

BP35A1
コマンドリファレンスマニュアル
(Single-hop Edition)

Version 1.3.0

注意事項

1. 本仕様書に記載されている内容は本仕様書発行時点のものであり、予告なく変更することがあります。
2. 本仕様書に記載されている情報は、正確を期すために慎重に作成したのですが、誤りがないことを保障するものではありません。万一、本仕様書に記載されている情報の誤りに起因する損害がお客様に生じた場合におきましても、当社は一切その責任を負いません。
3. 本仕様書に記載された技術情報の使用に関連し発生した第三者の特許権、著作権その他の知的財産権の侵害等に関し、当社は一切その責任を負いません。当社は本仕様書に基づき当社または第三者の特許権、著作権その他の知的財産権を何ら許諾するものではありません。
4. 本使用の全部または一部を当社の事前承諾を得ずに転載または複製することはご遠慮ください

改版履歴

VER.	改訂内容 (対応ファーム Ver)	改訂日付	改訂者
1.3.0	新規作成	2014/12/25	ローム

1. 概要

本ドキュメントは BP35A1 で使用されているコマンドの使い方を記述した文書です。

1.1 SK コマンド

BP35A1 で使用されている SKSTACK-IP 用 SK コマンドになります。

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 プロダクト設定コマンド

プロダクト設定コマンドでは UART ポートなどを設定できます。

コマンドは ASCII 文字で指定し、コマンド引数の区切りにはスペースを使います。

2. 目次

注意事項	2
改版履歴	3
1. 概要	4
1.1 SK コマンド	4
1.2 プロダクト設定コマンド	4
2. 目次	5
3. コマンド一覧	8
4. コマンドリファレンス	10
4.1 SKSREG	11
4.1.1 仮想レジスタ	12
4.2 SKINFO	14
4.3 SKSTART	15
4.4 SKJOIN	16
4.5 SKREJOIN	18
4.6 SKTERM	19
4.7 SKSENDTO	20
4.8 SKCONNECT	22
4.9 SKSEND	23
4.10 SKCLOSE	25
4.11 SKPING	26
4.12 SKSCAN	27
4.13 SKREGDEV	28
4.14 SKRMDEV	29
4.15 SKSETKEY	30
4.16 SKRMKEY	31
4.17 SKSECENABLE	32
4.18 SKSETPSK	33
4.19 SKSETPWD	34
4.20 SKSETRBID	35
4.21 SKADDNBR	36
4.22 SKUDPPORT	37
4.23 SKTCPPORT	38
4.24 SKSAVE	39

4.25	SKLOAD	40
4.26	SKERASE.....	41
4.27	SKVER	42
4.28	SKAPPVER	42
4.29	SKRESET	43
4.30	SKTABLE.....	44
4.31	SKDSLEEP	45
4.32	SKRFLO	46
4.33	SKLL64	47
4.34	WOPT (プロダクト設定コマンド)	48
4.35	ROPT (プロダクト設定コマンド)	49
4.36	WUART (プロダクト設定コマンド).....	50
4.37	RUART (プロダクト設定コマンド).....	52
5.	イベント	53
5.1	ERXUDP	53
5.2	ERXTCP	53
5.3	EPONG.....	54
5.4	ETCP.....	54
5.5	EADDR	55
5.6	ENEIGHBOR.....	55
5.7	EPANDESC.....	56
5.8	EEDSCAN	56
5.9	EPORT.....	57
5.10	EHANDLE.....	57
5.11	EVENT	58
6.	待ち受けポート番号	60
6.1	UDP ポート	60
6.2	TCP ポート.....	60
7.	TCP タイムアウト時間	61
8.	周波数とチャンネル番号	62
9.	エラーコード.....	63
10.	コマンドチュートリアル	64
10.1	UDP 通信.....	64
10.1.1	コーディネータの起動	65
10.1.2	デバイスの起動	66
10.2	TCP 通信	67

10.2.1	コーディネータの起動	68
10.2.2	デバイスの起動	69
10.3	Wi-SUN B ルートを想定した通信	71
10.3.1	Wi-SUN コーディネータ (PAA) の起動 (スマートメータ側)	72
10.3.2	Wi-SUN デバイスの起動	73
11.	注意事項	74
11.1	変更について	74
11.2	ファームウェアについて	74
11.2.1	ファームウェア使用許諾	74
11.2.2	ファームウェアバージョンについて	74
11.2.3	ファームウェアバージョンの確認方法	74
12.	コピーライト	75

3. コマンド一覧

● SK コマンド

No.	コマンド	内容
1	SKSREG	仮想レジスタの内容を表示・設定します
2	SKINFO	現在の主要な通信設定値を表示します
3	SKSTART	端末を PAA (PANA 認証サーバ) として動作開始します
4	SKJOIN	指定した接続先 IP アドレスに対して 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
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。
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
7	SKSENDTO	指定した宛先に UDP でデータを送信します
8	SKCONNECT	指定した宛先に TCP の接続要求を発行します
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
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
11	SKPING	指定した IPv6 宛てに ICMP Echo request を送信します
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
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
14	SKRMDEV	指定した IP アドレスのエントリ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
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
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
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
18	SKSETPSK	PANA 認証に用いる PSK を登録します
19	SKSETPWD	指定したパスワードから PSK を生成して登録します
20	SKSETRBID	指定された ID から各 Route-B ID を生成して設定します

No.	コマンド	内容
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
22	SKUDPPORT	UDP の待ち受けポートを指定します
23	SKTCPPORT	TCP の待ち受けポートを指定します
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
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
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
27	SKVER	SKSTACK IP のファームウェアバージョンを表示します
28	SKAPPVER	アプリケーションのファームウェアバージョンを表示します
29	SKRESET	プロトコル・スタックの内部状態を初期化します
30	SKTABLE	SKSTACK IP 内の各種テーブル内容を画面表示します
31	SKDSLEEP	スリープモードに移行します
32	SKRFLO	受信時のローカル周波数を Lower Local か Upper Local に設定します
33	SKLL64	MAC アドレス(64bit)から IPv6 リンクローカルアドレスへ変換した結果を表示します

