TTC技術レポート
Technical Report

TR-1052

EMS・アグリゲーションコントローラー -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 EMS･Aggregation Controller and Smart meter (Route-B)

第2.0版

2023年11月16日

一般社団法人
情報通信技術委員会
THE TELECOMMUNICATION TECHNOLOGY COMMITEE

目次

第 1 章　共通仕様 10
1.1　概要 10
1.2　ID および認証鍵 11
1.3　アプリケーション 11
1.3.1　アプリケーションレベルにおける要求頻度 12
1.3.2　再接続処理 14
1.3.3　スマートメーターの生存確認ができない等課題への対応 14
1.3.4　コントローラーの置き換えに対する対応 15
第 2 章　920MHz（JJ-300.10 方式 A：Wi-SUN）用 B ルート下位レイヤ実装 16
2.1　概要 16
2.2　物理層 17
2.3　MAC 層 17
2.4　LoWPAN アダプテーション層 17
2.5　ネットワーク層 17
2.5.1　IP アドレッシング 18
2.5.2　近隣探索 18
2.5.3　マルチキャスト 19
2.6　トランスポート層 19
2.7　セキュリティ処理 19
2.8　各種動作処理 19
2.8.1　MAC 処理 19
2.8.2　ネットワーク処理 23
2.8.3　認証鍵交換 24
2.9　処理シーケンス 28
第 3 章　2.4GHz 帯無線 LAN 用 B ルート下位レイヤ実装 29
3.1　概要 29
3.2　物理層 29
3.3　MAC 層 30
3.3.1　フレームフォーマット概要 30
3.4　ネットワーク層 31
3.5　IP アドレス 32
3.5.1　ユニキャストアドレス 33
3.5.2　マルチキャストアドレス 33
3.6　近隣探索 33
3.7　トランスポート層 34
3.8　セキュリティ処理 34
3.9　認証・暗号 35
3.9.1　WPA2-PSK(AES) 36

3.9.2 WPA3-SAE(オプション) 37
3.10 鍵更新 40
3.10.1 AP 機能 40
3.10.2 STA 機能（クライアント機能） 40
3.11 暗号化と改ざん検知 40
3.12 リプレイアタック対策 40
3.13 DoS 対策 40
3.14 各種動作処理 40
3.14.1 B ルート Wi-Fi 接続開始／終了処理 40
3.14.2 宅内 AP 交換（再設定） 45
3.14.3 宅内 AP 故障時（接続完了後） 46
3.14.4 EMS・アグリゲーションコントローラー交換 47
3.14.5 スマートメーターが複数台の場合 48
3.14.6 EMS・アグリゲーションコントローラーが複数台の場合 49
3.15 処理シーケンス 50
第 4 章 IEEE802.3 下位レイヤ実装 52
4.1 概要 52
4.2 物理層 52
4.3 MAC 層 53
4.3.1 フレームフォーマット概要 53
4.4 ネットワーク層 53
4.4.1 IP アドレス 55
4.4.2 ユニキャストアドレス 55
4.4.3 マルチキャストアドレス 56
4.4.4 近隣探索 57
4.5 トランスポート層 57
4.6 処理シーケンス 58

＜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	2021年3月17日	制定
第2.0版	2023年11月16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。

[802.11ax-2021] IEEE Standard for Information Technology--Telecommunications and Information Exchange between Systems Local and Metropolitan Area Networks--Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 1: Enhancements for High-Efficiency WLAN

[802.11n-2020] IEEE Standard for Information technology-- Local and metropolitan area networks-- Specific requirements-- Part 11: Wireless LAN Medium Access Control (MAC)and Physical Layer (PHY) Specifications Amendment 5: Enhancements for Higher Throughput IEEE 802.11-2020

[IEEE 802.15.4g-2012] IEEE Standard for Local and metropolitan area networks--Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs) Amendment 3: Physical Layer (PHY) Specifications for Low-Data-Rate, Wireless, Smart Metering Utility Networks

[802.15.4-2020] IEEE Standard for Low-Rate Wireless Networks

[802.3u-1995] IEEE Standards for Local and Metropolitan Area Networks: Supplement - Media Access Control (MAC) Parameters, Physical Layer, Medium Attachment Units, and Repeater for 100Mb/s Operation, Type 100BASE-T (Clauses 21-30)

[AH] IP Authentication Header, IETF RFC 4302

[JJ-300.10v2方式A] TTC標準 JJ-300.10v2方式A, 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

[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 1.14

[EL-SDG2] ECHONET-Lite System Design Guidelines_2nd edition

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

[GL-L] 資源エネルギー庁次世代スマートメーター制度検討会・EMS・アグリゲーションコントローラースマートメーターBルート(低圧スマート電力量メーター)運用ガイドライン［第5.0版］

[GL-H] 資源エネルギー庁次世代スマートメーター制度検討会・EMS・アグリゲーションコントローラースマートメーターBルート(高圧スマート電力量メーター)運用ガイドライン［第2.0版］

[NAI] The Network Access Identifier, IETF RFC 4282

[SHIF-H1.00] 双方向対応高圧スマート電力量メータ・コントローラー間アプリケーション通信インタフェース仕様書Version 1.00

[SHIF-L1.10] ELの低圧スマート電力量メータ・コントローラー間アプリケーション通信インタフェース仕様書Version 1.10

[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 8200

[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. 用語・略語

AES-128	Advanced Encryption Standard。米国NIST(アメリカ国立標準技術研究所)によって標準化されたブロック長128ビットの共通鍵暗号方式(FIPS-197)で鍵長として128ビットを用いるもの。
AP	無線LAN親機（アクセスポイント）
BPSK	Binary Phase-Shift Keying（二位相偏移変調）
Bルート	スマートメーターとEMS・アグリゲーションコントローラー間の通信路を指す。
Bルート認証ID	本仕様では、スマートメーターとEMS・アグリゲーションコントローラー間のペアリングをするために使用されるID。スマートメーターのSSIDとして使用される。
CCK	Complementary Code Keying（相補型符号変調方式）
CCMP	Counter mode with CBC-MAC Protocol
CCM*	Counter with CBC-MAC mode
CSMA-CA	Carrier Sense Multiple Access with Collision Avoidance
DSSS	Direct Sequence Spread Spectrum（直接拡散方式）
DBPSK	Differential Binary Phase-Shift Keying（差動位相偏移変調方式）
DQPSK	Differential Quadrature Phase-Shift Keying（差動四相位相偏移変調）
EL AIF認証	ECHONET Lite AIF仕様に正しく適合していることを証明する認証
EMS・アグリゲーションコントローラー（コントローラー）	下位レイヤにおいて、JJ-300.10v2方式A（高圧・低圧のスマートメーター）、2.4GHz帯無線LAN（低圧スマートメーター）、IEEE802.3方式（高圧スマートメーター）に対応し、上位レイヤにおいて、ELが定める双方向対応高圧スマート電力量メータ若しくは、低圧スマート電力量メータとの接続に関するEL AIF認証を取得したノードを言う、
HTTP	Hypertext Transfer Protocol

