TTC技術レポート
Technical Report

TR-1052

HEMS-スマートメーター（Bルート）通信インタフェース実装詳細ガイドライン

Detailed implementation guideline for communication interface between HEMS and Smart meter (Route-B)

第1.0版

2014年3月17日制定

一般社団法人

情報通信技術委員会

THE TELECOMMUNICATION TECHNOLOGY COMMITEE

Telecommunication Technology Committee

目　次

＜参考＞

１．　国際勧告等との関連

本技術レポートに関する国際勧告は本文中に記載している。

２．改版の履歴

版数	制定日	改版内容
第1.0版	2014年3月17日	制定

３．参照文章

各章で共通に参照されるドキュメントは次の通りである。

[802.15.4-2006] IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 15.4: Wireless Medium Access (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs)

[AH] IP Authentication Header, IETF RFC 4302

[JJ-300.10v2] TTC標準 JJ-300.10v2, ECHONET Lite向けホームネットワーク通信インタフェース（IEEE802.15.4/4e/4g 920MHz帯無線）第２版

[JJ-300.11v2] TTC標準 JJ-300.11v2, ECHONET Lite向けホームネットワーク通信インタフェース（ITU-T G.9903 狭帯域 OFDM PLC）

[EAP] Extensible Authentication Protocol (EAP), IETF RFC 3748

[EAP-PSK] The EAP-PSK Protocol: A Pre-Shared Key Extensible Authentication Protocol (EAP) Method, IETF RFC 4764

[EL] The Echonet Lite Specification Version 1.01/Version 1.10

[ESP] IP Encapsulating Security Payload (ESP), IETF RFC 4303

[G3-PLC] Narrowband orthogonal frequency division multiplexing power line communication transceivers for G3-PLC networks, ITU-T G.9903 (2013)

[GL] JSCAスマートハウス・ビル標準・事業促進検討会 HEMSースマートメーター（Bルート）運用ガイドライン第1版

[NAI] The Network Access Identifier, IETF RFC 4282

[SHIF] ECHONET CONSORTIUM スマート電力量メータ・HEMSコントローラ間アプリケーション通信インタフェース仕様書 Ver1.00

[ICMP6] Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification, IETF RFC 4443

[IPv6] Internet Protocol, Version 6 (IPv6) Specification, IETF RFC 2460

[ND] Neighbor Discovery for IP version 6 (IPv6), IETF RFC 4861

[PANA] Protocol for Carrying Authentication for Network Access (PANA), IETF RFC 5191

[SLAAC] IPv6 Stateless Address Autoconfiguration, IETF RFC 4862

[TLS-PSK] Pre-Shared Key Ciphersuites for Transport Layer Security (TLS), IETF RFC 4279

４．技術レポート作成部門

第１．０版　：　次世代ホームネットワークシステム専門委員会

５．本技術レポート「HEMS-スマートメーター（Bルート）通信インタフェース実装ガイドライン」の制作体制

本ガイドラインは、TTC次世代ホームネットワークシステム専門委員会(委員長：山崎毅文[NTT])での審議を経てTTC技術レポートとしてとして公開するものである。

はじめに

本ガイドラインは、スマートメーター・HEMS（コントローラ）間の通信、いわゆるBルートについてECHONET LiteによるBルートアプリケーションのための下位レイヤ通信インタフェースの実装ガイドラインである。本ガイドラインでは通信メディアとして920MHz帯無線（[JJ-300.10v2] 方式A:Wi-SUN、方式B:ZigBee）及び、PLC（[JJ-300.11v2] G3-PLC）を用いた場合について説明する。

なお、該当する下位レイヤプロトコルもしくは通信メディアの追加や更新がある場合には、適宜、本ガイドラインの改定を行う。追加・更新の提案については、TTC次世代ホームネットワークシステム専門委員会　事務局へご連絡をいただきたい。

第1章　共通仕様

本ガイドラインでは、図 1-1に示すようにスマートメーターとHEMSは１：１で接続される構成とし、スマートメーターがHEMSを認証した後に接続させるために、両者の間の通信は[JJ-300.10v2]もしくは[JJ-300.11v2][G3-PLC]で定められた認証・鍵交換、及びMAC層による暗号化によって保護される。

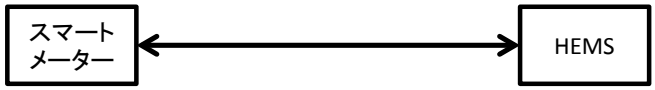

図 1-1 1:1 接続

1.1 ID および認証鍵

Bルートの下位レイヤ通信において必要となるID・パスワードは[GL]に記載されているBルート認証ID・パスワードに基づき、表 1-1のように定める。これらID・パスワードを、後述する各通信メディアでの使用に適した形に変換し使用すること。

ID・パスワードはスマートメーター及びHEMSが本通信インタフェース仕様に基づく通信を行う前に各機器に設定されているものとし、スマートメーターとHEMSへの配布・設定方法は本章のスコープ外である。

表 1-1 B ルートで使用する ID および認証鍵

名称	説明
Bルート認証ID	特定のスマートメーターとHEMSを結びつけるために使用されるユニークなID。0～9、A～FのASCII文字で構成される32桁の文字列（32オクテット長）とする。本ガイドラインでは後述するルールにより、[JJ-300.10v]方式A及び[JJ-300.11v2]では[EAP]で使用するIDやネットワーク識別子（920MHz帯無線）に変換され、[JJ-300.10v2]方式Bでは[TLS-PSK]で使用するPSK IdentityやZIP NetworkIDに変換して利用する。
（Bルート認証用）パスワード	Bルート認証IDに結びつけられたパスワード（0～9、a～z、A～ZのASCII文字で構成される12桁の文字列）。本ガイドラインでは後述するルールにより、[JJ-300.10v]方式A及び[JJ-300.11v2]では[EAP-PSK]で用いるPSKを生成するために使用され、[JJ-300.10v2]方式Bでは[TLS-PSK]で用いるPSKを生成するために使用される。

1.2 アプリケーション

アプリケーション層として、ECHONET Lite[EL]に基づく「スマート電力量メータ・HEMSコントローラ間アプリケーション通信インタフェース仕様書」[SHIF]を使用する。本書記載の仕様に基づくノードは、[EL]に規定される必須機能を全てサポートしなければならない。

尚、[EL]で規定されるノード立ち上げ処理を実施するタイミングは、[JJ-300.10v2]方式Aの場合、PANAのAuthentication and Authorization Phase後とし、[JJ-300.11v2]の場合、スマートメーターがHEMSに対してLBP　ACCEPTED送信後とし、[JJ-300.10v2]方式Bの場合、ブートストラップシーケンス後とする。

1.2.1 アプリケーションレベルにおける要求頻度

他のシステムとの共有周波数であることを考慮して、アプリケーションレベルでの要求頻度は節度あるものとすべきである。

スマートメーターは、一般的にDoS攻撃とみなされない範囲において、受信頻度に制限を設けず、ベストエフォートで応答することを基本とするが、DoS攻撃とみなした場合、一定時間（10分間程度）、当該HEMSからの要求には無応答となる場合がある。

1.2.2 再接続処理

通信が正常に行われなくなったと判断した場合（例えば、[SHIF]3.2章に記載されるスマートメーターからの定期動作が受信出来なくなった場合）、HEMS側は再度接続処理を行っても良い。[JJ-300.10v2]方式A、Bの場合、スマートメーター側は該当PANAセッションをクローズする。[JJ-300.11v2]の場合、スマートメーター側は該当LBPセッションをクローズする。

スマートメーター及びHEMSは、前回使用時の無線チャネル(920MHz無線の場合)、PAN IDを記憶しておき、再接続処理にあたっては優先的に接続を試行することを推奨する。

第2章　　920MHz（JJ-300.10 方式A：Wi-SUN）用Bルート下位レイヤ実装

2.1 概要

本章では[JJ-300.10v2]の5.9に記載される方式Aに基づくシングルホップスマートメーター・HEMS間推奨通信仕様を用いて実装する場合について補足を行う。

920MHz帯無線のIEEE802.15.4g/e上でIPv6を動作させるために6LoWPANを使用し、UDPにより認証プロトコルとしてPANA、アプリケーションプロトコルとしてECHONET Liteを動作させる（図 2-1）。

