLF>
Input Parameters		
Name	Type	Description
<MODE>	UINT8	1: 端末で利用可能な IP アドレス一覧 EADDR イベントが発生します。  2: ネイバーキャッシュ ENEIGHBOR イベントが発生します。  F: TCP ハンドル状態一覧 EHANDLE イベントが発生します。
Response Parameters		
Name	Type	Description



#### 4.30 SKLL64

64 ビット MAC アドレスを IPv6 リンクローカルアドレスに変換した結果を表示します。

Input		Response
SKLL64+ <ADDR64><CRLF>	→	
	←	<IPADDR><CRLF>
Input Parameters		
Name	Type	Description
<ADDR64>	UINT8[8]	64 ビット MAC アドレス
Response Parameters		
Name	Type	Description
<IPADDR>	UINT8[16]	IPv6 リンクローカルアドレスが出力されます。

## 5. イベント

### 5.1 ERXUDP

自端末宛での UDP（マルチキャスト含む）を受信すると通知されます。

```

ERXUDP +
<SENDER> +
<DEST> +
<RPORT> +
<LPORT> +
<SENDERLLA> +
<SECURED> +
<DATALEN> +
<DATA><CRLF>

```

パラメータ名	型	解説
<SENDER>	UINT8[16]	送信元 IPv6 アドレス
<DEST>	UINT8[16]	送信先 IPv6 アドレス
<RPORT>	UINT16	送信元ポート番号
<LPORT>	UINT16	送信先ポート番号
<SENDERLLA>	UINT8[8] または UINT16	送信元の MAC 層アドレス (64bit)
<SECURED>	UINT8	1: 受信した IP パケットを構成する MAC フレームが暗号化されていた場合 0: 受信した IP パケットを構成する MAC フレームが暗号化されていなかった場合
<DATALEN>	UINT16	受信したデータの長さ
<DATA>	CHAR[]	受信データ

### 5.2 ERXTCP

TCP でデータを受信すると通知されます。

```

ERXTCP +
<SENDER> +
<RPORT> +
<LPORT> +
<DATALEN> +
<DATA><CRLF>

```

パラメータ名	型	解説
<SENDER>	UINT8[16]	送信元 IPv6 アドレス
<RPORT>	UINT16	送信元ポート番号
<LPORT>	UINT16	送信先ポート番号
<DATALEN>	UINT16	受信したデータの長さ
<DATA>	CHAR[]	受信データ

### 5.3 EPONG

ICMP Echo reply を受信すると通知されます。		
EPONG + <SENDER><CRLF>		
パラメータ名	型	解説
<SENDER>	UINT8[16]	送信元 IPv6 アドレス

### 5.4 ETCP

TCP の接続、切断処理が発生すると通知されます。		
ETCP + <STATUS>+ <HANDLE> <CRLF>		
パラメータ名	型	解説
<STATUS>	UINT8	TCP 処理ステータス  1: 相手先との接続完了(成功)  3: 切断成功、または相手先から切断された(対応するハンドル番号が通知されます) 接続に失敗した(HANDLE=0 で通知されます)  4: 指定された接続元ポート番号がすでに使われている  5: データ送信完了(成功)  データ送信でタイムアウトが発生すると、ETCP 3 <HANDLE>で切断となり、そのハンドルは回収されます。
<HANDLE>	UINT8	イベント対象となった TCP ハンドル番号
<IPADDR>	UINT8[16]	STATUS = 1 の場合のみ 接続先、または接続元の IP アドレスが通知されます
<RPORT>	UINT16	STATUS = 1 の場合のみ 相手側の接続ポート番号が通知されます
<LPORT>	UINT16	STATUS = 1 の場合のみ 自端末の接続ポート番号が通知されます

### 5.5 EADDR

自端末で利用可能な IPv6 アドレス一覧を通知します。		
EADDR <CRLF> <IPADDR>+<CRLF> ... <IPADDR>+<CRLF>		
パラメータ名	型	解説
<IPADDR>	UINT8[16]	IPv6 アドレス(グローバル、リンクローカル両方を含む全

		て)

## 5.6 ENEIGHBOR

自端末のネイバーキャッシュ内の IPv6 エントリを一覧を通知します。

```
ENEIGHBOR<CRLF>
<IPADDR>+<LLA><CRLF>
...
<IPADDR>+<LLA><CRLF>
```

パラメータ名	型	解説
<IPADDR>	UINT8 [16]	ネイバーキャッシュに登録されている IPv6 アドレス(グローバル、リンクローカル両方を含む全て)
<LLA>	ADDR64	<IPADDR>に対応するリンク層 64bit アドレス

## 5.7 EPANDESC

アクティブスキャンを実行して発見した PAN を通知します。

以下に一例を示します。

```
EPANDESC <CRLF>
Channel:21 <CRLF>
Channel Page:09 <CRLF>
Pan ID:8888 <CRLF>
Addr:12345678ABCDEF01 <CRLF>
LQI:E1<CRLF>
```