ICMP	Internet Control Message Protocol
IP	Internet Protocol。RFC791(IPv4)、RFC2460(IPv6)に定義されるデータグラムベースのパケット通信規格。現在広く使われているバージョンは４(IPv4)。次世代規格としてバージョン６(IPv6)が制定されている。本仕様ではIPv6を用いる。
IPアドレス	IPネットワーク上に接続されたノードへパケットを転送するための識別子。IPv6アドレスの長さは128ビットである。
MAC	Medium Access Control
MIC	Message Integrity Code。データが改ざんされているか検証するために使われる値。
Nonce	セキュリティにおいて、リプレイ攻撃などを防ぐためにメッセージ中に使用する(疑似)乱数。
OFDM	Orthogonal Frequency Division Multiplexing（直交波周波数分割多重）
OFDMA	Orthogonal Frequency Division Multiple Access（直交周波数分割多元接続）
PHY	Physical Layer
PSK	Pre-Shared Key。事前共有鍵。X.509などの証明書を使用せず事前に両ノードで同じ秘密(鍵)を設定し、認証時に用いる方式。
*QAM	Quadrature Amplitude Modulation（直行振幅変調）
QPSK	Quadrature Phase Shift Keying（四位相偏移変調）
SSID	Service Set Identifier（APの識別名） スマートメーターのSSIDとしては、Bルート認証IDを使用する。
STA	無線LAN子機（ステーション）
TKIP	Temporal Key Integrity Protocol（無線LANの暗号化プロトコル）
UDP	User Datagram Protocol。RFC768によって定義されIP上で動作するトランスポートプロトコル。パケットの喪失やデータの誤りを訂正する機能はない。
Wi-Fi	IEEE802.11をベースにした無線通信規格。スマートメーターはSTAモードについて2.4GHz帯のWi-Fi4の認証取得を必須とし、Wi-Fi6を任意とする。
WPA2-PSK	Wi-Fi Protected Access Pre-Shared Key（認証・暗号化方式のWi-Fi標準セキュリティ規格のひとつ）
WPA3-SAE	Wi-Fi Protected Access Simultaneous Authentication of Equal（認証・暗号化方式のWi-Fi標準セキュリティ規格のひとつ）
アグリゲーションコントローラー	需要家の電力の需要と供給のバランスを制御するコントローラー
スマートメーター（SM）	本仕様書では、下位レイヤにおいて、JJ-300.10v2方式A（高圧・低圧のスマートメーター）、2.4GHz帯無線LAN（低圧スマート

	メーター）、IEEE802.3方式（高圧スマートメーター）に対応し、上位レイヤにおいて、ECHONET Lite(EL)が定める双方向対応高圧スマート電力量メータ若しくは、低圧スマート電力量メータとしてECHONET Lite AIF仕様に正しく適合していることを証明する認証(EL AIF認証)を取得したノードを言う。

5. 技術レポート作成部門

第２．０版　：　IoTエリアネットワーク専門委員会 (WG3600)

6. 本技術レポートの制作体制

本ガイドラインは、 IoTエリアネットワーク専門委員会 (WG3600) (委員長美原義行)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、2025年に導入が開始される次世代スマートメーター（以下、スマートメーター）とEMS・アグリゲーションコントローラー間の通信、いわゆるBルートについて、アグリゲーション等新たなサービスを実現するECHONET LiteによるBルートアプリケーション通信を円滑に実現することを目的とした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、スマートメーターが、低圧/高圧のスマートメーターで共通に利用可能な通信メディアとして920MHz帯無線（[JJ-300.10v2方式A] 、低圧スマートメーターで利用可能なメディアとしてIEEE802.11n（/ax）（2.4GHz帯無線LAN）、高圧スマートメーターで利用可能なメディアとしてIEEE 802.3方式を用いる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、 IoTエリアネットワーク専門委員会(WG3600)　事務局へご連絡をいただきたい。

第1章　共通仕様

1.1　概要

本ガイドラインでは、スマートメーターは、下位レイヤにおいて、JJ-300.10v2方式A（高圧・低圧のスマートメーター）、2.4GHz帯無線LAN（低圧スマートメーター）、IEEE802.3方式（高圧スマートメーター）に対応し、上位レイヤにおいて、ECHONET Lite(EL)が定める双方向対応高圧スマート電力量メータ若しくは、低圧スマート電力量メータとしてECHONET Lite AIF仕様に正しく適合していることを証明する認証(EL AIF認証)を取得したノードを言う。

また、EMS・アグリゲーションコントローラー（以下、コントローラー）は、下位レイヤにおいて、JJ-300.10v2方式A（高圧・低圧のスマートメーター）、2.4GHz帯無線LAN（低圧スマートメーター）、IEEE802.3方式（高圧スマートメーター）に対応し、上位レイヤにおいて、ELが定める双方向対応高圧スマート電力量メータ若しくは、低圧スマート電力量メータとの接続に関するEL AIF認証を取得したノードを言う、

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コントローラーは１：N（N=最大3）で接続される構成とし、スマートメーターがコントローラーを認証した後に接続させるために、両者の間の無線通信はJJ-300.10v2方式A、2.4GHz帯無線LAN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。詳しくは、以下に定める。

- ○ 高圧・低圧のスマートメーター共に JJ-300.10v2 方式 A においては、最大接続台数は、コントローラー1 台とする。
- ○ 低圧のスマートメーターで 2.4GHz 帯無線 LAN で接続する場合は､最大 3 台のコントローラーが、1 台の低圧スマートメーターへ接続できるものとする。また、同一の 2.4GHz 帯無線 LAN に複数の低圧スマートメーターが接続された場合も、各低圧スマートメーターに対し、最大３台のコントローラーが接続できるものとする。
- ○ 高圧のスマートメーターで IEEE802.3 方式で接続する場合は、最大 3 台のコントローラーが、1 台の高圧スマートメーターへ接続できるものとする。また、同一の IEEE802.3 方式をサポートするスイッチングハブ等通信機器に複数の高圧スマートメーターが接続された場合も、各高圧スマートメーターに対し、最大３台のコントローラーが接続できるものとする。