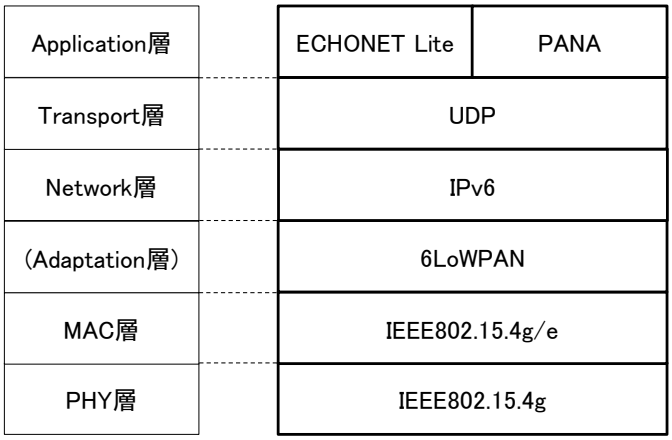

図 2-1 方式 A スタック図

図 2-2に接続シーケンスの概要を示す。

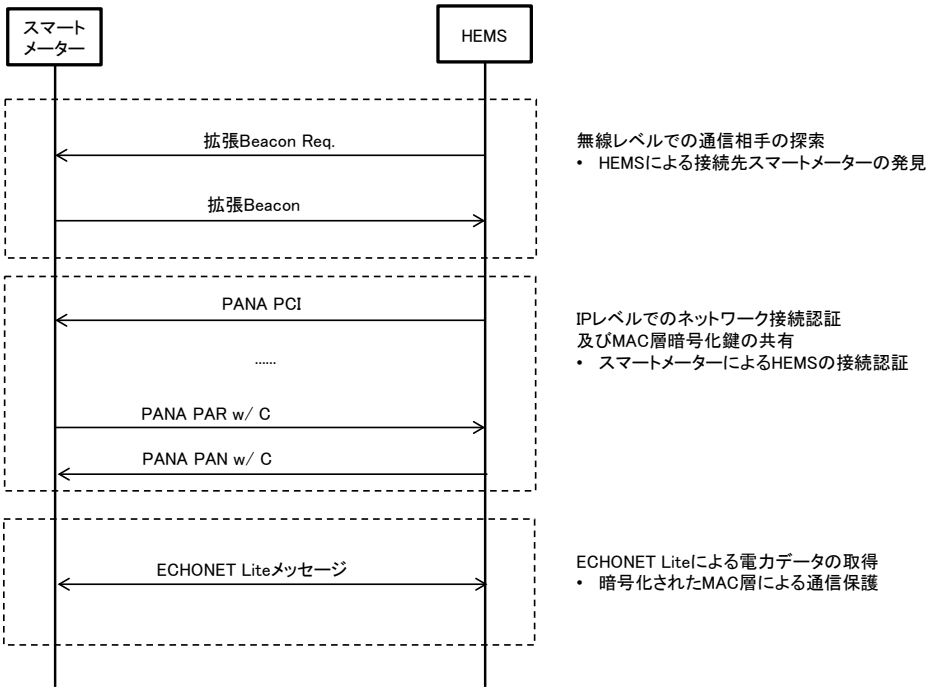

図 2-2 接続シーケンス概要

2.2 物理層

[JJ-300.10v2]の5.9.2に従う。

2.3 MAC 層

[JJ-300.10v2]の5.9.3に従う。

2.4 LoWPAN アダプテーション層

[JJ-300.10v2]の5.9.4.2に従う。

2.5 ネットワーク層

IPv6については、表 2-1に従い、ICMPv6については、表 2-2に従うこと。それ以外のネットワーク層の項目については[JJ-300.10v2]の5.9.4.3に従う。

表 2-1 ネットワーク層:IPv6

Item number	Item description	Reference section in standard	Support (Y:Yes, N:No, O:Option)
IP1	Header Format	[IPv6] 3	Y
IP1.1	Extension Headers	-	O
IP1.2	Extension Header Order	[IPv6]4.1	O
IP1.3	Options	[IPv6] 4.2	O
IP1.4	Hop-by-Hop Options Header	[IPv6] 4.3	O
IP1.5	Routing Header	[IPv6]4.4	O
IP1.6	Fragment Header	[IPv6] 4.5	O
IP1.7	Destination Options Header	[IPv6] 4.6	O
IP1.8	No Next Header	[IPv6]4.7	Y
IP1.9	AH Header	[AH]	O
IP1.10	ESP Header	[ESP]	O
IP2	Deprecation of Type 0 Routing Headers	[IPv6-RH]	O*1
IP3	Path MTU Discovery	[IPv6] 5	O
IP4	Flow Labels	[IPv6] 6	Y
IP5	Traffic Classes	[IPv6] 7	Y

*1: IP1.5をサポートする場合、IP2もサポートすること。

表 2-2 ネットワーク層:ICMPv6

Item number	Item description	Reference section in standard	Support (Y:Yes, N:No, O:Option)
ICMP1	Message Format	[ICMP6] 2.1	Y
ICMP2	Message Source Address Determination	[ICMP6] 2.2	Y
ICMP3	Message Checksum Calculation	[ICMP6] 2.3	Y
ICMP4	Message Processing Rules	[ICMP6] 2.4	Y
ICMP5	Destination Unreachable Message	[ICMP6] 3.1	Y*1
ICMP6	Packet Too Big Message	[ICMP6] 3.2	O
ICMP7	Time Exceeded Message	[ICMP6] 3.3	O
ICMP8	Parameter Problem Message	[ICMP6] 3.4	Y
ICMP9	Echo Request Message	[ICMP6] 4.1	Y
ICMP10	Echo Reply Message	[ICMP6] 4.2	Y

*1: port unreachable (code=4)のみ適用する。

2.5.1 IP アドレッシング

[JJ-300.10v2]の5.9.4.3.1に従う。

2.5.2 近隣探索

近隣要請メッセージと近隣応答メッセージ以外については、[JJ-300.10v2]の5.9.4.3.2に従う。近隣要請メッセージの送信はオプショナルであるが近隣要請メッセージを受信したノードは近隣応答メッセージで応答すること（**表 2-3**）。

表 2-3 近隣要請メッセージと近隣応答メッセージ

Item number	Item description	Support (Y:Yes, N:No, O:Option)	Notes
ND8	Neighbor Solicitation (NS) Message	-	ND8.1,ND8.2, ND8.3を参照
ND8.1	NS Transmission	O	どちらか一方を選択すること.
ND8.2	No NS Transmission	O	
ND8.3	NS Reception	Y	
ND9	Neighbor Advertisement (NA) Message	-	ND9.1, ND9.2, ND9.3, ND9.4を参照
ND9.1	Solicited NA Transmission	Y	
ND9.2	Solicited NA Reception	ND8.1:Y ND8.2:N	
ND9.3	Unsolicited NA Transmission	N	
ND9.4	Unsolicited NA Reception	N	

2.5.3 マルチキャスト

[JJ-300.10v2]の5.9.4.3.3に従う。

2.6 トランスポート層

[JJ-300.10v2]の5.9.4.4に従う。

2.7 セキュリティ処理

[JJ-300.10v2]の5.9.5および5.9.7に従う。
実装するにあたり、MAC層の鍵の切り替えタイミングによる差異を吸収するため、最低新旧２つの鍵を保持できるようにすること。

2.8 各種動作処理

本節では起動シーケンスを説明する。

2.8.1 MAC 処理

スマートメーターは、自身のIEEE802.15.4 PANネットワークを形成するために、次のステップを実施する。

スマートメーターは、自装置が利用可能な無線チャネルの中で、ED Scan及びEnhanced Active Scanを実施し、利用環境の良い無線チャネル帯及び周囲で利用されていないPAN IDを検出する。利用する無線チャネルは、スマートメーターで選択して良く、利用環境の良い無線チャネル帯が見つからない場合の処理も、スマートメーターの判断で決定してよい。尚、PAN IDは周囲で利用されているもの以外から決定する。

スマートメーターのEnhanced Active Scanでは、スマートメーターの送信元MACアドレスを設定したEnhanced Beacon Requestコマンドをブロードキャスト送信する。このEnhanced Beacon Requestの目的は、スマートメーターの周囲で利用されているPAN IDの調査であるため、IEsフィールドによるフィルタリングは行わなくてもよい。IEsフィールドによるフィルタリングを行わないことで、スマートメーター周囲のシステムから可能な限りのEnhanced Beaconを応答として期待できる。

Enhanced Beacon Requestコマンドを受信した周囲のシステムは、応答として、Enhanced Beaconを返す必要がある。その際Enhanced Beaconの宛先は、Enhanced Beacon Requestの送信元アドレスに対するユニキャストにすべきである。

HEMSは、自宅のスマートメーターを検出するため、IEsフィールドを用いたEnhanced Active Scanを実施する。HEMSが送信するEnhanced Beacon RequestのPayload IEsフィールドにMLME IE(Group ID=0x1)を利用、Sub-ID=0x68(Unmanaged)のIE Contentsに、自身が所持するBルート認証IDの下位8octets（ネットワーク識別子）を含めて送信する。スマートメーターはPayload IEsのMLME IE内に格納されたネットワーク識別子が、自身が持つネットワーク識別子と一致する場合に、スマートメーターはEnhanced Beaconを返すことで応答とする。同じIDを持った装置であることの確認をするため、HEMSからのEnhanced Beacon Requestと同じ情報を、Enhanced BeaconのPayload IEsフィールドに含める。