● プロダクト設定コマンド

No.	コマンド	内容
34	WOPT	ERXUDP、ERXTCP のデータ部の表示形式を設定します
35	ROPT	WOPT コマンドの設定状態を表示します
36	WUART	UART 設定 (ボーレート、キャラクター間インターバル、フロー制御) を設定します。
37	RUART	WUART コマンドの設定状態を表示します

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 (FE80:0000:0000:0000:021D:1290:1234:5678) で入力します。

● 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。

● プロダクト設定コマンドフォーマット

1つのコマンドは改行 (<CR>) で区切られた1行の文である必要があります。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<CR>、区切りのスペースは'+ '記号で示してあります。

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。

コマンド例：

PAN ID = 0x8888 を設定する場合

```
SKSREG S3 8888
```

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進数で指定されます。
<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

4.1.1 仮想レジスタ

仮想レジスタは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。

レジスタ番号	内容	属性	初期値	値域	保存
S02	自端末が使用する周波数の論理チャンネル番号	R/W	0x21	0x21 – 0x3C	○
S03	自端末の PAN ID	R/W	0xFFFF	0x0000 – 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	0x00000000	0x00000000–0xFFFFFFFF	×
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	0x00000384 (900 秒)	0x0000003C–0xFFFFFFFF	×
S17	自動再認証フラグ 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。 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。	R/W	1	0 or 1	×

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	×
SA1	<p>ICMP メッセージ処理制御</p> <p>平文の ICMP Echo Request, Reply を受信した際の処理を指定します。</p> <p>0:受信を破棄します 1(初期値):受け入れ処理します</p> <p>PANA 認証完了後に本レジスタを 0 にして平文の ICMP Echo Request を受信しない設定に切り替えることで、暗号化された ping のみで相手との疎通が確認できます。</p>	R/W	1	0 or 1	×
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	×
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

4.2 SKINFO

現在の主要な通信設定値を表示します。

コマンド例 :

IPv6 アドレス= FE80:0000:0000:0000:021D:1290:1234:5678

MAC アドレス=001D129012345678

ch=0x21 (33ch)

PAN ID = 0x8888

で設定の場合

SKINFO

Response

EINFO FE80:0000:0000:0000:021D:1290:1234:5678 001D129012345678 21 8888 FFFE

OK

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。
<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。
<PANID>	UINT16	現在の PAN ID を表示します。
<ADDR16>	UINT16	FFFE が表示されます。

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

で PAA を起動する場合

```
SKSETPWD C 0123456789AB
SKSETRBID 00112233445566778899AABBCCDDEEFF
SKSREG S3 8888
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

で IP アドレス FE80:0000:0000:0000:021D:1290:1234:5678 の PAA へ接続する場合

```
SKSETPWD C 0123456789AB
SKSETRBID 00112233445566778899AABBCCDDEEFF
SKSREG S3 8888
SKJOIN FE80:0000:0000:0000:021D:1290:1234:5678
```

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ます、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) データ部の入力はエコーバックされません。

コマンド例 :

```
SKSENDTO 1 FE80:0000:0000:0000:021D:1290:1234:5678 0E1A 0 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。

WOPT コマンドで初期設定 (バイナリ表示設定) では、データは 16 進数 ASCII 表現である必要はありません。受信側では、入力した内容がそのまま忠実に出力されます。

SK STACK のオリジナル仕様設定 (WOPT コマンドで 16 進 ASCII 設定) では、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	暗号化オプション 0: 必ず平文で送信 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。 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。
<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>の組み合わせです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。

コマンド例 :

接続先 IPv6 アドレス= FE80:0000:0000:0000:021D:1290:1234:5678 の

ポート番号:3610(0x0E1A) (ECHONET Lite 用)に接続要求する場合

```
SKCONNECT FE80:0000:0000:0000:021D:1290:1234:5678 0E1A 0E1A
```

接続に成功するとコーディネータとデバイスの両端末で以下の様にイベントが表示され、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。

Response

```
OK
```

```
ETCP 01 01 FE80:0000:0000:0000:021D:1290:1234:5678 0E1A 0E1A
```

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) データ部の入力はエコーバックされません。

コマンド例 :

```
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。

WOPT コマンドで初期設定 (バイナリ表示設定) では、データは 16 進数 ASCII 表現である必要はありません。受信側では、入力した内容がそのまま忠実に出力されます。

SK STACK のオリジナル仕様設定 (WOPT コマンドで 16 進 ASCII 設定) では、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。

コマンド例：

ハンドル番号 1 (デフォルトはポート番号 : 3610) の TCP コネクションの切断要求をする場合

SKCLOSE 1

Response

OK

切断が成功した場合、OK の後に以下のイベントが発生します。数十秒かかります。

ETCP 03 01

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。

コマンド例 :

IPv6 アドレス= FE80:0000:0000:0000:021D:1290:1234:5678 宛に

ICMP Echo request を送信する場合

```
SKPING FE80:0000:0000:0000:021D:1290:1234:5678
```

Response

```
OK
```

Echo reply を受信した場合

```
EPONG FE80:0000:0000:0000:021D:1290:1234:5678
```

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 コードが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

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
SKPSECENABLE+ <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。

コマンド例：

ハンドル番号 3 (デフォルトはポート未設定) にポート番号 80 (0x0050) を設定する場合

```
SKUDPPORT 3 0050
```

Response

```
OK
```

※本設定は不揮発性メモリに保存できます。

方法としては、オートロード設定 (SFF レジスタ) を有効にし、SKSAVE コマンドで不揮発メモリに保存することで、電源再投入後に本ポート設定が不揮発メモリからオートロードされます。