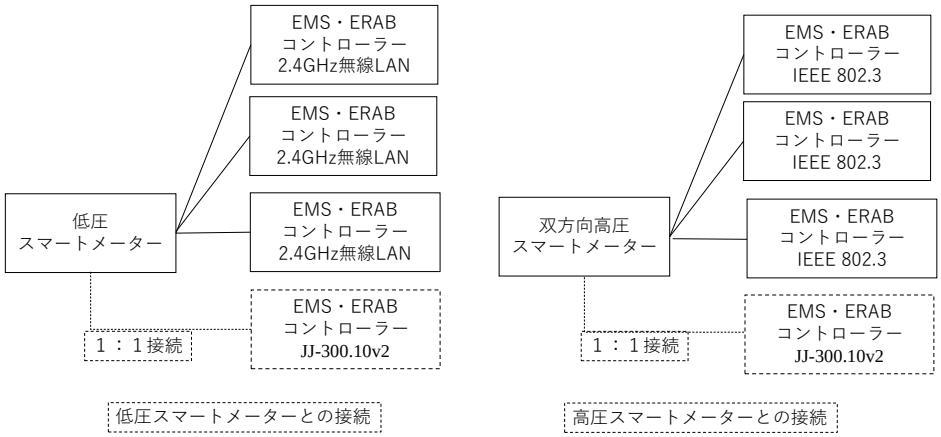


図 1-1 1:N 接続

資源エネルギー庁次世代スマートメーター制度検討会EMS・アグリゲーションコントローラースマートメーターBルート(高圧スマート電力量メーター)運用ガイドライン［第2.0版］（GL-H）、同(低圧スマ

ート電力量メーター)運用ガイドライン［第5.0版］（GL-L）は、第10章セキュリティの基本要件において、「AルートとBルートはアイソレーションされた設計とする。アイソレーションの定義は、IPパケットの転送機能は持たせず、ネットワークドメインを分離することとする。」と定義している。

尚、高圧・低圧のスマートメーター共にデータアクセス品質の安定性をベストエフォート方式で構築する。また、高圧・低圧のスマートメーター共にIPアドレス若しくは物理アドレスを用いた端末認証を行わない、接続タイムスタンプを用いた接続制御は実装されない、実装とする。安定したデータ転送を実現するためには、スマートメーターBルートのユーザーが、本ガイドラインが定める最大同時接続数やアクセス頻度のルールを順守することが求められる。

1.2 ID および認証鍵

スマートメーター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、資源エネルギー庁次世代スマートメーター制度検討会EMS・アグリゲーションコントローラースマートメーターBルート(高圧スマート電力量メーター)運用ガイドライン［第2.0版］（GL-H）、同(低圧スマート電力量メーター)運用ガイドライン［第5.0版］（GL-L）に記載されているBルート認証ID・パスワードの定義に基づき、表 1 1に定める。

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EMS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では[EAP]で使用するIDやネットワーク識別子に変換され、2.4GHz帯無線LAN方式ではWPA2-PSKおよびWPA3-SAE※で使用するPSK Identityやネットワーク識別子に変換して利用する。※WPA3への対応は任意とする。2022/12/01以降に取得するすべてのWi-Fi認証機器は、WPA3の取得が必須（WPA2はオプションとして追加取得可能）となっている。
（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2.4GHz帯無線LAN方式でPSKを生成するために使用される。

また、スマートメーターBルートのユーザーは、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EMS・アグリゲーションコントローラー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する。これらID・パスワードの配布方法に関しては、（GL-H）（GL-L）等を参照すること。

なお、Bルート認証IDとパスワードはお客さまに通知されているものであり、通信部交換において認証ID・パスワードが変更されるものではない。

1.3 アプリケーション

アプリケーション層として、ECHONET Liteを使用する。ECHONET Lite接続に関する詳細は、双方向対応高圧スマート電力量メータ・コントローラー間アプリケーション通信インタフェース仕様書Version 1.00、低圧スマート電力量メータ・コントローラー間アプリケーション通信インタフェース仕様書Version 1.10等最新版に準拠する。本書記載の仕様に基づくノードは、ECHONET機器オブジェクト詳細規定Release R に規定される必須プロパティ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下位層のリンク確立後(認証処理がある場合は認証処理後)とする。

1.3.1 アプリケーションレベルにおける要求頻度

アプリケーションレベルでの要求頻度は、アグリゲーターがその供出リソースの監視及び制御の用途に用いる用務を満たしたうえで、節度あるものとすべきである。例えば、アグリゲーターからは、制御対象リソースに対して10秒周期での高速フィードバックを行うために6秒周期でのスマートメーターからのデータ取得を必要としていることが報告されている。

一方、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。ELの低圧スマート電力量メータ・コントローラー間アプリケーション通信インタフェース仕様書Version 1.10[SHIF-L1.10]、双方向対応高圧スマート電力量メータ・コントローラー間アプリケーション通信インタフェース仕様書Version 1.00[SHIF-H1.00]は、以下のように規定する。

- ○ 「1 台のスマート電力量メータは、最大 3 台（通信頻度：10[sec]×1 台、30[sec]×1 台、30[min]×1 台）までのコントローラーとの通信をサポートし、ベストエフォートで対応する。」　引用元「2.4.1 項　連続要求[SHIF-L1.10] [SHIF-H1.00]」
- ○ コントローラー応答待ちタイマー　20[sec]以上(表 1-2, 1-3 参照)　尚、コントローラーの応答待ちタイマー値は、低圧スマート電力量メータ若しくは双方向対応高圧スマート電力量メータからの要求に対してコントローラーより応答が無い場合に、スマート電力量メータが次の要求を行うことができるまでの待ち時間を規定するものである。引用元 「2.4.2 項　応答待ちタイマー[SHIF-L1.10] [SHIF-H1.00]」

表 1-2 コントローラーの応答待ちタイマー（低圧電力量メータクラス）

応答待ちタイマー1	20 [sec]以上	OPC 数 1 の場合 ただし、以下の EPC の場合は除く。 ・EPC＝0xE2 積算電力量計測値履歴1（正方向計測値） ・EPC＝0xE4 積算電力量計測値履歴1（逆方向計測値） ・EPC＝0xEC 積算電力量計測値履歴2（正方向、逆方向計測値） ・EPC＝0xEE 積算電力量計測値履歴 3（正方向、逆方向計測値）
応答待ちタイマー2	60 [sec]以上	OPC 数 2 以上の場合、または以下の EPC の場合。 ・EPC＝0xE2 積算電力量計測値履歴1（正方向計測値） ・EPC＝0xE4 積算電力量計測値履歴1（逆方向計測値） ・EPC＝0xEC 積算電力量計測値履歴2（正方向、逆方向計測値） ・EPC＝0xEE