この動作により、HEMSは自宅スマートメーターの候補を検出する（図 2-3）。

(1) シーケンス処理

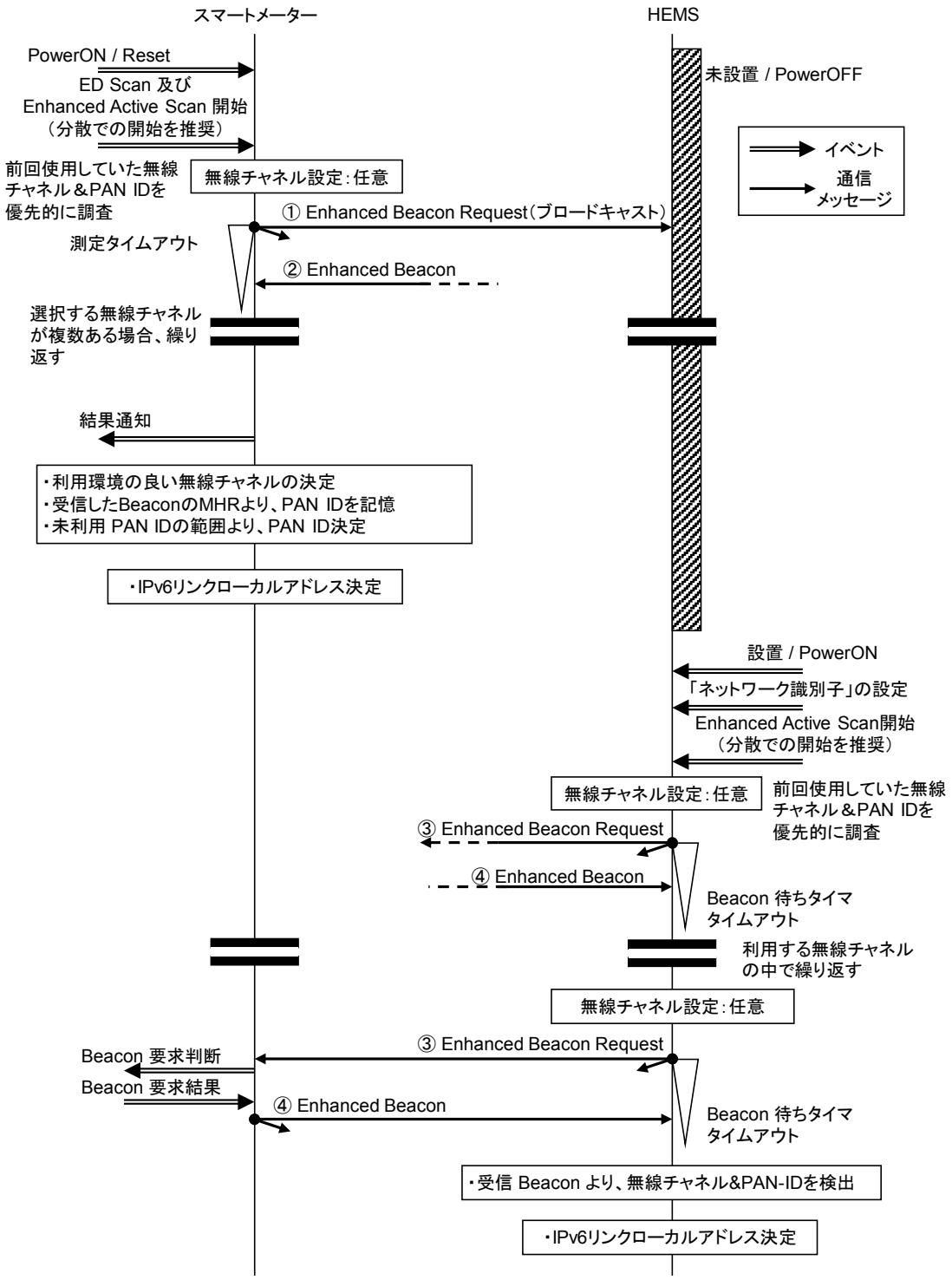

図 2-3 MAC 処理

⑵ パラメータ

図 2-3内の各フレームにおけるパラメータを**表 2-4**～**表 2-8**に示す。

表 2-4 ①Enhanced Beacon Requestパラメータ (送信元：スマートメーター)

パラメータ名	内容	値	備考
送信元	スマートメーター	“64bitアドレス”	
宛先	ブロードキャスト	0xFFFF	
Information Elements (IEs) フィールド	利用しない	－	

表 2-5 ②Enhanced Beaconパラメータ (送信元：周囲のシステム)

パラメータ名	内容	値	備考
送信元	別宅スマートメーター	“64bitアドレス”	
宛先	スマートメーター	“64bitアドレス”	
Information Elements (IEs) フィールド	利用しない	－	
Beacon Payload フィールド	利用しない	－	

表 2-6 ③Enhanced Beacon Requestパラメータ(送信元：HEMS)

パラメータ名			内容	値	備考
送信元			HEMS	“64bitアドレス”	
宛先			ブロードキャスト	0xFFFF	
Information Elements (IEs) フィールド					
	Header IEs		利用しない	－	
	Payload IEs	MLME IE	Outer IE descriptor	Length	0x0a	IE Content長
				Group ID	0x1	MLME
				Type	0x1	
			Sub-IE descriptor	Length	0x8	Sub-IE Content長
				Sub-ID	0x68	ネットワーク識別子用
				Type	0x0	
				Sub-IE Content	ネットワーク識別子	8 octets長
		List termination		Length	0x0	
				Group ID	0xf	Payload IEの終了を示す

表 2-7 ④Enhanced Beaconパラメータ (送信元：スマートメーター)

パラメータ名			内容	値	備考
送信元			スマートメーター	“64bitアドレス”	
宛先			HEMS	“64bitアドレス”	
Information Elements (IEs) フィールド					
	Header IEs		利用しない	―	
	Payload IEs	MLME IE	Outer IE descriptor	Length	0x0a	IE Content長
				Group ID	0x1	MLME
				Type	0x1	
			Sub-IE descriptor	Length	0x8	Sub-IE Content長
				Sub ID	0x68	ネットワーク識別子用
				Type	0x0	
				IE Content	ネットワーク識別子	8 octets長
		List termination		Length	0x0	
				Group ID	0xf	Payload IEの終了
Beacon Payload フィールド			利用しない	―	

表 2-8 MLME IEのSub-ID 割当て

Sub-ID value	Content length	Name	Description
0x68	Variable	Unmanaged (ネットワーク識別子)	ネットワーク識別子を示すSub-IDとして[JJ-300.10v2]で定義された値

また、Enhanced Active ScanタイマーとEnhanced Beacon Request連続送信回数について**表 2-9**に示す。

表 2-9 Enhanced Active ScanタイマーとEnhanced Beacon Request連続最大送信回数

項目名	内容	値	備考
Enhanced Active Scanタイマー	Enhanced Active ScanによるEnhanced Beacon待ち時間	5 [sec]	HEMSがスマートメーターからの応答を待つ時間(推奨値)
Enhanced Beacon Request連続最大送信回数	連続してEnhanced Beacon Request送信する回数	3 [回]	

2.8.1.1 Enhanced Beacon Request 最大送信回数

HEMSからのEnhanced Beacon Request連続最大送信回数（**表 2-9**）に達してもスマートメーターからのEnhanced Beaconの応答を得られなかった場合、一定時間あけてから再度Enhanced Beacon Requestを送信するか、処理を中断すること。

2.8.2 ネットワーク処理

スマートメーター及びHEMSは、 [SLAAC]に従い、DAD(Duplicate Address Detection)処理を実施してもよい（**図 2-4**）。

(1) シーケンス図

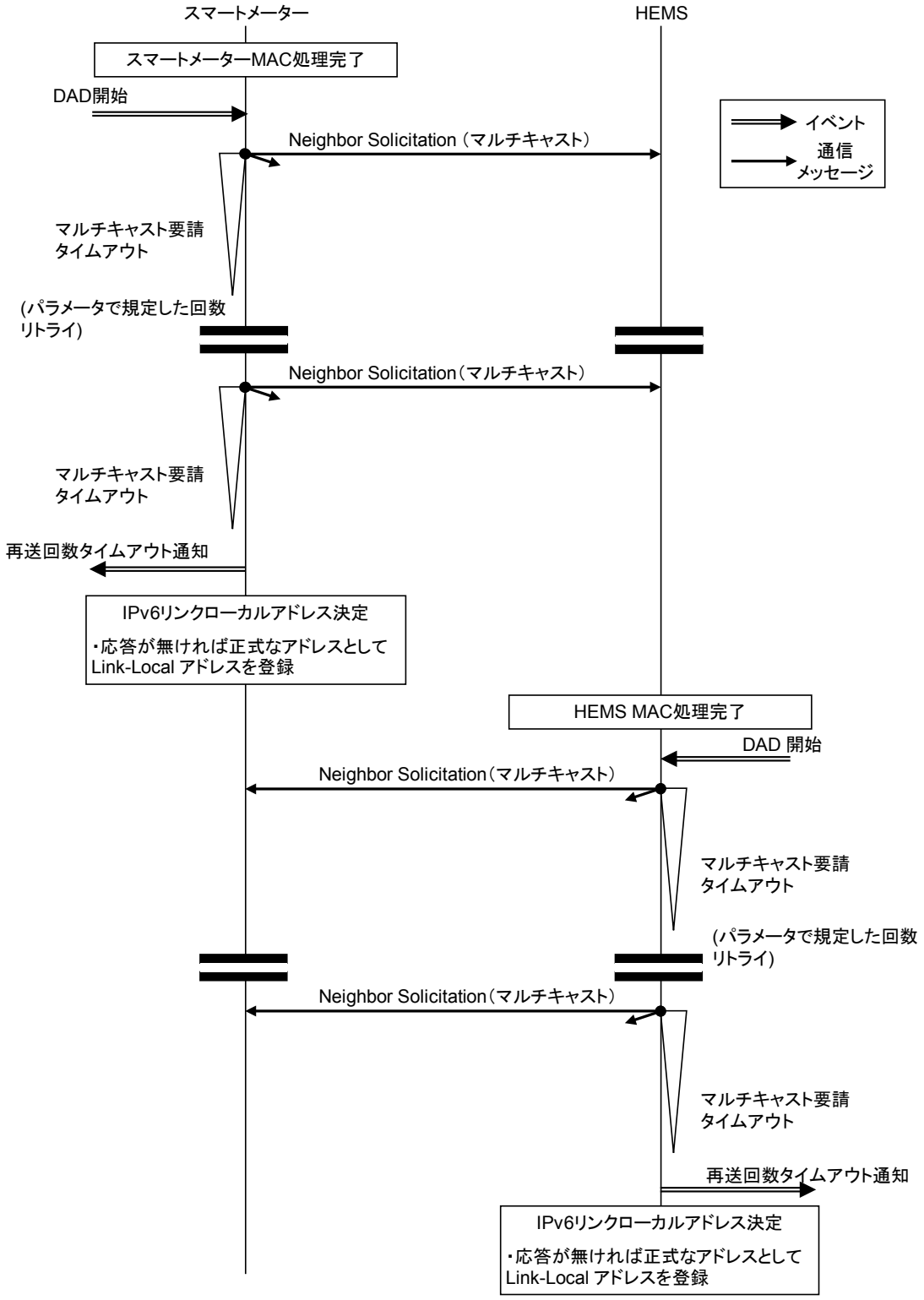

図 2-4 DAD処理

⑵ パラメータ

DADのパラメータを**表 2-10**に示す。

表 2-10 DADのパラメータ

パラメータ名	内容	値	備考
再送タイマー	NSのタイムアウト	1 [sec]	IPv6と同じ [RETRANS_TIMER]
リトライ回数	NSの送信回数	3 [回]	IPv6と同じ [MAX_MULTICAST_ SOLICIT]