```
SKSREG SFF 1
```

```
SKSAVE
```

ポート設定状態については、SKTABLE E コマンドで確認できます。

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。

コマンド例：

ハンドル番号 2 (デフォルトはポート未設定) にポート番号 80 (0x0050) を設定する場合

```
SKTCPPORT 2 0050
```

Response

```
OK
```

※本設定は不揮発性メモリに保存できます。

方法としては、オートロード設定 (SFF レジスタ) を有効にし、SKSAVE コマンドで不揮発メモリに保存することで、電源再投入後に本ポート設定が不揮発メモリからオートロードされます。

```
SKSREG SFF 1
```

```
SKSAVE
```

ポート設定状態については、SKTABLE E コマンドで確認できます。

Input		Response
SKUDPPORT+ <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 of 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 SKAPPVER

アプリケーションのファームウェアバージョンを表示します。

EAPPVER イベントが発生します。

Input		Response
SKAPPVER<CRLF>	→	
	←	EAPPVER + <VERSION><CRLF> OK<CRLF>
Input Parameters		
Name	Type	Description
Response Parameters		
Name	Type	Description
<VERSION>	CHAR[]	バージョン番号が ASCII 文字で出力されます。

4.29 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。

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

Input Parameters

Name	Type	Description

Response Parameters

Name	Type	Description

4.30 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。

コマンド例 :

SKTABLE 1

Response

EADDR

FE80:0000:0000:0000:021D:1290:1234:5678

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。 E:待ち受けポート設定状態一覧 EPORT 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

4.31 SKDSLEEP

スリープモードに移行します。

スリープモードから通常モード (受信モード) へは、5 番端子(WKUP 端子)を”L”にすることで復帰します。WKUP 端子は通常は”H”にしてください。

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

Input Parameters

Name	Type	Description

Response Parameters

Name	Type	Description

4.32 SKRFLO

受信時のローカル周波数を Lower Local か Upper Local に設定します。

ただし、IF 周波数は、720kHz になります。(データレート 100kbps)

Input		Response
SKRFLO+ <MODE><CRLF>	→	
	←	OK<CRLF>
Input Parameters		
Name	Type	Description
<MODE>	UNIT8	00:Lower Local モード(デフォルト) 01:Upper Local モード
Response Parameters		
Name	Type	Description

4.33 SKLL64

MAC アドレス(64bit)から IPv6 リンクローカルアドレスへ変換した結果を表示します。

コマンド例 :

SKLL64 001D129012345678

Response

FE80:0000:0000:0000:021D:1290:1234:5678

Input		Response
SKLL64 + <ADDR64><CRLF>	→	
	←	<IPADDR><CRLF>

Input Parameters

Name	Type	Description
<ADDR64>	UINT8[8]	端末の IEEE 64bit MAC アドレス

Response Parameters

Name	Type	Description
<IPADDR>	UINT8[16]	入力した MAC アドレスから変換したリンクローカルアドレスを表示します。

4.34 WOPT (プロダクト設定コマンド)

ERXUDP、ERXTCP のデータ部の表示形式を設定します。

コマンド例：

「16 進 ASCII 文字 (SK STACK オリジナル)」で設定する場合

WOPT 01

※本コマンドは、実行する度に設定が内部 FLASH メモリに書き込み保存され、電源を再起動しても設定は保存されています。FLASH メモリへの書き込み回数には制限 (10,000 回以下) がありますので、制限回数には注意し、設定時に一度だけ本コマンドを実行するようにしてください。また、デフォルト設定以外の動作につきましては、お客様の検証にてご判断ください。

Input		Response
WOPT+ <MODE><CR>	→	
	←	OK<CR>

Input Parameters

Name	Type	Description									
<MODE>	UNIT8	<table border="1"> <thead> <tr> <th>Bit</th> <th>内容</th> <th>値 (太字デフォルト)</th> </tr> </thead> <tbody> <tr> <td>bit0</td> <td>ERXUDP、 ERXTCP の表示</td> <td>0=バイナリ表示, 1=16進 ASCII 表示</td> </tr> <tr> <td>Bit1-7</td> <td>予約</td> <td>-</td> </tr> </tbody> </table>	Bit	内容	値 (太字デフォルト)	bit0	ERXUDP、 ERXTCP の表示	0 =バイナリ表示, 1=16進 ASCII 表示	Bit1-7	予約	-
Bit	内容	値 (太字デフォルト)									
bit0	ERXUDP、 ERXTCP の表示	0 =バイナリ表示, 1=16進 ASCII 表示									
Bit1-7	予約	-									

Response Parameters

Name	Type	Description

4.35 ROPT (プロダクト設定コマンド)

WOPT コマンドの設定状態を表示します。

コマンド例 :

ROPT

Response (デフォルト設定時)

OK 00

Input		Response
ROPT<CR>	→	
	←	OK+<MODE><CR>

Input Parameters

Name	Type	Description

Response Parameters

Name	Type	Description
<MODE>	UINT8	WOPT での設定値

4.36 WUART (プロダクト設定コマンド)

UART 設定 (ボーレート、キャラクター間インターバル、フロー制御) を設定します。

ボーレート設定は、再起動後に反映されます。

キャラクター間インターバルとフロー制御設定は、即時反映されます。

コマンド例 :

「ボーレート 9600bps、フロー制御有効」で設定する場合

WUART 83

※本コマンドは、実行する度に設定が内部 FLASH メモリに書き込み保存され、電源を再起動しても設定は保存されています。FLASH メモリへの書き込み回数には制限 (10,000 回以下) がありますので、制限回数には注意し、設定時に一度だけ本コマンドを実行するようにしてください。また、デフォルト設定以外の動作につきましては、お客様の検証にてご判断ください。

Input		Response
WUART+ <MODE><CR>	→	
	←	OK<CR>

Input Parameters																	
Name	Type	Description															
<MODE>	UNIT8	<table border="1"> <thead> <tr> <th>Bit</th> <th>内容</th> <th>値 (太字デフォルト)</th> </tr> </thead> <tbody> <tr> <td>bit0-2</td> <td>ボーレート</td> <td>0=115200, 1=2400, 2=4800, 3=9600, 4=19200, 5=38400, 6=57600 (bps)</td> </tr> <tr> <td>bit3</td> <td>予約</td> <td>-</td> </tr> <tr> <td>bit4-6</td> <td>キャラクター 間インター バル</td> <td>0=なし, 1=100, 2=200, 3=300, 4=400, 5=50 (usec)</td> </tr> <tr> <td>bit7</td> <td>フロー制御</td> <td>0=無効, 1=有効</td> </tr> </tbody> </table>	Bit	内容	値 (太字デフォルト)	bit0-2	ボーレート	0=115200 , 1=2400, 2=4800, 3=9600, 4=19200, 5=38400, 6=57600 (bps)	bit3	予約	-	bit4-6	キャラクター 間インター バル	0=なし , 1=100, 2=200, 3=300, 4=400, 5=50 (usec)	bit7	フロー制御	0=無効 , 1=有効
		Bit	内容	値 (太字デフォルト)													
		bit0-2	ボーレート	0=115200 , 1=2400, 2=4800, 3=9600, 4=19200, 5=38400, 6=57600 (bps)													
		bit3	予約	-													
		bit4-6	キャラクター 間インター バル	0=なし , 1=100, 2=200, 3=300, 4=400, 5=50 (usec)													
bit7	フロー制御	0=無効 , 1=有効															
Response Parameters																	
Name	Type	Description															

4.37 RUART (プロダクト設定コマンド)

WUART コマンドの設定状態を表示します。

コマンド例 :

RUART

Response (デフォルト設定時)

OK 00

Input		Response
RUART<CR>	→	
	←	OK+<MODE><CR>

Input Parameters

Name	Type	Description

Response Parameters

Name	Type	Description
<MODE>	UINT8	WUART での設定値

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>
  