		積算電力量計測値履歴 3(正方向、逆方向計測値)

表 1-3 コントローラーの応答待ちタイマー(双方向対応高圧電力量メータクラス)

パラメータ名	値	備考
応答待ちタイマー1	40[sec]以上	OPC数1の場合 ただし、以下のEPCの場合は除く。 ・EPC=0xE7 積算有効電力量計測値履歴(正方向計測値) ・EPC=0xE8 積算有効電力量計測値履歴(逆方向計測値) ・EPC=0xC6 需要電力計測値履歴(正方向計測値) ・EPC=0xC8 需要電力計測値履歴(逆方向計測値) ・EPC=0xCE 力測積算無効電力量(遅れ)計測値履歴(正方向計測値) ・EPC=0xCF 力測積算無効電力量(遅れ)計測値履歴(逆方向計測値) ・EPC=0xED 積算有効電力量計測値履歴2(正方向、逆方向計測値)
応答待ちタイマー2	180[sec]以上	OPC数2以上の場合、または以下のEPCの場合。 ・EPC=0xE7 積算有効電力量計測値履歴(正方向計測値) ・EPC=0xE8 積算有効電力量計測値履歴(逆方向計測値) ・EPC=0xC6 需要電力計測値履歴(正方向計測値) ・EPC=0xC8 需要電力計測値履歴(逆方向計測値) ・EPC=0xCE 力測積算無効電力量(遅れ)計測値履歴(正方向計測値) ・EPC=0xCF 力測積算無効電力量(遅れ)計測値履歴(逆方向計測値) ・EPC=0xED 積算有効電力量計測値履歴2(正方向、逆方向計測値)

スマート電力量メータ及びコントローラーは、要求と応答を1セットとし、ひとつの要求に対してひとつの応答を返す。コントローラーは、要求に対応する応答を受信した場合、応答待ちタイマーの満了を待たず次の要求を行うことが可能である。一方、要求に対する応答を受信できない場合は、コントローラーは応答待ちタイマーの満了後に次の要求を行うことが可能である。なお、[SHIF-L1.10] [SHIF-H1.00]は、1:1通信に対する規定であり、連続要求とは同一装置からの要求が連続する場合を示す。1台のスマート電力量メータは、最大3台(通信頻度:10[sec]×1台、30[sec]×1台、30[min]×1台)までのコントローラーとの通信をサポートし、ベストエフォートで対応する。

[SHIF-L1.10] [SHIF-H1.00]において連続要求が定める値を上回るアクセス（但し、現行のスマート電力量メータクラスのデータ提供品質を損なわない）、同コントローラーの応答待ちタイマー値を下回るアクセス（概ね5割以上）、コントローラーからの同時アクセスがDoS/DDoS攻撃とみなされる場合は、一定時間（10分間程度）、EMS・アグリゲーションコントローラーからの要求には無応答となる場合がある。

例えば、複数のコントローラーが通信頻度10[sec]未満での通信を行った場合は、DoS/DDoS攻撃とみなされる場合がある。但し、コントローラーが前回のアクセス要求への返信の受信後や応答待ちタイマーが切れた後に、新たに要求するアクセスはDoSと見做さない。

また、スマートメーターは、低圧、高圧ともに、１対１接続のWi-SUN以外は、全てのコントローラーは、宅内AP等ユーザー管理のネットワーク機器配下となることを想定する（ユーザーが宅内APを設置し、同時接続数等を宅内APで管理する。宅内APを設置せず、SMをAP動作させ複数のEMSコントローラーを直接収容する形態は想定していない）。情報管理の観点からお客さまの機器情報をスマートメーター側のフィルタリング情報として使用しない。

1.3.2 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、EMS・アグリゲーションコントローラー側は再度接続処理を行っても良い。JJ-300.10v2方式Aの場合はスマートメーター側は該当PANAセッションを、2.4GHz帯無線LANの場合はアソシエーションを切断する。

920MHz無線の場合、スマートメーター及びEMS・アグリゲーションコントローラーは、前回使用時の無線チャネル(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。

2.4GHz帯無線LAN及びIEEE802,3方式の場合、スマートメーターは過去の接続の認証結果を保管する機能を持たない。

コントローラーは、高圧・低圧共にスマートメーターが離脱することを踏まえて設計し、双方向対応高圧スマート電力量メータクラス、若しくは、低圧スマート電力量メータクラスにおけるECHONET Lite通信において生存を確認する。それでも生存が確認できなくなった場合、JJ-300.10v2を使用しているならば、スマートメーターに対して、再接続をするべきである。再接続は、下記の 1) から 5) のいずれかの段階から行うことが想定される。しかし、1)から5)に向かうほど、再接続の時間がかかることが想定される。

1) PANA再認証
2) PANA初回認証
3) Enhanced Beacon Request
4) IPv6 層の Neighbor Solicitation - Advertisement
5) 全Channel のActive Scan

1.3.3 スマートメーターの生存確認ができない等課題への対応

生存確認は、スマートメーター側は、コントローラーの生存確認を行わないこと。コントローラーは、本ガイドラインが規定するネットワーク層以下ではなく、アプリケーション層においてECHONET Liteコマンド（Get[0x80]等）で行なうこと。ECHONET Lite システム設計指針第2版[EL-SDG2]第６章スマート電力量メータ AIF 仕様に関する実装事例と指針においては、スマートメーターの生存を確認することができない等、現行スマートメーターの接続上の課題と課題解決への期待する動作が明示されている。参照されたい。

1.3.4 コントローラーの置き換えに対する対応

現行のスマートメーターにおいては、古いコントローラーを、新しいコントローラーに置き換える際、スマートメーターが、何らかの制約や手続きが必要な仕様だった結果、ユーザーに不必要な混乱を招いた事例が報告される。具体的な報告例としては以下の１）～３）が例示される。

１） 一旦、B ルート接続をすると、切断処理をしない限り、次のコントローラーに接続できないケース。（一般的なユーザーは、切断手続きをせずに、古いコントローラーを外してしまうため、新しいコントローラーに接続できないという事象となってしまう。）

２） スマートメーターの1 次側電源を10 秒以上切らないと、次のコントローラーを接続できないケース。（家庭の主電源を落とすことになるため、現実的には、実施困難となる。）

３） Bルート接続が途切れて24 時間以上空かないと、次のコントローラーを接続できないケース。（いつ新しいコントローラーを付けられるようになるか、ユーザが把握できないことになってしまう。）