2.8.2.1 DAD 失敗

DADが失敗した場合（他ノードが該当IPアドレスを使用していた場合）、処理を中断してもよいし、起動シーケンスをやり直してもよい。

2.8.2.2 相互の IPv6 アドレス解決

HEMSからスマートメーターに対してPANAによる認証を実施するため、スマートメーターのIPv6アドレスを検出する必要がある。相互のアドレス解決の方法として、スマートメーターからのEnhanced BeaconのMACアドレスから、IPv6リンクローカルアドレスを推定する。
MACアドレスからの判断であるため、[ND]によるNeighbor Discoveryは実施しなくてもよい。

2.8.2.3 Neighbor Discovery

Neighbor Discoveryを実施して、応答を受信しなかった場合においても、MACアドレスから生成したIPv6リンクローカルアドレスを使用してよい。

2.8.3 認証鍵交換

HEMS（PaC[1]）の動作は、以下を推奨する。MAC_P[2]を計算する際、ID_S[3]に関連づけられたPSKから計算されたAKを選択すること。ID_Sに紐付けられたPSK（から計算されたAK）が確認できない場合は、EAP認証を失敗させること。また、PAA[4]は、次の動作を必須とする。MAC_S[5]を計算する際、ID_P[6]に関連づけられたPSKから計算されたAKを選択すること。ID_Pに紐付けられたPSK（から計算されたAK）が確認できない場合は、EAP認証を失敗させること。

2.8.3.1 PANA の各フェーズでの処理

2.8.3.1.1 Authentication and Authorization Phase

このフェーズはPANA起動時に実行される。つまりHEMSが設置され、ネットワークに接続し、IPアドレスの設定が終了した直後に実行される。また、Termination フェーズによってPANAのセッションが終

1 PaC: PANA Client。[PANA]参照。
2 MAC_P: EAP ピア側が計算する Message Authentication Code。[EAP-PSK]参照。
3 ID_S: EAP サーバ側識別子。[EAP-PSK]参照。
4 PAA: PANA Authentication Agent。[PANA]参照。
5 MAC_S: EAP サーバ側が計算する Message Authentication Code。[EAP-PSK]参照。
6 ID_P: EAP ピア側識別子。[EAP-PSK]参照。

了した後とPANAのセッションがタイムアウトした後に再度スマートメーターと接続する場合にも実行される。

このフェーズの結果、PANAのライフタイムを持つセッションが確立される。PAA(スマートメーター)とPaC(HEMS)はマスター鍵(MSK/EMSK)を共有し、マスター鍵からMAC層用暗号鍵を導出しMAC層へ鍵情報(ライフタイムを含む)の受け渡しが行われる。PANAのセッションライフタイムは、本章では規定しないが、推奨値は24時間（86400秒）とする。

Authentication and Authorizationフェーズのシーケンスを図 2-5に示す。

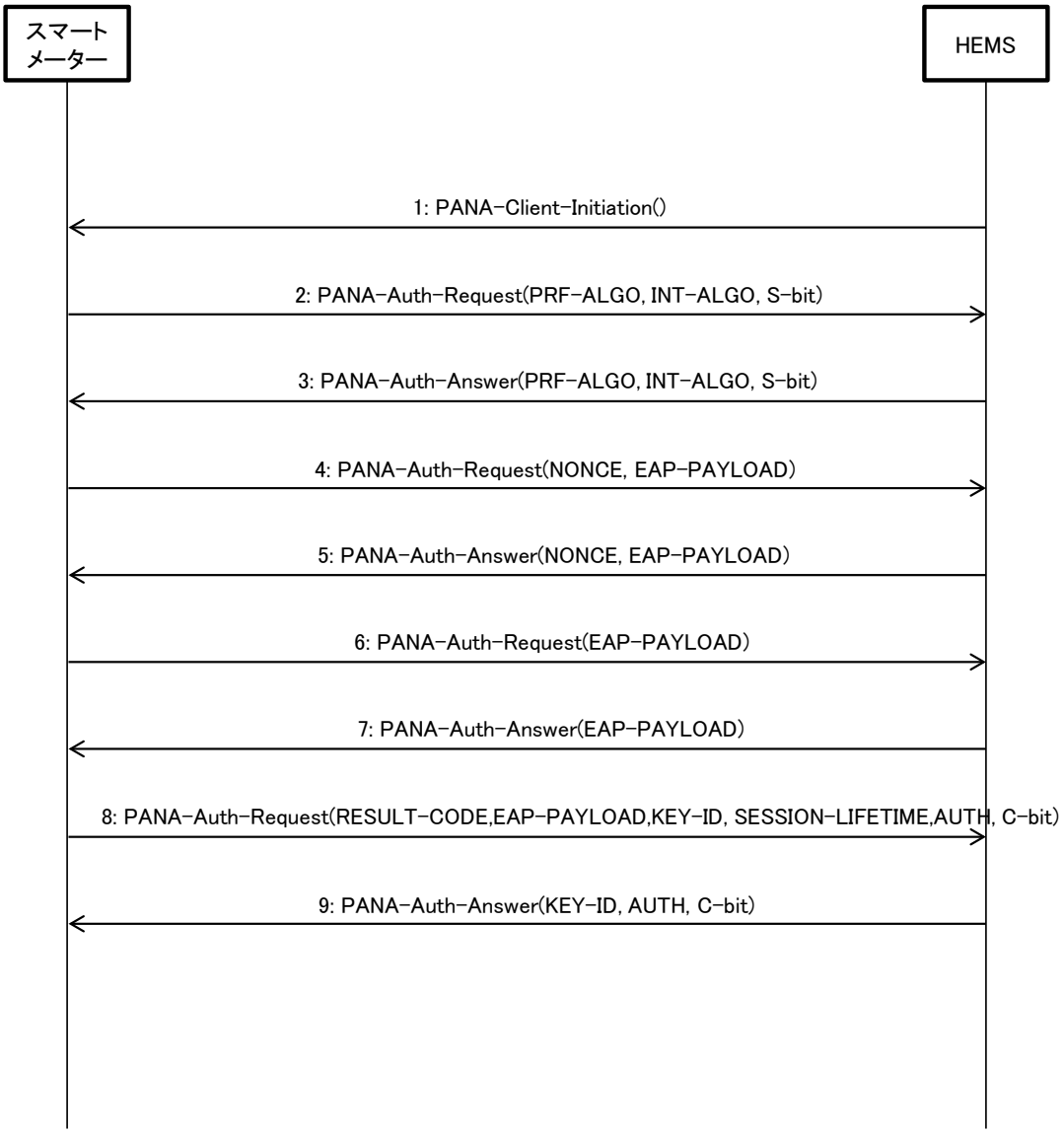

図 2-5 Authentication and Authorization フェーズ

2.8.3.1.2 Access Phase

このフェーズは、PANAセッションが確立された状態(セッションのライフタイム期間中)である。PANAセッションが維持されているか確認するために、PANA Pingを任意に実行できる。

HEMS（PaC）からPANA Pingを送信する場合のシーケンスを図 2-6に例示する。

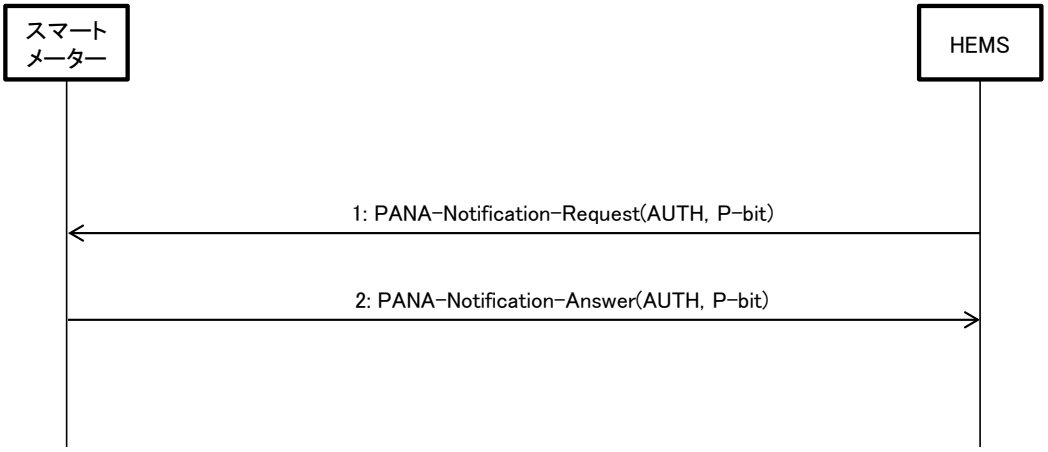

図 2-6 PANA Access フェーズにおける PANA-Ping シーケンス例

2.8.3.1.3 Re-authentication Phase

確立したPANAのセッションを更新するために実行される。このフェーズはAuthentication and Authorizationフェーズにて設定されたセッションのライフタイムが切れる前に実行しなければならない。目安としてライフタイムの8割が過ぎた時点で実行すべきである。この時新旧複数のMSK/EMSKが存在することになるが、鍵使用者は新しく生成されたMSK/EMSK（から生成された鍵）を優先して使用すること。シーケンス図を図 2-7に示す。