```

Name	Type	Description
<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。

```

ERXDATA +
<SENDER> +
<RPORT> +
<LPORT> +
<DATALEN> +
<DATA><CRLF>
  
```

Name	Type	Description
<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>		
Name	Type	Description
<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>		
Name	Type	Description
<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せん。
<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>		
Name	Type	Description
<IPADDR>	UINT8[16]	IPv6 アドレス(リンクローカル)

5.6 ENEIGHBOR

自端末のネイバーキャッシュ内の IPv6 エントリ一覧を通知します。		
ENEIGHBOR<CRLF> <IPADDR>+<ADDR64>+<ADDR16><CRLF> ... <IPADDR>+<ADDR64>+<ADDR16><CRLF>		
Name	Type	Description
<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(リンクローカル)
<ADDR64>	UINT8[8]	<IPADDR>に対応するリンク層 64bit アドレス
<ADDR16>	UNIT16	FFFF が表示します。

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:001D129012345678 <CRLF>
LQI:E1 <CRLF>
PairID <CRLF>
```

Name	Type	Description
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 ED 値(RSSI)
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>
```

Name	Type	Description
<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 ED 値(RSSI)

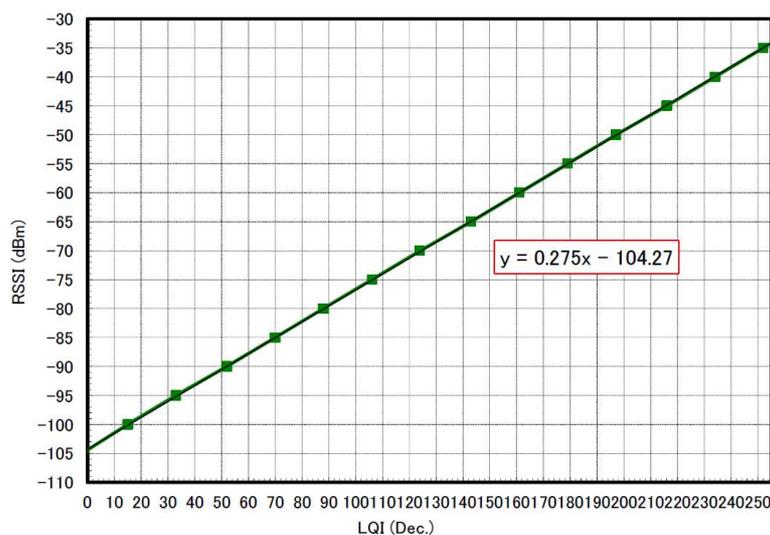


図 1. LQI(ED 値) vs RSSI

5.9 EPORT

UDP または TCP の待ち受けポート設定状態を一覧表示します。
未設定のポートは、すべての表示項目が 0 に設定されています。

```
EPORT<CRLF>
<PORT_UDP><CRLF>
<PORT_UDP><CRLF>
<PORT_UDP><CRLF>
<PORT_UDP><CRLF>
<PORT_UDP><CRLF>
<PORT_UDP><CRLF>
<PORT_UDP><CRLF>
<CRLF>
<PORT_TCP><CRLF>
<PORT_TCP><CRLF>
<PORT_TCP><CRLF>
<PORT_TCP><CRLF>
OK<CRLF>
```

ハンドル 1~6 の順に UDP ポート番号が表示されます

インデックス 1~4 の順に TDP ポート番号が表示され

Name	Type	Description
<PORT_UDP>	UINT16	UDP 待ち受けポート番号設定値
<PORT_TCP>	UINT16	TCP 待ち受けポート番号設定値