そこで、スマートメーターは、以下の対応を行うこと。

ア）上記事例１） ２） ３）のような実装は行わない。

イ）後から接続のコントローラーが優先されるような実装は行わない。（台数制限はそもそもベストエフォートなので、スマートメーター側から接続を切る機能は有しない。）

一方、コントローラー側は、以下の項目を推奨機能として実装すること。

ア）複数のコントローラーが同時に存在した場合、複数のコントローラーが、スマートメーターを交互に取り合うような事態が起きることが想定される。従って、コントローラーは、複数コントローラー存在時に、交互にスマートメーターを取り合わないようにするための仕組み（自動接続機能を外すことを可能とする等）を持つことが推奨される。

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EMS・アグリゲーションコントローラー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。

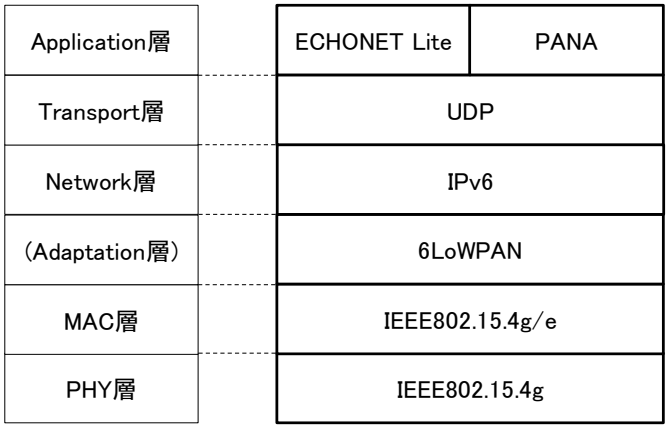
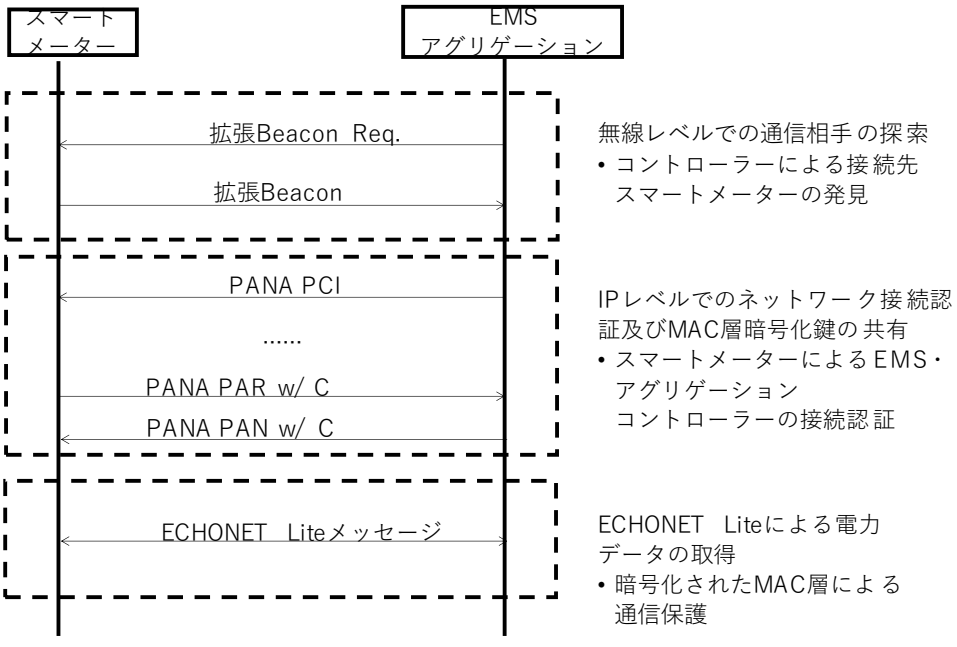


図 2-1 920MHz(JJ-300.10 方式 A:Wi-SUN)スタック図

図2-2に接続シーケンスの概要を示す。



※Bルート認証IDの下4桁をビーコンでブロードキャストしている

図 2-2 接続シーケンス

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、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方式A]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方式A]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方式A]の5.9.4.3.3に従う。

2.6 トランスポート層

[JJ-300.10v2方式A]の5.9.4.4に従う。

2.7 セキュリティ処理

[JJ-300.10v2方式A]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。

コントローラーは、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。コントローラーが送信する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、コントローラーからの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、コントローラーは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