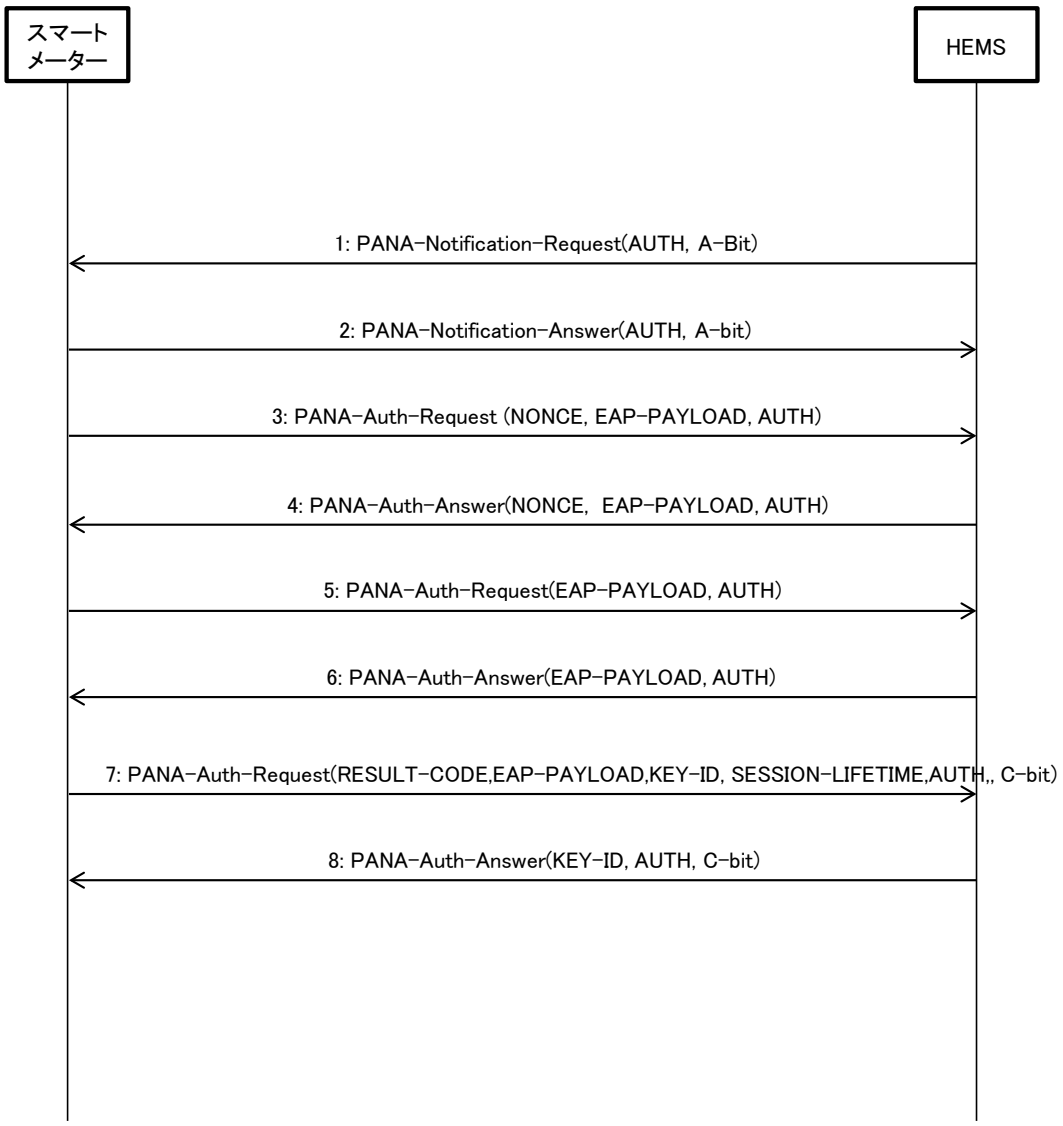

図 2-7 PANA Re-authentication フェーズシーケンス

2.8.3.1.4 Termination Phase

このフェーズはPANAを終了させる時点で実行され、PANAのセッションを終了する。

Termination requestを必ず実行する必要はないが、受信した際は適切に処理すること。Termination phaseが実行されない場合は、PANAセッションライフタイムの有効期限切れを待ってPANAのセッションを終了する。

HEMS（PaC）からPANAセッション終了をリクエストする場合のシーケンスを図 2-8に例示する。

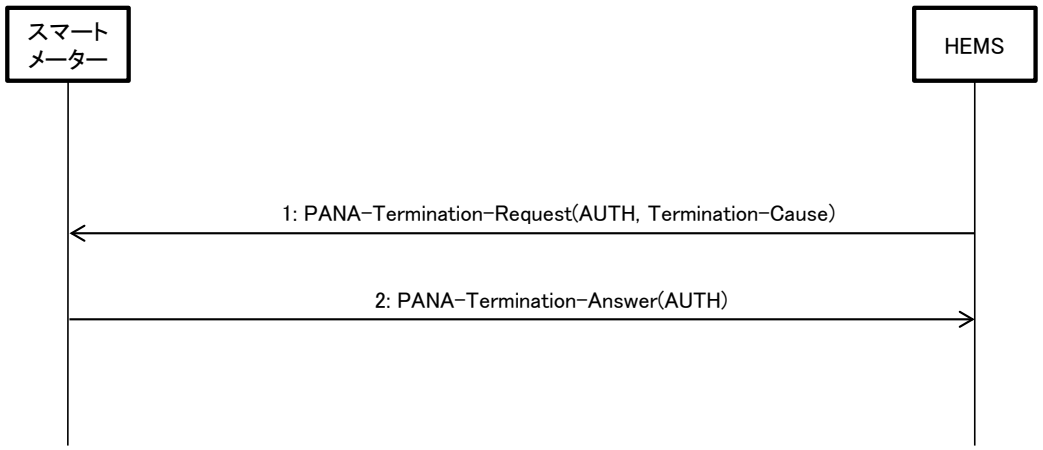

図 2-8 PANA Termination フェーズシーケンス

2.8.3.2 PANA メッセージの再送処理

PANAメッセージの再送処理はデフォルト値を含めRFC5191の第9章に準拠するが、以下に本章における補足を述べる。

再送信回数が最大再送回数(MRC)に達しても、宛先から応答を得ることができなかった（PANA Pingを含む）PANAリクエスト送信側は、既存PANAセッションを終了させる。HEMSがPANAリクエスト送信側の場合、HEMSは起動シーケンスから再度やり直すこと。尚、消去されたPANAセッションで導出されたMACフレーム暗号鍵も同時に無効とする。そのため、（PANAリクエストに対する応答がなかった）宛先に対して、有効な暗号鍵を持たない場合、本章で暗号化の対象となるMACフレームを送出してはならない。

HEMSはスマートメーターとの間で継続して通信ができない（例：スマートメーターからの30分検針値が時間をおいて複数回の要求を行っても取得できないなど）ことを判断した時点で、再度起動シーケンスからやり直し、新規PANAセッションを確立すること。

2.8.3.2.1 Re-Authentication Phase 起動の失敗

最大再送回数(MRC)に達する前にライフタイム期限が過ぎて、PANAセッションが終了した場合には、Re-Authentication Phaseを終了して直ちに起動シーケンスから再度やり直すこと（この場合、PANAについてもAuthentication and Authorization Phaseを起動する）。

2.8.3.3 Access Phase での PCI 受信

スマートメーター（PAA）は、既にPANA セッションを確立している（Access Phase中の）HEMS（PaC）からPCIを受信した場合、新しいPANAセッションにてPANA Security Association（PANA SA）の設定を開始すること。認証が成功して新たなPANA SA（及びPANAセッション）が確立された場合、ただちに新しいPANA SA（及びPANAセッション）の使用を開始し、当該HEMSとの間の古いPANA SA（及びPANAセッション）を削除すること（この時スマートメーターはHEMSへPTRを送信しなくてもよい）。

またこの時、同一のHEMS（PaC）に対して無制限に複数のPANA SAが作成されることを防ぐために、スマートメーターは同一HEMSに対して同時に存在できるPANA SAの数を2つに制限すべきである。

2.8.3.4 不正な PANA メッセージの受信

[PANA]の5.5節に従い、PANAメッセージの構成の不備やAUTH AVP中のハッシュ値が不正であるPANAメッセージを受信した場合、受信したノードはメッセージを廃棄すること。

2.8.3.5 認証エラー

[EAP]で規定されるように、EAP authenticatorが認証エラー（EAP peerとの認証失敗）を検知した場合、EAP peerとの認証処理を廃棄し、EAP Failure (Code 4)を設定したEAPメッセージを送信することになる。

EAP authenticatorとなるPAA（スマートメーター）はこのEAPメッセージとともに、Result-Code AVPにPANA_AUTHENTICATION_REJECTEDもしくは、PANA_AUTHORIZATION_REJECTEDが含まれたメッセージ（Cフラグ付き）を送信する。

EAP peerとなるPaC（HEMS）において認証エラー（EAP authenticatorとの認証失敗）を検知した場合、EAP authenticatorとの認証処理を廃棄し、PANAのフェーズ処理を中止する。

これらにより、PANAのフェーズ処理が完了しなかった場合、PaC（HEMS）は再度起動シーケンスからやり直してもよいしPANAのみをやり直してもよい。

第3章　PLC（G3-PLC）用Bルート下位レイヤ実装

3.1 概要

本章では、[G3-PLC]および[JJ-300.11v2]のIPv6通信上でECHONET Liteをアプリケーションプロトコルとして使用したスマートメーター~HEMS間の通信インタフェースを実装する場合について補足を行う。

図 3-1に本章で述べるネットワークスタックを示す。[G3-PLC]上でIPv6を動作させるために6LoWPANを使用し、アプリケーションプロトコルとしてECHONET Liteを動作させる。

Application層		ECHONET Lite
Transport層		UDP
Network層		IPv6
（Adaptation層）		6LowPAN (ITU-T G.9903 (2013))
MAC層		G3-PLC (ITU-T G.9903 (2013))
PHY層		G3-PLC (ITU-T G.9903 (2013))