5.10 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>
OK<CRLF>
```

Name	Type	Description
<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

5.11 EVENT

EVENT + <NUM>+ <SENDER> + <PARAM><CRLF>						
Name	Type	Description				
<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 イベント: 直後に EEDSCAN イベントが発生します 0x20 イベント: 直後に EPANDESC イベントが発生します 0x21 イベント: 型: UINT8 <table border="1" data-bbox="603 1659 1369 1977"> <tbody> <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。</td> </tr> </tbody> </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。
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。					

		<p>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> <ol style="list-style-type: none"> 1) キャリアセンスでビジーになった 2) 送信時間制限で送信要求がキャンセルされた 3) 相手から Ack が得られなかった <p>2 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. 待ち受けポート番号

6.1 UDP ポート

6 個の UDP ポートが利用可能です。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

周波数と論理チャンネル番号、S02 レジスタ設定値の対応は以下の通りです。

周波数 (2 単位チャンネル) (MHz)	論理チャンネル番号 (ch)	S02 レジスタ設定値
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け付けたが、実行結果が失敗した

10. コマンドチュートリアル

10.1 UDP 通信

BP35A1 では、コーディネータとデバイスのどちらでも使用することができます。UDP 通信を行う為のコマンドシーケンスとしては以下の概略図の様になります。

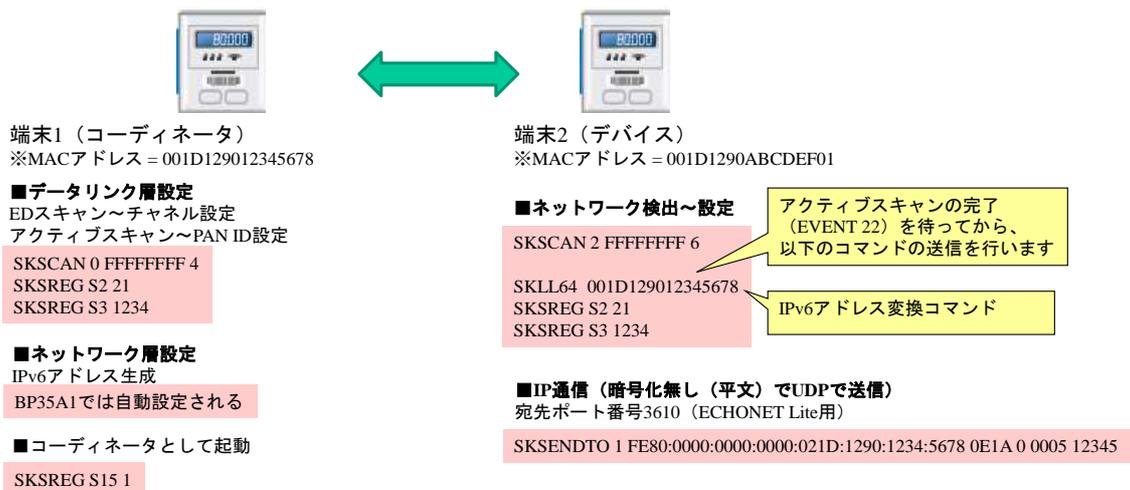


図 2. UDP 通信 コマンドシーケンス概略図

10.1.1 コーディネータの起動

まず初めに以下の手順でコーディネータ側を起動します。

■データリンク層設定

コーディネータ側のチャンネル設定について、ED スキャンしてチャンネルの空き具合で判断してください。PAN ID も必要であればアクティブスキャンして周囲の別のコーディネータを発見した後、重複しない PAN ID を選択してください。0xFFFF 以外の値を設定してください。

ED スキャン

SKSCAN 0 FFFFFFFF 4

チャンネル設定 (例: ※33ch (0x21) (922.5MHz) に設定)

SKSREG S2 21

アクティブスキャン

SKSCAN 2 FFFFFFFF 6

PAN ID 設定 (例: ※1234 に設定)

SKSREG S3 1234

■ネットワーク層設定

IPv6 アドレス生成については、BP35A1 内で自動設定されます。

■コーディネータ起動

コーディネータとして動作開始

SKSREG S15 1

10.1.2 デバイスの起動

次に以下の手順でデバイス側を起動します。

■ネットワーク検出～設定

アクティブスキャンで発見した PAN 情報(=接続先のコーディネータ)からチャンネルと PAN ID を取得して、それを S2 と S3 で設定します。

アクティブスキャン

```
SKSCAN 2 FFFFFFFF 6
```

※アクティブスキャンの完了(EVENT 22)を待ってから、以下のコマンド送信を行ってください。

IPv6 アドレス変換(例:取得したコーディネータ MAC アドレスが 001D129012345678 の場合)

```
SKLL64 001D129012345678
```

結果より、FE80:0000:0000:0000:021D:1290:1234:5678 を取得します。

チャンネル設定 (例:※33ch(0x21)(922.5MHz)に設定)

```
SKSREG S2 21
```

PAN ID 設定 (例:※1234 に設定)

```
SKSREG S3 1234
```

■IP 通信(暗号化無し(平文)UDP)

コーディネータ(FE80:0000:0000:0000:021D:1290:1234:5678)に対して暗号化無し(平文)で UDP でデータを送信します。宛先ポート番号:3610(0x0E1A)(ECHONET Lite 用)