パラメータ名	型	解説
Channel	UINT8	発見した PAN の周波数(論理チャンネル番号)
Channel Page	UINT8	発見した PAN のチャンネルページ
Pan ID	UINT16	発見した PAN の PAN ID
Addr	ADDR64	アクティブスキャン応答元のアドレス
LQI	UINT8	受信したビーコンの受信 RSSI (LQI - 107dBm)
PairID	CHAR[8]	(IE が含まれる場合) 相手から受信した Pairing ID

## 5.8 EEDSCAN

ED スキャンの実行結果を、RSSI 値で一覧表示します。

```
EEDSCAN<CRLF>
<CHANNEL> + <RSSI>...<CHANNEL> + <RSSI><CRLF>
```

パラメータ名	型	解説
<CHANNEL>	UINT8	測定した周波数の論理チャンネル番号
<RSSI>	UINT8	測定した RSSI 値 (RSSI - 107dBm)

## 5.9 EHANDLE

TCP ハンドルの現在の状態を一覧表示します。

未使用（開放状態）のハンドルは、すべての表示項目が 0 に設定されています。

EHANDLE<CRLF>

<HANDLE> + <IPADDR> + <RPORT>+ <LPORT><CRLF>

<HANDLE> + <IPADDR> + <RPORT>+ <LPORT><CRLF>

<HANDLE> + <IPADDR> + <RPORT>+ <LPORT><CRLF>

<HANDLE> + <IPADDR> + <RPORT>+ <LPORT><CRLF>

<HANDLE> + <IPADDR> + <RPORT>+ <LPORT><CRLF>

<HANDLE> + <IPADDR> + <RPORT>+ <LPORT><CRLF>

OK<CRLF>

パラメータ名	型	解説
<HANDLE>	UINT8	ハンドル番号 (1-6)
<IPADDR>	UINT8 [16]	この TCP ハンドルの接続先 IP アドレス(コロン表記)
<RPORT>	UINT16	この TCP ハンドルの接続先ポート番号
<LPORT>	UINT16	この TCP ハンドルの接続元ポート番号

## 5.10 EVENT

EVENT + <NUM>+ <SENDER> + <PARAM><CRLF>						
パラメータ名	型	解説				
<NUM>	UINT8	イベント番号 1:NSを受信した 2:NAを受信した 5:Echo Requestを受信した 0x1F:ED スキャンが完了した 0x20:Beaconを受信した 0x21:UDP 送信処理が完了した 0x22:アクティブスキャンが完了した  0x24:PANA による接続過程でエラーが発生した(接続が完了しなかった) 0x25:PANA による接続が完了した 0x26:接続相手からセッション終了要求を受信した 0x27: PANA セッションの終了に成功した 0x28: PANA セッションの終了要求に対する応答がなくタイムアウトした(セッションは終了) 0x29:セッションのライフタイムが経過して期限切れになった  0x32:ARIB108 の送信総和時間の制限が発動した(このイベント以後、あらゆるデータ送信要求が内部で自動的にキャンセルされます) 0x33:送信総和時間の制限が解除された				
<SENDER>	UINT8 [16]	イベントのトリガーとなったメッセージの発信元アドレス				
<PARAM>		イベント固有の引数  0x1F: 直後に EEDSCAN イベントが発生します  0x20: 直後に EPANDESC イベントが発生します  0x21: UINT8 <table><tr><td>0</td><td>UDP の送信に成功  データが無線区間に送出され、ユニキャストの場合、送信相手からAckを受信したことを表します</td></tr><tr><td>1</td><td>UDP の送信に失敗  UDP マルチキャストの場合、キャリアセンスでビジ</td></tr></table>	0	UDP の送信に成功  データが無線区間に送出され、ユニキャストの場合、送信相手からAckを受信したことを表します	1	UDP の送信に失敗  UDP マルチキャストの場合、キャリアセンスでビジ
0	UDP の送信に成功  データが無線区間に送出され、ユニキャストの場合、送信相手からAckを受信したことを表します					
1	UDP の送信に失敗  UDP マルチキャストの場合、キャリアセンスでビジ					

			<p>ーとなった、または送信時間制限で送信要求がキャンセルされたことを表します。 ユニキャストの場合、下記いずれかの要因で 1 になります。</p> <ul style="list-style-type: none"> <li>1) キャリアセンスでビジーになった</li> <li>2) 送信時間制限で送信要求がキャンセルされた</li> <li>3) 相手から Ack が得られなかった</li> </ul>
		2	<p>UDP を送信する代わりにアドレス要請 (Neighbor Solicitation) を行ったことを表します。 アドレス解決が成功すると、指定された UDP が自動的に再送信されます。</p>