図 3-1 ネットワークスタック

接続シーケンスの概要は図 3-2となる。

スマートメーターをPANコーディネーターとし、HEMSを端末として動作させる。

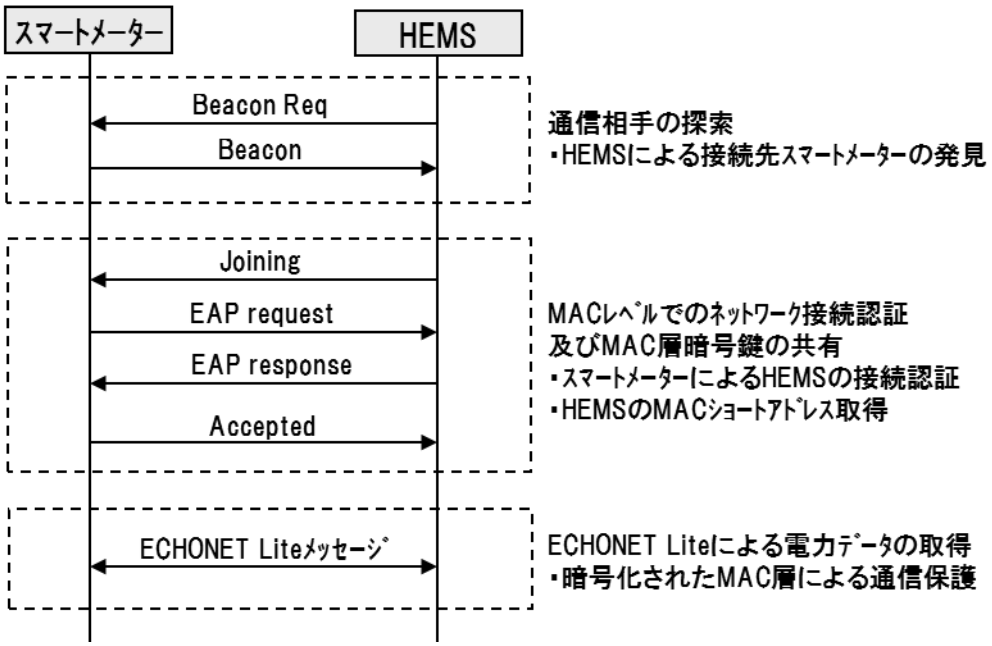

図 3-2 接続シーケンス図（概要）

3.2 物理層

物理層の仕様は[JJ-300.11v2]に従う。

したがって、[G3-PLC]のAnnex F (Regional Requirements for Japan)が適用される。

また、Interleaverは[JJ-300.11v2]に従う。

以下には、Bルート通信インタフェースとして備えるべき仕様を示す。

3.2.1 Frame control header (FCH)

FCHを構成するフィールドのうち、Coherent Modeについてはdifferential modeを使用する（表 3-1）。他のフィールドについては、[G3-PLC]及び[JJ-300.11v2]に従う。

表 3-1 FCH の Coherent Mode 値

名称	ビットサイズ	値	備考
Coherent Mode	1	0	日本仕様ではdifferential modeを選択

3.3 MAC 層

MAC層の仕様は[JJ-300.11v2]に従う。

以下には、Bルート通信インタフェースとして備えるべき仕様を示す。

3.3.1 MAC 変数

最小バックオフ指数については8をデフォルト値として使用する（表 3-2）。

表 3-2 MAC 変数

変数名	説明	範囲	デフォルト値	備考
macMaxBE	最大バックオフ指数	0～20	8	
macMinBE	最少バックオフ指数	0～macMaxBE	8	

3.3.2 優先度制御

優先度制御はNormal priorityのみ使用する。このため、Normal priorityのパケットはNormal priority Contention window (NPCW)のタイミングで送信される。

3.3.3 Security Level

暗号化にあたっては、秘匿(confidentiality)と認証(authenticity)の両方を実施するため、ENC-MIC-32 (Security level 5)を使用すること。

3.3.4 PAN ID

PANコーディネーター（スマートメーター）がBルートに割り当てるPAN IDは表 3-3の通りとする。

表 3-3 B ルート向け PAN ID

Bits:15	14	13-10	9-8	7-0
1	Reserved	0/1	0	0/1

※Reserved=”0”とする。

※PAN IDは0xFCFF（1111110011111111）とANDを取る（G.9903 (2013) Table9-30参照）。

3.4 LoWPAN アダプテーション層

LoWPANアダプテーション層の仕様は[JJ-300.11v2]に従う。

したがって、Fragmentation、Header compressionの仕様も[JJ-300.11v2]に従う。

以下には、Bルート通信インタフェースとして備えるべき仕様を示す。

3.4.1 LOADng disabling[JJ-300.11v2]に従い、マルチホップルーティングLOADng機能を無効化して１：１のシングルホップ通信を行う。

3.4.2 broadcast

Bルート通信は１：１通信であるので、broadcastパケットのMesh headerのHopslftの値は”1”とすること。

3.5 ネットワーク層

[JJ-300.11v2]に従う。

3.6 トランスポート層

[JJ-300.11v2]に従う。

3.7 セキュリティ処理

通信セキュリティとしてMAC層による通信の保護（暗号化）を実施する。　MAC層でのセキュリティは[G3-PLC]（ITU-T G.9903 (2013)）に規定される以下の方式を適用する。

①MACレイヤの暗号化処理

・AES-128-CCM*

②EAP-PSKによる認証、鍵配布

3.7.1 認証

EAPは、認証する側であるEAP serverと認証される側であるEAP peerの2つのノードから構成される。[G3-PLC]では、EAP-PSKのメッセージをLBP (LoWPAN Bootstrapping Protocol)でカプセル化して伝送する。スマートメーターがEAP serverとなり、HEMSがEAP peerとなる。

3.7.1.1 EAP の最小構成

- EAP 認証メソッドとして、共通鍵ベースの EAP-PSK を使用する
- EAP-PSK の認証鍵のサイズは 16 オクテットとする
- EAP-PSK の結果、相互認証に成功した場合、AES-EAX を使って保護された PCHANNEL 上で GMK を EAP server から EAP peer に対し配布する。
- MSK, EMSK は、本章では使用しない。
- サーバ側認証子である EAP ID_S は[NAI]で規定される NAI とする

  NAIの長さは36オクテットを超えないこととする。
- クライアント側認証子である EAP ID_P は[NAI]で規定される NAI とする

  NAIの長さは36オクテットを超えないこととする。

3.7.1.2 B ルート認証 ID・パスワードから EAP 認証情報への変換

NAI への変換

32桁のBルート認証IDをもとに以下のルールでEAP Identifier（ID_S、ID_P）で使用するNAIを生成する。

【NAI生成ルール】
スマートメーター側NAI（EAP ID_S）：”SM”＋”Bルート認証ID” （34オクテット）
HEMS側NAI（EAP ID_P）：”HEMS”＋”Bルート認証ID” （36オクテット）

例：
Bルート認証IDが「0023456789ABCEDF0011223344556677」の場合、
スマートメーター側NAI（EAP ID_S）：「SM0023456789ABCEDF0011223344556677」
HEMS側NAI（EAP ID_P）：「HEMS0023456789ABCEDF0011223344556677」

PSK への変換

EAP-PSKで使用するPSKは以下のルールで生成する。

【PSK生成ルール】
Bルート認証IDに結びついたパスワードをもとに次のPSK生成関数（PSK_KDF）を使用して16オクテットのPSKを生成する。

PSK = PSK_KDF(パスワード)
= LSBytes16(SHA-256(Capitalize(パスワード))
(パスワード文字列を大文字化し、SHA-256でハッシュした出力の下位16オクテット)

例：
パスワードが「0123456789ab」の場合
PSK = LSBytes16(SHA-256(“0123456789AB”))
= 0xf58d060cc71e7667b5b2a09e37f602a2

3.7.1.3 鍵更新

MAC層の暗号化とメッセージ認証子のために使用する鍵の有効期限は、本章では特に規定しないが、推奨値は24時間（86400秒）とする。

3.7.1.4 EAP-PSK 鍵導出関数

EAP-PSKのネゴシエーションによって生成するTEK(16オクテット)の導出は次のように行う。導出されたTEKはEAP-PSKメッセージPCHANNELフィールド内のTagの導出とR/E/Reserved(計1オクテット)のAES-128 EAXモードによる暗号化の鍵として使用する。

TEK = AES-128(KDK, (T xor 1))

TとKDKは次のように導く：
T = AES-128(KDK, RAND_P)
KDK = AES-128(PSK, (AES-128(PSK, 0) xor 2))

ここでPSKは、EAP serverとEAP peerによって事前に共有されている16オクテット長の鍵(事前共有鍵、Pre-Shared Key)、RAND_PはEAP-PSKシーケンスの2番目のメッセージ(peerからserverへ送信)に含まれる16オクテット長の乱数、AES-128()関数はmodified counter modeを使用したAES暗号(128ビット)である。EAP-PSKの鍵導出の詳細に関しては、[EAP-PSK]のFigure 7及びFigure 3を参照のこと。

[EAP-PSK]のFigure 9における、2番目と3番目のEAP-PSKメッセージ中で使用されるMAC_PとMAC_Sの値は次のように導出する。

```
MAC_P = CMAC-AES-128(AK, ID_P || ID_S || RAND_S || RAND_P)
MAC_S = CMAC-AES-128(AK, ID_S || RAND_P)

AK = AES-128(PSK, (AES-128(PSK, 0) xor 1))
```

ここで、CMAC-AES-128()関数はAES-128()を用いたCMAC出力関数である。

EAP-PSKメッセージで使用されるPCHANNELフィールドのTagはTEKを鍵とするAES-128 EAXモードによって出力されるMAC値(16オクテット)であり、R/E/Reserved(1オクテット)フィールドはAES-128 EAXモードによって暗号化される。

```
R/E/Reserved暗号文, Tag = EAX(N, H, R/E/Reserved, TEK)

N: PCHANNELのNonceフィールド(4オクテット)
H: EAP Request/Responseメッセージの EAP Code, からRAND_Sまでのヘッダ(22オクテット)
```

3.7.2 MAC 層鍵共有

スマートメーターは、HEMSから受け取ったEAP-PSKの第2メッセージに含まれるMAC_Pが正しいことを検証した後、HEMSに対してMAC層で使用するセキュリティ鍵GMK (Group Master Key) を、EAP-PSKの第3メッセージのPCHANNELで保護して配送する。GMKは128ビット長とし、その生成方法については本文書では規定しないが、第3者に推測されないよう十分なランダム性を持たせ、適切に設定すること（スマートメーターの実装依存とする）。メッセージフォーマット等詳細については、[G3-PLC]の第10章 Securityを参照のこと。