```
SKSENDOTO 1 FE80:0000:0000:0000:021D:1290:1234:5678 0E1A 0 0005 12345
```

10.2 TCP 通信

BP35A1 で TCP 通信を行う為のコマンドシーケンスとしては以下の概略図の様になります。

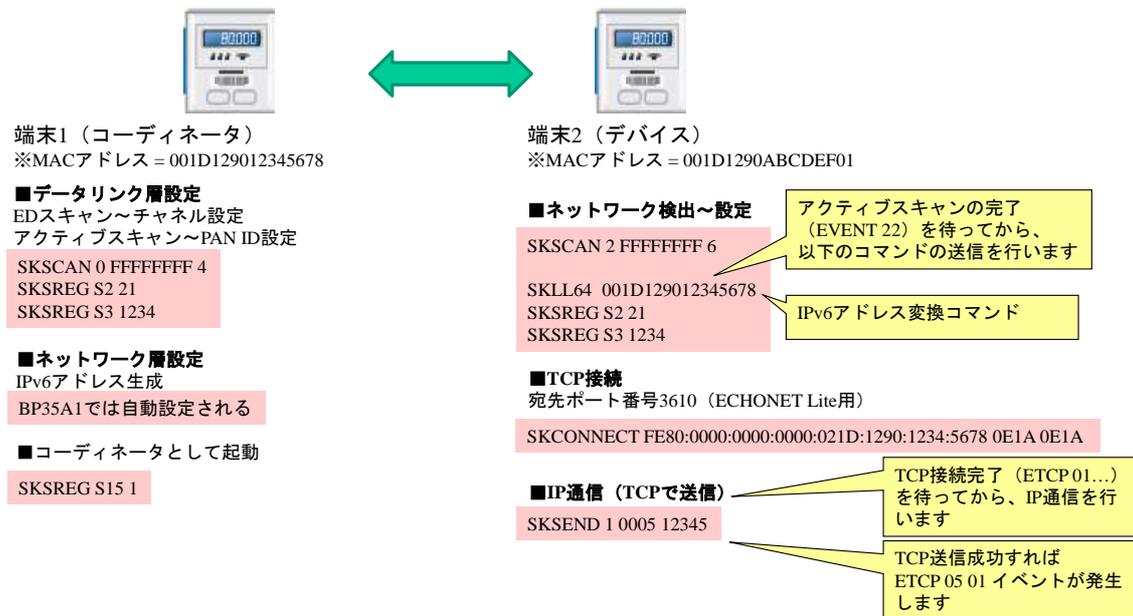


図 3. TCP 通信 コマンドシーケンス概略図

10.2.1 コーディネータの起動

まず初めに以下の手順でコーディネータ側を起動します。

■データリンク層設定

コーディネータ側のチャンネル設定について、ED スキャンしてチャンネルの空き具合で判断してください。PAN ID も必要であればアクティブスキャンして周囲の別のコーディネータを発見した後、重複しない PAN ID を選択してください。0xFFFF 以外の値を設定してください。

ED スキャン

SKSCAN 0 FFFFFFFF 4

チャンネル設定 (例: ※33ch (0x21) (922.5MHz) に設定)

SKSREG S2 21

アクティブスキャン

SKSCAN 2 FFFFFFFF 6

PAN ID 設定 (例: ※1234 に設定)

SKSREG S3 1234

■ネットワーク層設定

IPv6 アドレス生成については、BP35A1 内で自動設定されます。

■コーディネータ起動

コーディネータとして動作開始

SKSREG S15 1

10.2.2 デバイスの起動

次に以下の手順でデバイス側を起動します。

■ネットワーク検出～設定

アクティブスキャンで発見した PAN 情報(=接続先のコーディネータ)からチャンネルと PAN ID を取得して、それを S2 と S3 で設定します。

アクティブスキャン

```
SKSCAN 2 FFFFFFFF 6
```

※アクティブスキャンの完了(EVENT 22)を待ってから、以下のコマンド送信を行ってください。

IPv6 アドレス変換(例:取得したコーディネータ MAC アドレスが 001D129012345678 の場合)

```
SKLL64 001D129012345678
```

結果より、FE80:0000:0000:0000:021D:1290:1234:5678 を取得します。

チャンネル設定 (例:※33ch(0x21) (922.5MHz)に設定)

```
SKSREG S2 21
```

PAN ID 設定 (例:※1234 に設定)

```
SKSREG S3 1234
```

■TCP 接続

TCP 接続の確立を行います。例として、コーディネータ(FE80:0000:0000:0000:021D:1290:1234:5678)のポート番号:3610(0x0E1A) (ECHONET Lite 用)に接続要求を出します。

```
SKCONNECT FE80:0000:0000:0000:021D:1290:1234:5678 0E1A 0E1A
```

接続に成功するとコーディネータとデバイスの両端末で以下の様にイベントが表示され、接続のハンドル番号が 1 であることを示します。

端末 1(コーディネータ)

```
ETCP 01 01 FE80:0000:0000:0000:021D:1290:ABCD:EF01 0E1A 0E1A
```

端末 2(デバイス)

```
ETCP 01 01 FE80:0000:0000:0000:021D:1290:1234:5678 0E1A 0E1A
```

■IP 通信(TCP)

コーディネータ(FE80:0000:0000:0000:021D:1290:1234:5678)に対して TCP でデータ送信します。