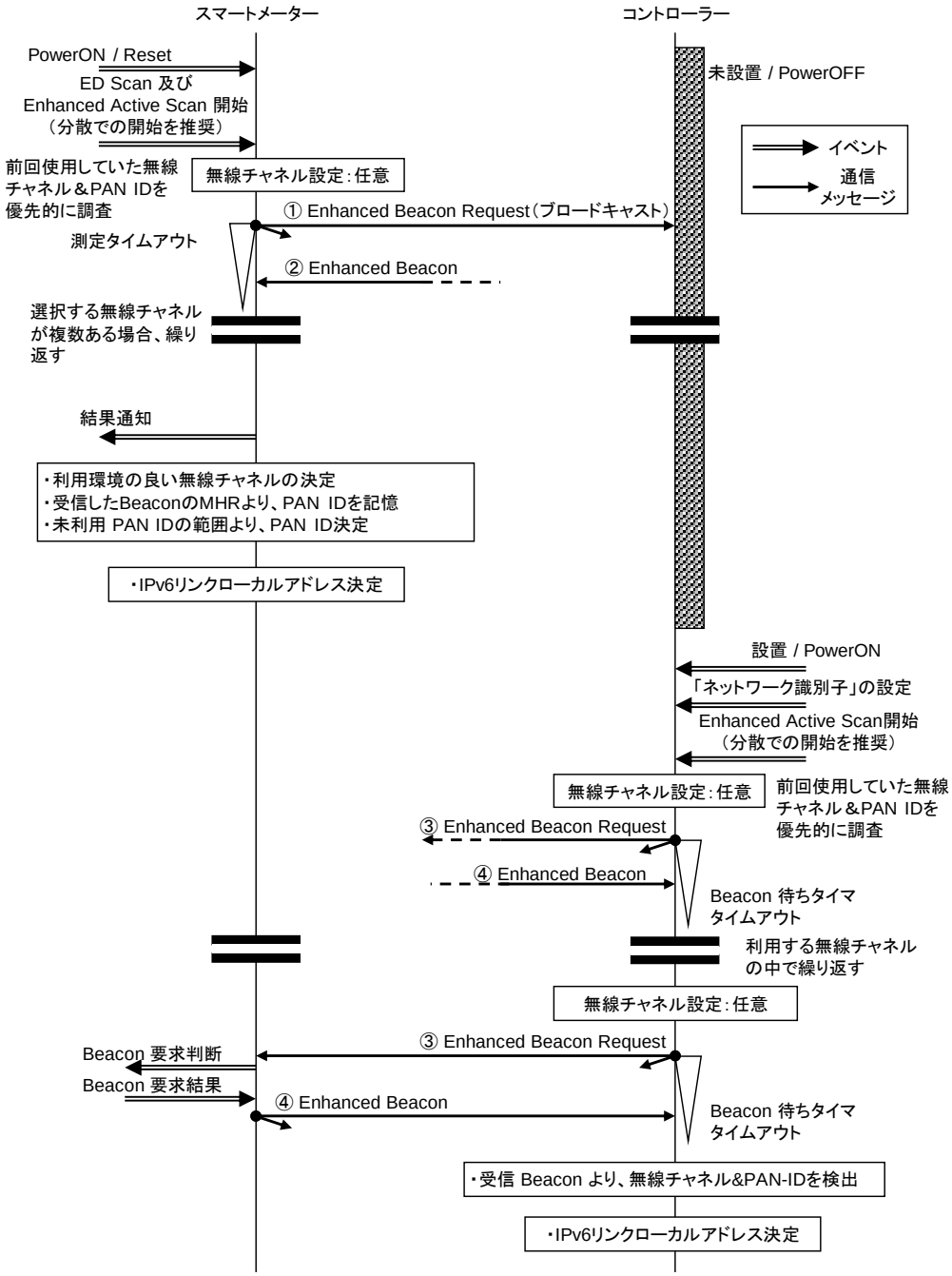


図 2-3 MAC 処理

（2）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:コントローラー)

<table>
<tr><td colspan="4">パラメータ名</td><td>内容</td><td>値</td><td>備考</td></tr>
<tr><td colspan="4">送信元</td><td>コントローラー</td><td>“64bitアドレス”</td><td></td></tr>
<tr><td colspan="4">宛先</td><td>ブロードキャスト</td><td>0xFFFF</td><td></td></tr>
<tr><td colspan="4">Information Elements（IEs）フィールド</td><td></td><td></td><td></td></tr>
<tr><td></td><td colspan="3">Header IEs</td><td>利用しない</td><td>－</td><td></td></tr>
<tr><td></td><td rowspan="6">Payload IEs</td><td rowspan="4">MLME IE</td><td rowspan="2">Outer IE descriptor</td><td>Length</td><td>0x0a</td><td>IE Content長</td></tr>
<tr><td>Group ID</td><td>0x1</td><td>MLME</td></tr>
<tr><td></td><td>Type</td><td>0x1</td><td></td></tr>
<tr><td rowspan="3">Sub-IE descriptor</td><td>Length</td><td>0x8</td><td>Sub-IE Content長</td></tr>
<tr><td>Sub-ID</td><td>0x68</td><td>ネットワーク識別子用</td></tr>
<tr><td>Type</td><td>0x0</td><td></td></tr>
<tr><td></td><td></td><td></td><td>Sub-IE Content</td><td>ネットワーク識別子</td><td>8 octets長</td></tr>
<tr><td></td><td></td><td colspan="2" rowspan="2">List termination</td><td>Length</td><td>0x0</td><td></td></tr>
<tr><td></td><td></td><td></td><td>Group ID</td><td>0xf</td><td>Payload IEの終了を示す</td></tr>
</table>

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				コントローラー	“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方式A]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]	EMS･アグリゲーションコントローラー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　2.8.1.1 Enhanced Beacon Request 最大送信回数

コントローラーからの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コントローラーは、 [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

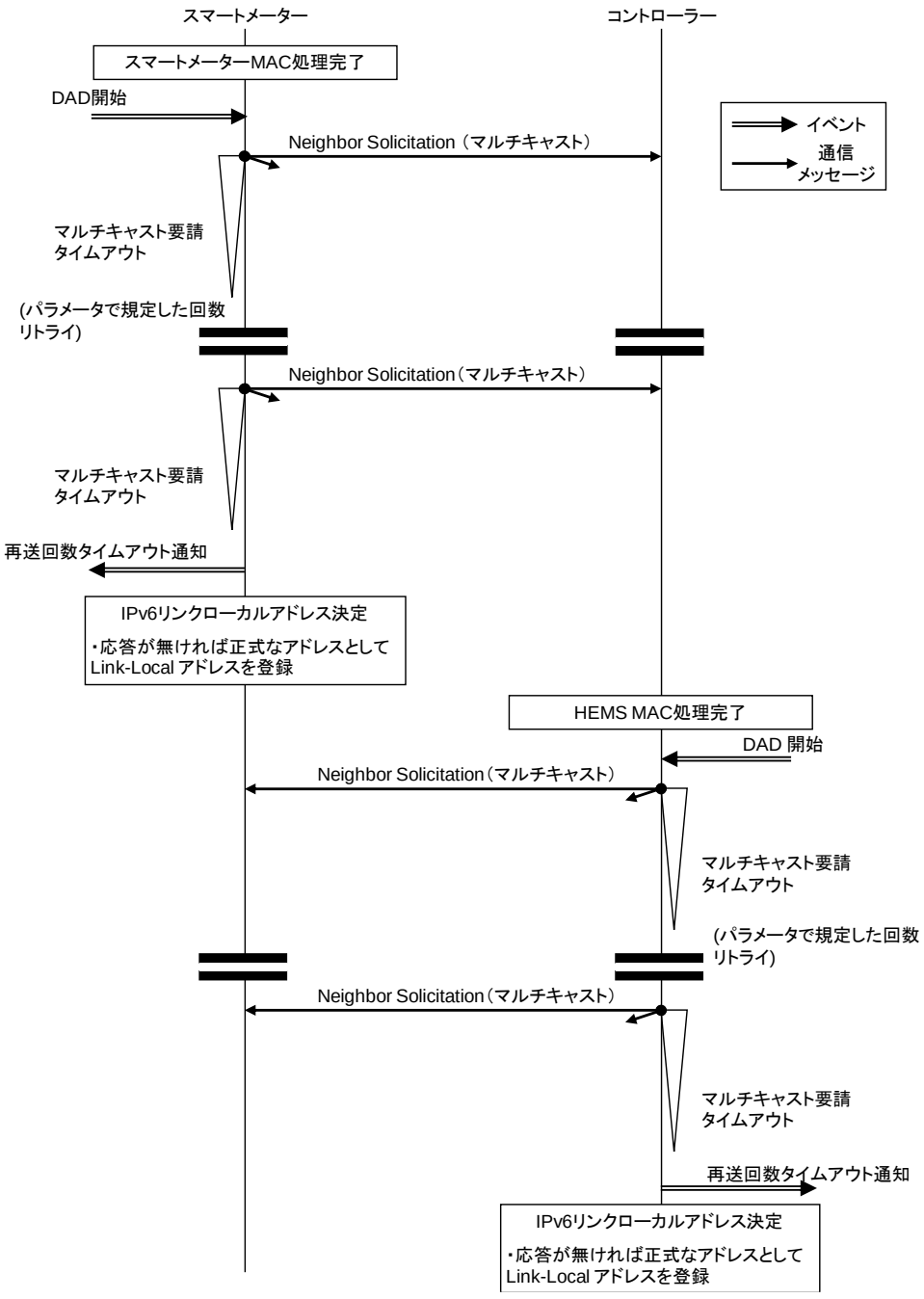


図 2-4 DAD処理

（2）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

コントローラー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

コントローラー（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EMS・アグリゲーションコントローラーが設置され、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