3.7.3 暗号化と改ざん検知

GMKを使用して[802.15.4-2006]に基づくMAC Dataフレームの暗号化を実施する。

EAP-PSKの第3メッセージによって、GMKの配送（更新を含む）がされた場合、最新のGMKを使用して送信MACフレームを暗号化すること。

MACフレームのFrame Counterの値は新規GMKを使用する毎にリセットし、スマートメーターは、送受信MACフレームのFrame Counterの値があふれる前に、GMKの更新を行わなければならない。

暗号化にあたっては、秘匿(confidentiality)と認証(authenticity)の両方を実施するため、ENC-MIC-32(Security level 5)を使用すること。受信したMACフレームのMIC検証に失敗した場合は、フレームを廃棄する。

Key identifierモードとして0x01を使用し、Key Identifierフィールドには Key Sourceは使用せず、1オクテットのKey Indexのみ使用する。

3.7.4 リプレイアタック対策

MACフレームの暗号化対象となるメッセージについては、[802.15.4-2006]におけるMAC Auxiliary SecurityヘッダのFrame Counter処理によってリプレイアタック対策を実施する。つまり、新たに受信したMACフレームのFrame Counter値が受信済みのMACフレームのFrame Counter値よりも小さい場合は当該MACフレームを廃棄する。

3.7.5 DoS 対策

各ノードは短期間に大量のメッセージを受信したときに、ノードの他の処理に影響を及ぼさないように対策をとるべきである（例：受信処理レートの制限、一定期間の無応答など）。

3.8 各種動作処理

本節では、スマートメーターと宅内のHEMSを接続するためのMAC層レベルの接続・切断シーケンスについて示す。1章で述べたように、スマートメーターとHEMSは１：１で接続される。したがって、PLCを伝送媒体としたスマートメーターとHEMSから構成されるPANが形成される。

図 3-3にBルートの接続シーケンスを示す。スマートメーターをPANコーディネーターとする。これにより、HEMS機器を取り付けた住戸がHEMS側からBルート開始のトリガをかける（ビーコンリクエストを送る）ことができる。

Bルート開始の接続トリガからMAC層のネットワーク探索、ネットワーク接続、セキュリティ認証については、[G3-PLC]で定義されるメッセージフォーマット、通信手順に準拠する。

HEMSは起動後のBeacon request の開始タイミングを分散させるしくみを搭載することを推奨する。

各機器は起動時にEUI-64アドレスが設定されており、スマートメーターのショートアドレスは0x0000に設定される。HEMSがBルート開始の接続トリガをスマートメーターへ送信すると、LBPを使用して、ネットワーク接続が確立した際にスマートメーターからHEMSのショートアドレスが設定される。

HEMSはスマートメーターとの通信断を認識した場合、スマートメーターへの再接続を試みる。

[G3-PLC]でのPANからの離脱方法は、HEMS側でLeave処理（「Kick」コマンド）を実行することにより、PANから離脱することができる。

一斉停電時などを考慮すると、再接続時に通信量が瞬間的に増大するケースが考えられるため、PAN IDを予め記憶している不揮発性メモリから展開し再利用することにより、ネットワーク探索シーケンス（Beacon request/responseシーケンス）を省くことができる。

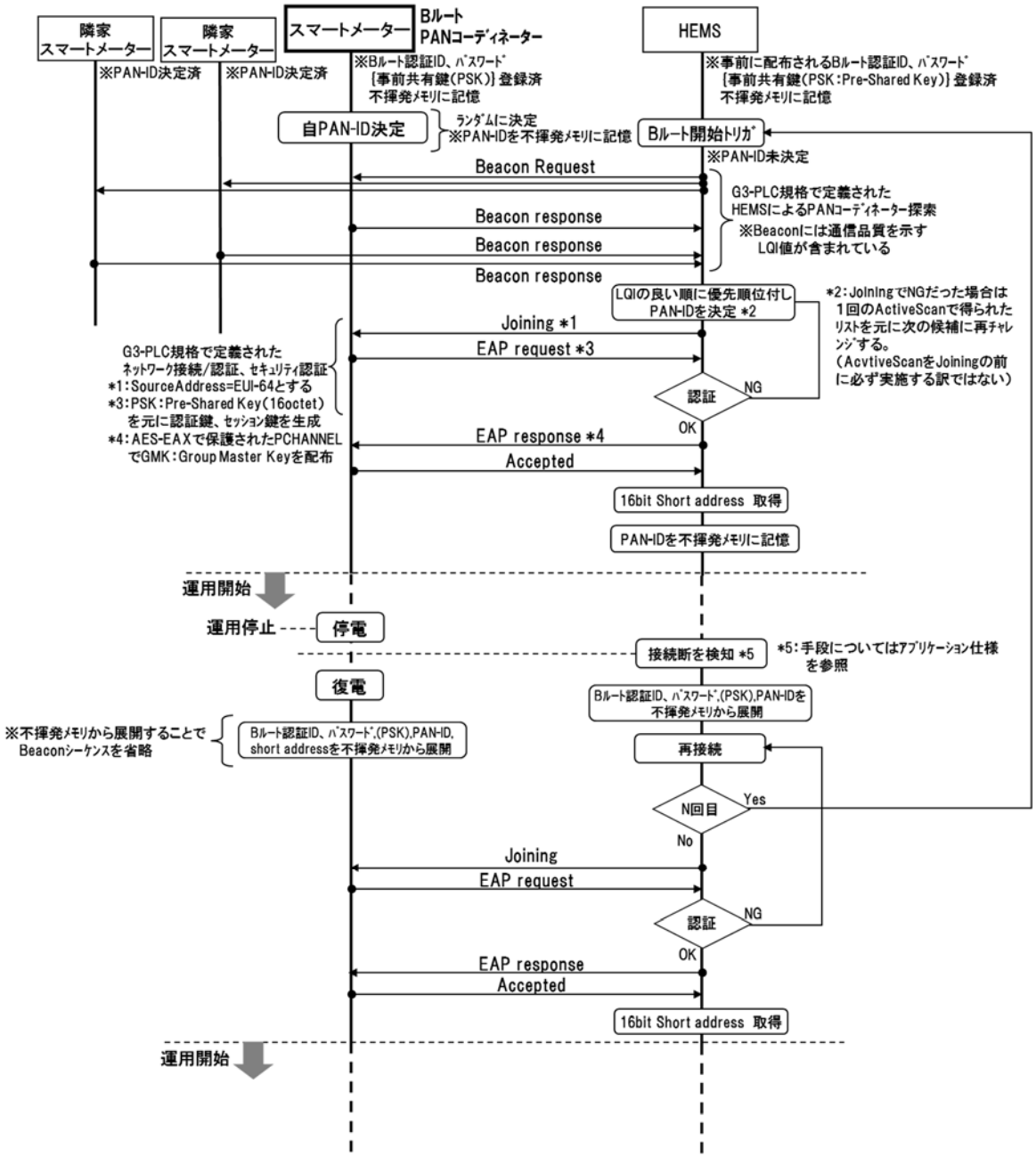

図 3-3 接続シーケンス(PLC)

第4章　920MHz（JJ-300.10 方式B：ZigBee）用Bルート下位レイヤ実装の概要

4.1 概要

本章では[JJ-300.10v2]の6に記載される920MHz用のIPv6に対応したZigBee IP仕様である方式Bを用いて、スマートメーター~HEMS間の通信インタフェースを実装する場合について補足を行う。なお方式Bにおいてはスマートメーターと HEMSが直接通信できない環境では、間に中継装置を置いても良い。

4.2 物理層

[JJ-300.10v2]の6.2.1記載の物理層をそのまま使う。

4.3 MAC 層

[JJ-300.10v2]の6.2.2記載のMAC層をそのまま使う。

4.4 LoWPAN アダプテーション層

[JJ-300.10v2]の6.2.3記載のLoWPANアダプテーション層をそのまま使う。

4.5 ネットワーク層

[JJ-300.10v2]の6.2.4記載のネットワーク層をそのまま使う。

4.6 トランスポート層

[JJ-300.10v2]の6.2.5記載のトランスポート層をそのまま使う。

4.7 セキュリティ仕様

[JJ-300.10v2]の6.2.6～6.2.10記載のTLS-PSK, EAP, PANAを使う。

B ルート認証 ID の ZIP NetworkID への変換と PSK Identity への適用

HEMSは、自宅のスマートメーターを検出するため、Active Scanを実施する。HEMSが送信するBeacon Requestに対して、スマートメーターは、自身が所持するBルート認証IDの下位16octetsをZIP NetworkIDとして設定したBeaconを応答する。HEMSは、受信したZIP NetworkIDが、自身が持つBルート認証IDの下位16octetsと一致する場合に、PANAセッションをスマートメーターに対して開始する。

PANAセッションにおいて、HEMSは、32octetsのBルート認証IDを[TLS-PSK]のClient Key Exchangeメッセージに含まれるPSK Identityに設定し、スマートメーターに通知する。スマートメーターは、自身が持つBルート認証IDと一致する場合に、当該Bルート認証IDに結びついたパスワードを利用して後述のルールで生成した16octetsのPSKを利用してTLS-PSK認証処理を実施する。(図 4-1)