## 6. ポート番号

### 6.1 UDP ポート

6 個の UDP ポートがアプリケーションから利用可能です。初期値は以下の通りです。

ハンドル	ポート番号
1	3610 (ECHONET Lite)
2	716 (PANA)
3	0
4	0
5	0
6	0

### 6.2 TCP ポート

4 個の TCP ポートが利用可能です。初期値は以下の通りです。

ポート番号
3610
0
0
0



## 7. TCP タイムアウト時間

TCP コマンドが通信障害などによって失敗した場合のタイムアウト時間とその結果は以下の通りです。

コマンド	秒数	イベント	結果
SKCONNECT	12 秒	ETCP 3 0	切断 (ハンドル開放)
SKCLOSE	20-28 秒	ETCP 3 <HANDLE>	切断 (ハンドル開放)
SKSEND	20-28 秒	ETCP 3 <HANDLE>	切断 (ハンドル開放)

## 8. 周波数とチャンネル番号

無線周波数と論理チャンネル番号の対応は以下のとおりです。

周波数 (MHz)	論理チャンネル番号
922.5	33(0x21)
922.7	34(0x22)
922.9	35(0x23)
923.1	36(0x24)
923.3	37(0x25)
923.5	38(0x26)
923.7	39(0x27)
923.9	40(0x28)
924.1	41(0x29)
924.3	42(0x2A)
924.5	43(0x2B)
924.7	44(0x2C)
924.9	45(0x2D)
925.1	46(0x2E)
925.3	47(0x2F)
925.5	48(0x30)
925.7	49(0x31)
925.9	50(0x32)
926.1	51(0x33)
926.3	52(0x34)
926.5	53(0x35)
926.7	54(0x36)
926.9	55(0x37)
927.1	56(0x38)
927.3	57(0x39)
927.5	58(0x3A)
927.7	59(0x3B)
927.9	60(0x3C)

## 9. エラーコード

ER01-ER03	reserved
ER04	指定されたコマンドがサポートされていない
ER05	指定されたコマンドの引数の数が正しくない
ER06	指定されたコマンドの引数形式や値域が正しくない
ER07-ER08	reserved
ER09	UART 入力エラーが発生した
ER10	指定されたコマンドは受付けたが、実行結果が失敗した

## 10. スタック仕様

### 10.1 準拠規格

Wi-SUN Alliance 規定「Wi-SUN-Echonet-Profile-2v01」またはそれ以降に準じます。

## 11. 無線仕様

項目名	設定値
変調方式	GFSK
ボーレート	100Kbps
周波数	922.5 ~ 927.9 MHz
帯域幅	400KHz (チャンネル 33~60)
出力レンジ	1mW 以上 20mW 以下
プリアンプル	15 バイト
プリアンプルパターン	010101...
SFD	0x7209
PSDU サイズ	最大 255 バイト
FCS	2 バイト
データホワイトニング	適用

### 11.1 ARIB T108 仕様

項目名	設定値
同時使用チャンネル	2 チャンネル
キャリアセンス	160 usec CSMA/CA 制御あり
送信時間制限	1回の送信 200msec 以下 2msec 以上休止
1 時間あたりの 送信時間総和	360 秒以下

## 12. MAC 仕様

### 12.1 IEEE 802.15.4

項目名	設定値
フレームフォーマット	IEEE 802.15.4e 準拠 (Frame Version = 0b10)
802.15.4e Amendment 対応	拡張ビーコン、拡張ビーコンリクエスト
動作モード	ノンビーコンモード
スーパーフレーム	未使用
Ack 制御機能	あり
MAC セキュリティ機能	あり
暗号キー最大登録数	8

### 13. 6LowPAN 仕様

6LowPAN に関する諸設定を以下に記します。

#### 13.1 6LowPAN

項目名	設定値
準拠 RFC	4944 (フラグメント) 6282 (ヘッダ圧縮)
分割を開始するペイロード長の閾値	220 バイト
フラグメント受信のタイムアウト	3 秒
非圧縮 IPv6 ヘッダ	対応 (初期では未使用)
隣接到達確認 (NUD) サポート	あり (初期値では未使用)
アドレス多重検出サポート	あり (初期値では未使用)

## 14. IP 仕様

IP/TCP/UDP に関する諸設定を以下に記します。

### 14.1 IP

項目名	設定値
MTU	1280 バイト
ネイバーキャッシュサイズ	8
IP フラグメントサポート	可能（オプションにより組み込み可能）
生成アドレス方式	LL64

### 14.2 TCP

項目名	設定値
最大コネクション数	6
待ち受けポート数	4

### 14.3 UDP

項目名	設定値
待ち受けポート数 (=最大 UDP ハンドル数)	6

## 15. 注意事項

### 15.1 変更

本コマンド仕様は予告なく変更される可能性があります。