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。

ズによってPANAのセッションが終了した後と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(コントローラー)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。

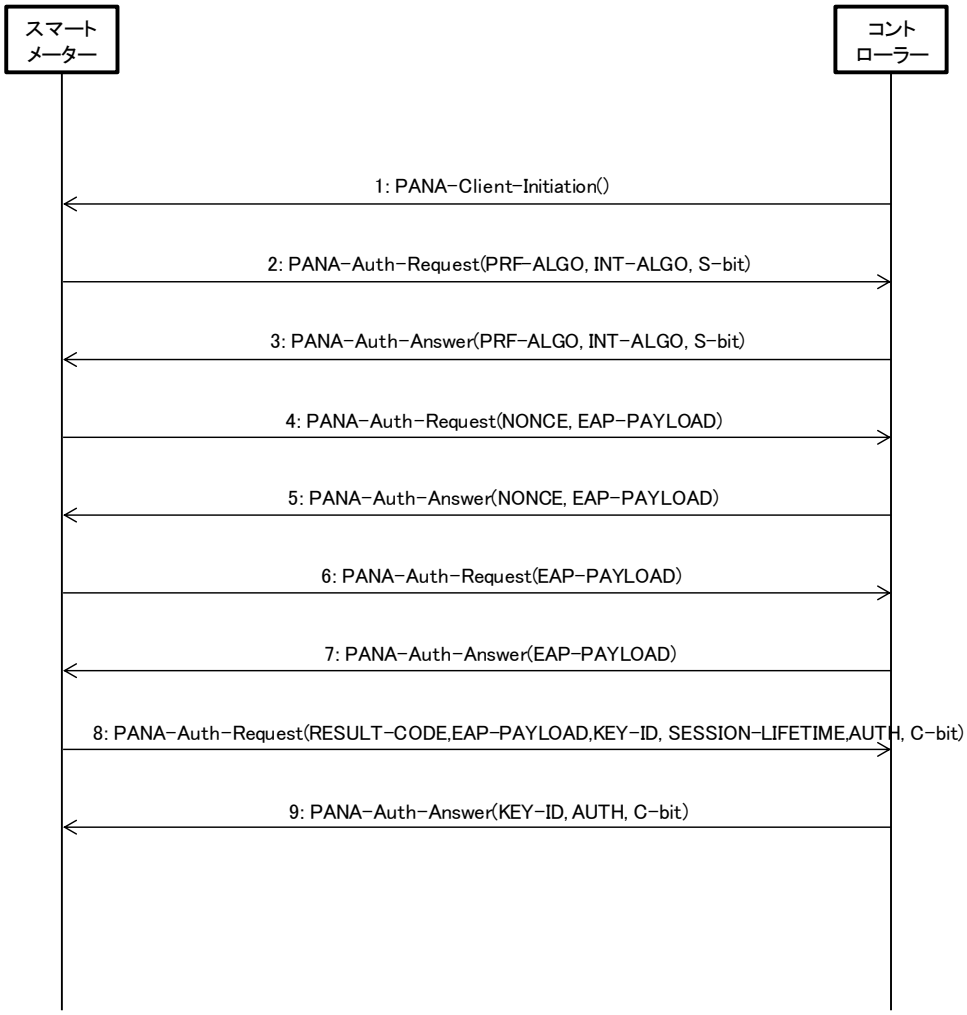


図 2-5 Authentication and Authorization フェーズ

2.8.3.1.2 Access Phase

スマートメーターとの通信が有効かを確認する方法として、ICMPv6のEcho Request – Echo Replyを使用してよい。

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 2-6に示す。

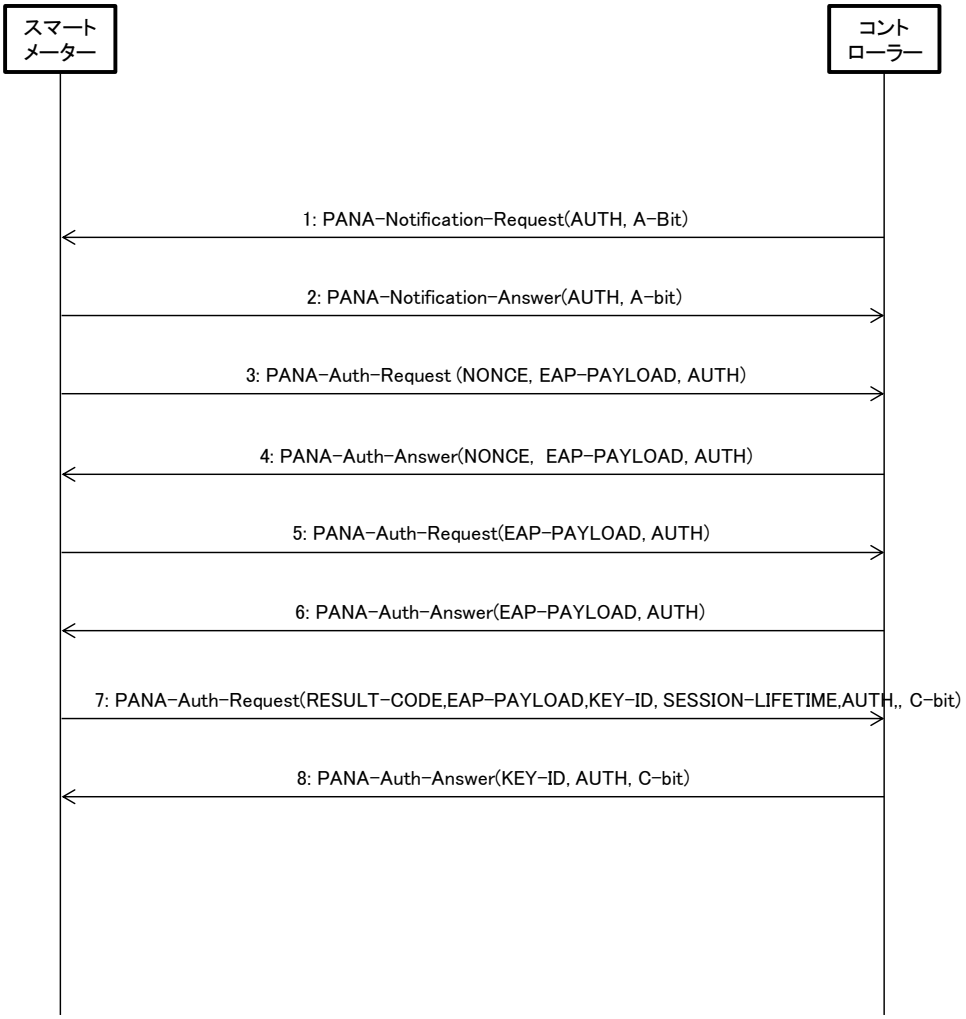


図 2-6 PANA Re-authentication フェーズシーケンス

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。

コントローラー（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 2-7に例示する。

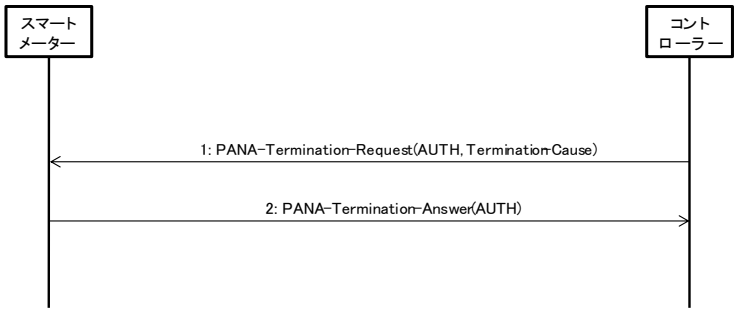


図 2-7 PANA Termination フェーズシーケンス

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。コントローラーがPANAリクエスト送信側の場合、コントローラー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。コントローラー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）コントローラー（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、当該コントローラーとの間の古い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コントローラーへPTRを送信しなくてもよい）。またこの時、同一のコントローラー（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コントローラー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（コントローラー）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（コントローラー）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。

2.9　処理シーケンス

2.1項 概要 図 2 2　接続シーケンスを参照のこと。

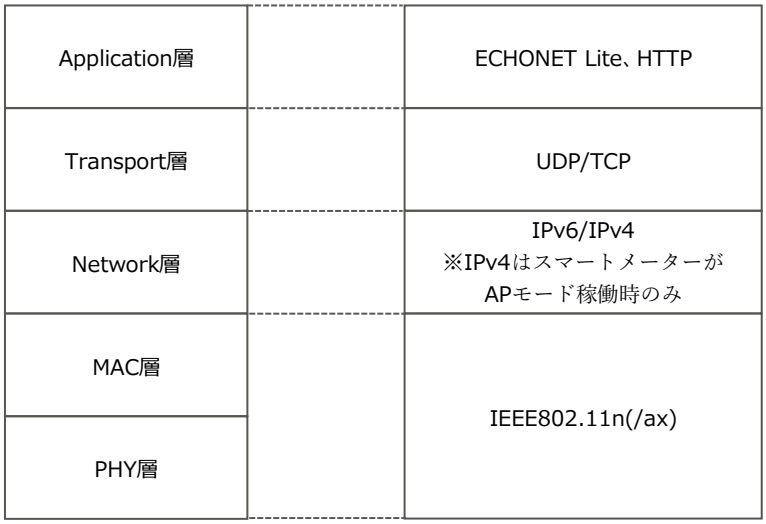