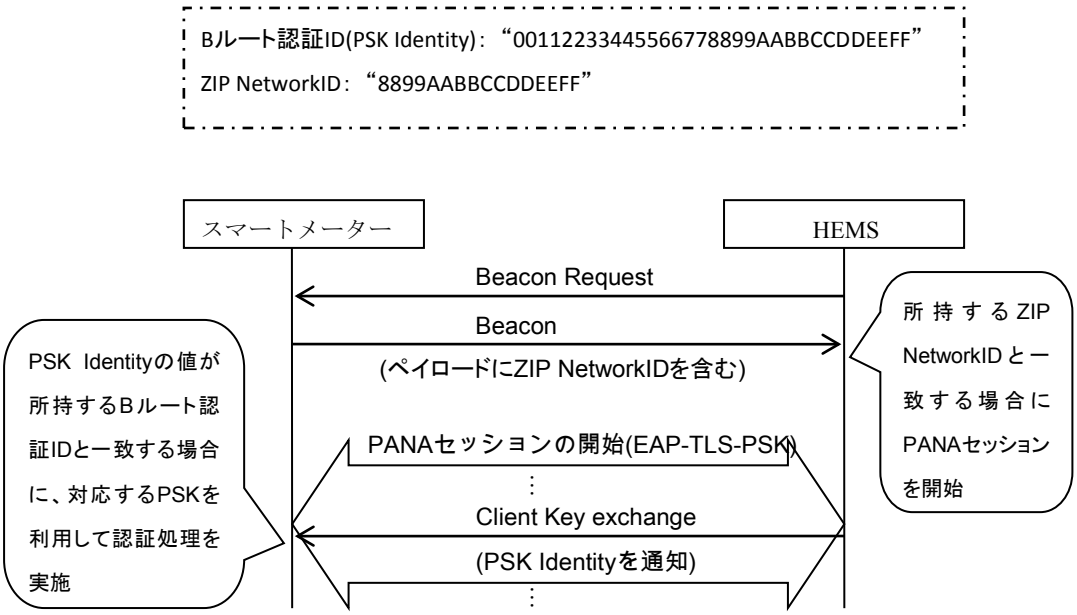

図 4-1 スマートメーター探索手順

パスワードの PSK への変換

[TLS-PSK]で使用するPSKは以下のルールで生成する。

【PSK生成ルール】
Bルート認証IDに結びついたパスワードをもとに次のPSK生成関数（PSK_KDF）を使用して16オクテットのPSKを生成する。

PSK = PSK_KDF(パスワード)
= LSBytes16(SHA-256(Capitalize (パスワード))
(パスワード文字列を大文字化し、SHA-256でハッシュした出力の下位16オクテット)

例：
パスワードが「0123456789ab」の場合
PSK = LSBytes16(SHA-256(“0123456789AB”))
= 0xf58d060cc71e7667b5b2a09e37f602a2

[GL]記載のBルート認証ID、パスワードなどのシステムに関する情報を使ったシーケンスは各種動作処理参照のこと。

4.8 各種動作処理

全体のシーケンスは次の図の通りとなる。

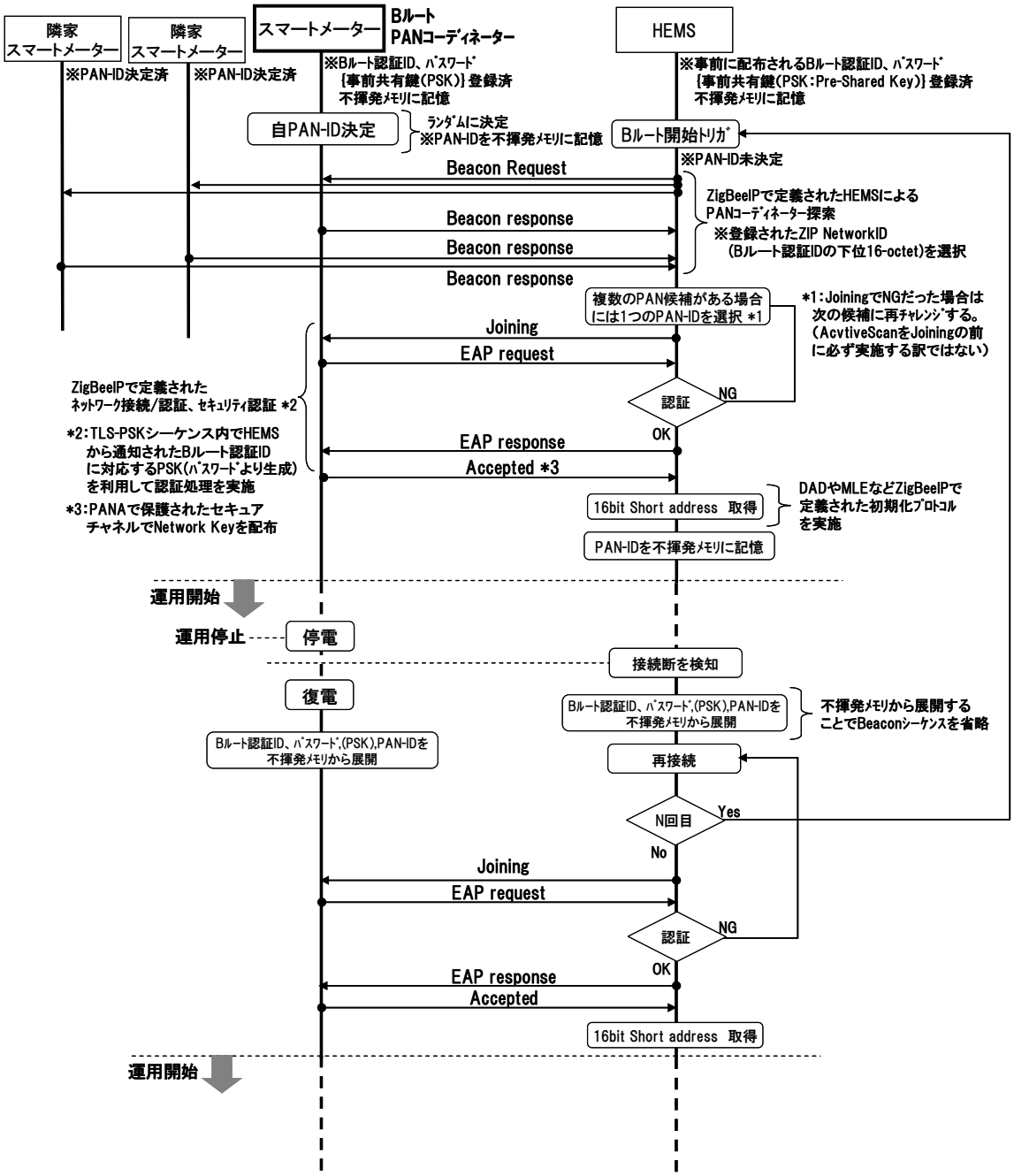

図 4-2 接続シーケンス図1(方式 B)

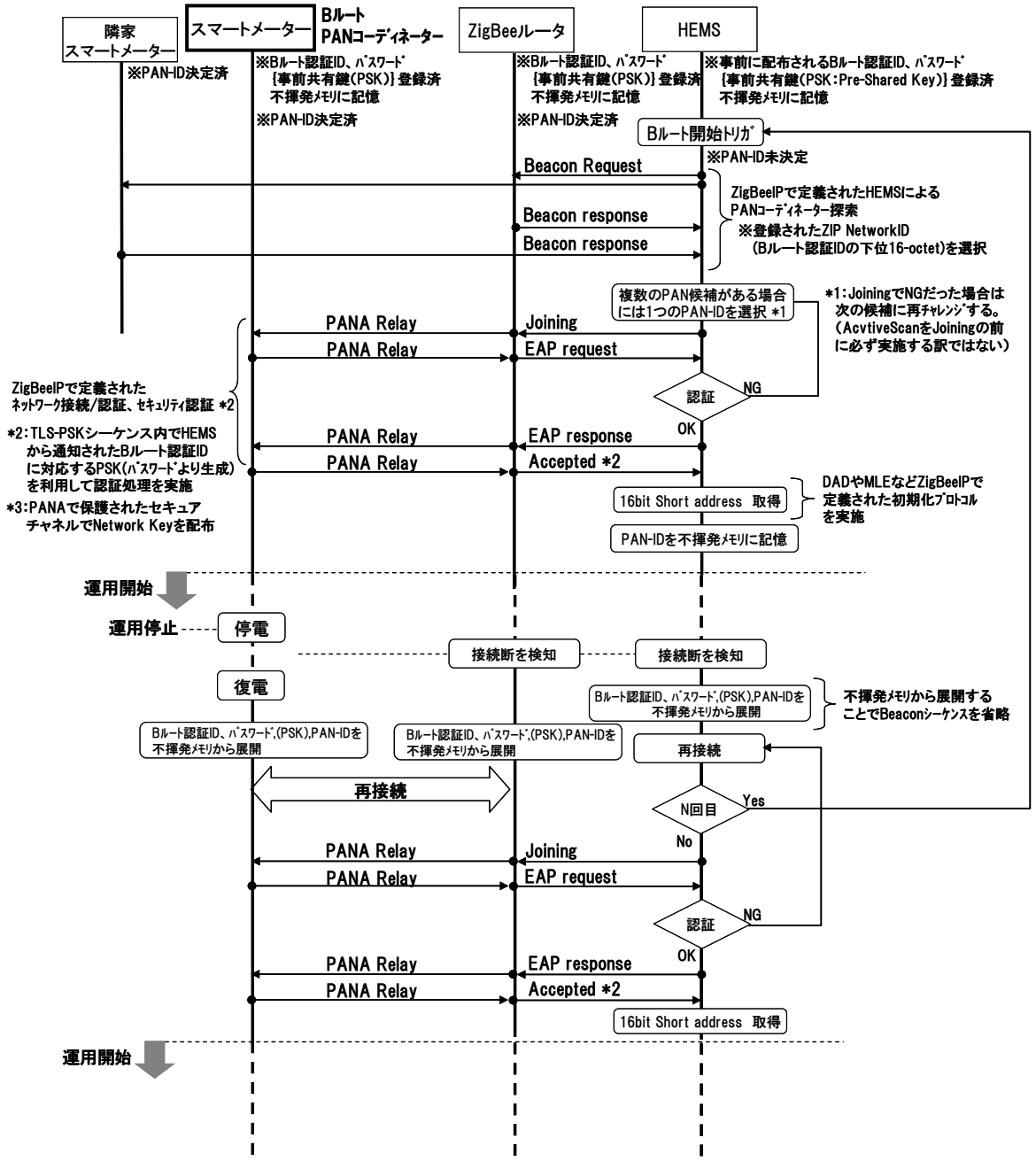

図 4-3 接続シーケンス図2(方式 B)