```
SKSEND 1 0005 12345
```

TCP 送信に成功すると以下のイベントが発生します。

```
ETCP 05 01
```

TCP コネクションは双方向ですので、端末 1 側で同様に「SKSEND 1 0005 12345」コマンドを発行すると、端末 2 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。

10.3 Wi-SUN B ルートを想定した通信

BP35A1 では、Wi-SUN コーディネータと Wi-SUN デバイスのどちらでも使用することができます。コマンドシーケンスとしては以下の概略図の様になります。

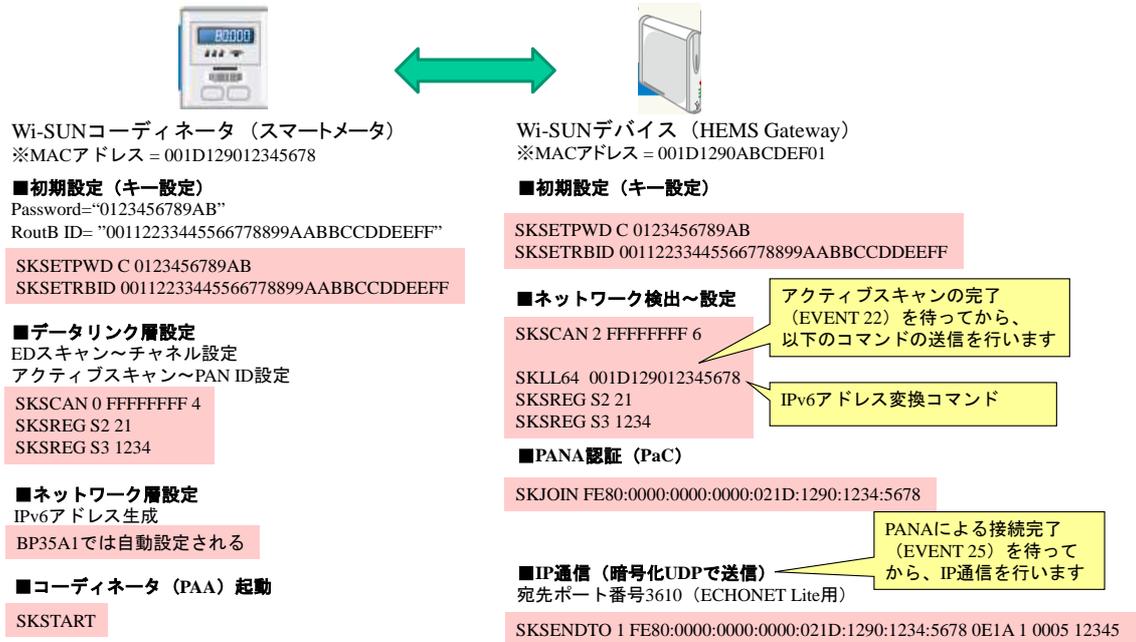


図 4. Wi-SUN B ルート コマンドシーケンス概略図

10.3.1 Wi-SUN コーディネータ (PAA) の起動 (スマートメータ側)

先ず初めに以下の手順でコーディネータ側を起動します。

■初期設定(キー設定)

例: ※Password = "0123456789AB",

※Rout-B ID = "00112233445566778899AABBCCDDEEFF"

```
SKSETPWD C 0123456789AB
SKSETRBID 00112233445566778899AABBCCDDEEFF
```

■データリンク層設定

コーディネータ側のチャンネル設定について、ED スキャンしてチャンネルの空き具合で判断してください。PAN ID も必要であればアクティブスキャンして周囲の別のコーディネータを発見した後、重複しない PAN ID を選択してください。0xFFFF 以外の値を設定してください。

ED スキャン

```
SKSCAN 0 FFFFFFFF 4
```

チャンネル設定 (例: ※33ch(0x21) (922.5MHz) に設定)

```
SKSREG S2 21
```

アクティブスキャン

```
SKSCAN 2 FFFFFFFF 6
```

PAN ID 設定 (例: ※1234 に設定)

```
SKSREG S3 1234
```

■ネットワーク層設定

IPv6 アドレス生成については、BP35A1 内で自動設定されます。

■コーディネータ(PAA)起動

PANA 認証サーバー(PAA)として動作開始

※自動的にコーディネータ設定(仮想レジスタ S15=1)されます。

```
SKSTART
```

10.3.2 Wi-SUN デバイスの起動

次に以下の手順で Wi-SUN デバイス側を起動します。

■初期設定(キー設定)

例: ※Password = "0123456789AB",

※Rout-B ID = "00112233445566778899AABBCCDDEEFF"

```
SKSETPWD C 0123456789AB
SKSETRBID 00112233445566778899AABBCCDDEEFF
```

■ネットワーク検出～設定

アクティブスキャンで発見した PAN 情報(=接続先のコーディネータ)からチャンネルと PAN ID を取得して、それを S2 と S3 で設定します。

アクティブスキャン

```
SKSCAN 2 FFFFFFFF 6
```

※アクティブスキャンの完了(EVENT 22)を待ってから、以下のコマンド送信を行ってください。

IPv6 アドレス変換(例: 取得したコーディネータ MAC アドレスが 001D129012345678 の場合)

```
SKLL64 001D129012345678
```

結果より、FE80:0000:0000:0000:021D:1290:1234:5678 を取得します。

チャンネル設定 (例: ※33ch(0x21) (922.5MHz)に設定)

```
SKSREG S2 21
```

PAN ID 設定 (例: ※1234 に設定)

```
SKSREG S3 1234
```

■PANA 認証(PaC)

発見したコーディネータ(FE80:0000:0000:0000:021D:1290:1234:5678)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 FE80:0000:0000:0000:021D:1290:1234:5678
```

※PANA による接続完了(EVENT 25)を確認し、次の IP 通信を行います。

■IP 通信(暗号化 UDP)

コーディネータ(FE80:0000:0000:0000:021D:1290:1234:5678)に対して暗号化して UDP でデータを送信します。宛先ポート番号: 3610(0x0E1A) (ECHONET Lite 用)

```
SKSENDOTO 1 FE80:0000:0000:0000:021D:1290:1234:5678 0E1A 1 0005 12345
```

11. 注意事項

11.1 変更について

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。

11.2 ファームウェアについて

11.2.1 ファームウェア使用許諾

本製品に内蔵されていますファームウェアにつきましては以下の使用許諾にご承諾の上ご使用下さい。

1. 本ソフトウェアは BP35A1 専用のファームウェアです。BP35A1 以外には使用しないで下さい。
2. 本ソフトウェアの著作権（著作権法第 27 条及び第 28 条の権利を含む）及びその他一切の知的財産権はローム株式会社が有します。本ソフトウェアは BP35A1 への使用に限り許諾するものとします。
3. 本ソフトウェアを第三者に譲渡、再使用許諾、貸与等を行わないで下さい
4. 本ソフトウェアのリバースエンジニアリング、逆コンパイル、逆アセンブリ、複製、変更等を禁じます。
5. ローム株式会社は本ソフトウェアを使用した全ての動作を保障するものではありません。本ソフトウェア使用によって、お客様に生じるいかなる直接的・間接的損害に関して、一切の責任を負いません。お客様にて十分ご評価の上、ご使用いただけますようお願い申し上げます。

11.2.2 ファームウェアバージョンについて

1. 本製品に書き込まれますファームウェアのバージョンは製造時点での最新のものとなります。
2. 出荷のタイミングによっては、最新のファームウェアとならない場合がございます。
3. ファームウェアのバージョン変更は予告なく変更いたします。
4. 書き込まれているファームウェアのバージョンは本製品の外観で判別する事はできません。
5. 同一梱包(BP35A1 納入仕様書『19.梱包仕様』に示す梱包単位：最大 100pcs)内には同一のファームウェアが書き込まれます。
6. ファームウェアの書き換え方法は、別途お問い合わせください。

11.2.3 ファームウェアバージョンの確認方法

起動後、以下のコマンドにて確認できます。

- ・「SKVER」コマンドにて、スタックバージョン
- ・「SKAPPVER」コマンドにて、アプリケーションバージョン

12. コピーライト

/*

- * Copyright (c) 2004-2010 Swedish Institute of Computer Science.
- * All rights reserved.
- *
- * Redistribution and use in source and binary forms, with or without
- * modification, are permitted provided that the following conditions
- * are met:
- * 1. Redistributions of source code must retain the above copyright
- * notice, this list of conditions and the following disclaimer.
- * 2. Redistributions in binary form must reproduce the above copyright
- * notice, this list of conditions and the following disclaimer in the
- * documentation and/or other materials provided with the distribution.
- * 3. Neither the name of the Institute nor the names of its contributors
- * may be used to endorse or promote products derived from this software
- * without specific prior written permission.
- *
- * THIS SOFTWARE IS PROVIDED BY THE INSTITUTE AND CONTRIBUTORS ``AS IS" AND
- * ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
- * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
- * ARE DISCLAIMED. IN NO EVENT SHALL THE INSTITUTE OR CONTRIBUTORS BE LIABLE
- * FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
- * DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
- * OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
- * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
- * LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
- * OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
- * SUCH DAMAGE.

*/

/*

- * Copyright (c) 2001-2003, Adam Dunkels.
- * All rights reserved.
- *

- * Redistribution and use in source and binary forms, with or without
- * modification, are permitted provided that the following conditions
- * are met:
 - * 1. Redistributions of source code must retain the above copyright
 - * notice, this list of conditions and the following disclaimer.
 - * 2. Redistributions in binary form must reproduce the above copyright
 - * notice, this list of conditions and the following disclaimer in the
 - * documentation and/or other materials provided with the distribution.
 - * 3. The name of the author may not be used to endorse or promote
 - * products derived from this software without specific prior
 - * written permission.
 - *
- * THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS" AND ANY EXPRESS
- * OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED
- * WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
- * ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY
- * DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
- * DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE
- * GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS
- * INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY,
- * WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING
- * NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS
- * SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
- */

- /*
- * Copyright (C) 1995, 1996, 1997, and 1998 WIDE Project.
- * All rights reserved.
- *
- * Redistribution and use in source and binary forms, with or without
- * modification, are permitted provided that the following conditions
- * are met:
 - * 1. Redistributions of source code must retain the above copyright
 - * notice, this list of conditions and the following disclaimer.
 - * 2. Redistributions in binary form must reproduce the above copyright
 - * notice, this list of conditions and the following disclaimer in the

- * documentation and/or other materials provided with the distribution.
- * 3. Neither the name of the project nor the names of its contributors
 - * may be used to endorse or promote products derived from this software
 - * without specific prior written permission.
- *
* THIS SOFTWARE IS PROVIDED BY THE PROJECT AND CONTRIBUTORS ``AS IS" AND
* ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
* ARE DISCLAIMED. IN NO EVENT SHALL THE PROJECT OR CONTRIBUTORS BE LIABLE
* FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
* DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
* OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
* OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
* SUCH DAMAGE.
*/

/*
* HMAC-SHA-224/256/384/512 implementation
* Last update: 06/15/2005
* Issue date: 06/15/2005
*
* Copyright (C) 2005 Olivier Gay <olivier.gay@a3.epfl.ch>
* All rights reserved.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
* 1. Redistributions of source code must retain the above copyright
* notice, this list of conditions and the following disclaimer.
* 2. Redistributions in binary form must reproduce the above copyright
* notice, this list of conditions and the following disclaimer in the
* documentation and/or other materials provided with the distribution.
* 3. Neither the name of the project nor the names of its contributors
* may be used to endorse or promote products derived from this software

- * without specific prior written permission.
- *
- * THIS SOFTWARE IS PROVIDED BY THE PROJECT AND CONTRIBUTORS ``AS IS" AND
- * ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
- * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
- * ARE DISCLAIMED. IN NO EVENT SHALL THE PROJECT OR CONTRIBUTORS BE LIABLE
- * FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
- * DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
- * OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
- * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
- * LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
- * OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
- * SUCH DAMAGE.
- */

- /*
- * FIPS 180-2 SHA-224/256/384/512 implementation
- * Last update: 02/02/2007
- * Issue date: 04/30/2005
- *
- * Copyright (C) 2013, Con Kolivas <kernel@kolivas.org>
- * Copyright (C) 2005, 2007 Olivier Gay <olivier.gay@a3.epfl.ch>
- * All rights reserved.
- *
- * Redistribution and use in source and binary forms, with or without
- * modification, are permitted provided that the following conditions
- * are met:
- * 1. Redistributions of source code must retain the above copyright
- * notice, this list of conditions and the following disclaimer.
- * 2. Redistributions in binary form must reproduce the above copyright
- * notice, this list of conditions and the following disclaimer in the
- * documentation and/or other materials provided with the distribution.
- * 3. Neither the name of the project nor the names of its contributors
- * may be used to endorse or promote products derived from this software
- * without specific prior written permission.
- *

* THIS SOFTWARE IS PROVIDED BY THE PROJECT AND CONTRIBUTORS ``AS IS" AND
* ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
* ARE DISCLAIMED. IN NO EVENT SHALL THE PROJECT OR CONTRIBUTORS BE LIABLE
* FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
* DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
* OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
* OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
* SUCH DAMAGE.
*/

Copyright(C) 2011-2014 Skyley Networks, Inc. All Rights Reserved.