IP 層以降の接続シーケンスに関しては、[SHIF-H1.00]及び[SHIF-L1.10]を合わせて参照する。

第3章　2.4GHz帯無線LAN用Bルート下位レイヤ実装

3.1　概要

本仕様で述べるスタック図を示す。2.4GHz帯無線LAN規格上にIPv6を動作させ、UDPおよびHTTPによるデータ通信、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 3-1 2.4GHz 帯無線 LAN におけるスタック図



一般的に2.4GHz帯無線LAN利用においては、干渉等で通信が困難な場合が存在する。これら本方式での通信特性は、総務省「Wi-Fi提供者向けセキュリティ対策の手引き（令和2年5月版）https://www.soumu.go.jp/main_content/000690267.pdf」を参考にされたい。

3.2　物理層

2.4GHz 帯無線 LAN における物理層仕様を示す。本仕様は IEEE802.11 で定義された PHY 仕様を採用し、技術基準適合証明の取得を前提とする。

表 3-12.4GHz 帯無線 LAN 方式規格

項目	仕様
準拠規格	IEEE802.11n(/ax)※1
周波数帯	2.4GHz
チャネル	1～13ch(2412～2472MHz)
伝送方式	IEEE802.11n : OFDM方式 (IEEE802.11ax : OFDM方式、OFDMA方式)※1
最大伝送速度※2	2.4GHz: IEEE802.11n : 600Mbps(40MHz 4×4) (IEEE802.11ax: 2.3Gbps(40MHz 8×8))※1
変調方式	IEEE802.11n:BPSK,QPSK,16QAM,64QAM (IEEE802.11ax:BPSK,QPSK,16QAM,64QAM,256QAM,1024QAM)※1
アクセス方式	CSMA/CA

※1.IEEE802.11ax への対応は任意とする。

※2.規格上の最大スペックを示す。

3.3 MAC 層

MAC層の仕様については、IEEE802.11n、またはIEEE802.11ax※で規定する”AP”または”STA”とし、通信仕様は、同Mandatory仕様に準拠する。なお、スマートメーターおよびコントローラーは、IEEE802.11n、またはIEEE802.11ax※のMandatory仕様において、以下表3－2の機能に限定する。

表 3-2　MAC 層機能の特記事項

機能	値	備考
認証方式	WPA2-PSK、(WPA2-PSK/WPA3-SAE)※	WPA-PSKは使用禁止とする。
暗号方式	AES	TKIPは使用禁止とする。
ANY接続	拒否を有効とする	APモードの時のみサポートする。
SSID	ステルス機能	スマートメーターのAPモードは、ステルスモード(Beacon停止)とする。

※WPA3への対応は任意とする。2022/12/01以降に取得するすべてのWi-Fi認証機器は、WPA3の取得が必須（WPA2はオプションとして追加取得可能）となっている。

3.3.1 フレームフォーマット概要

MACフレームフォーマット概要を以下に示す。

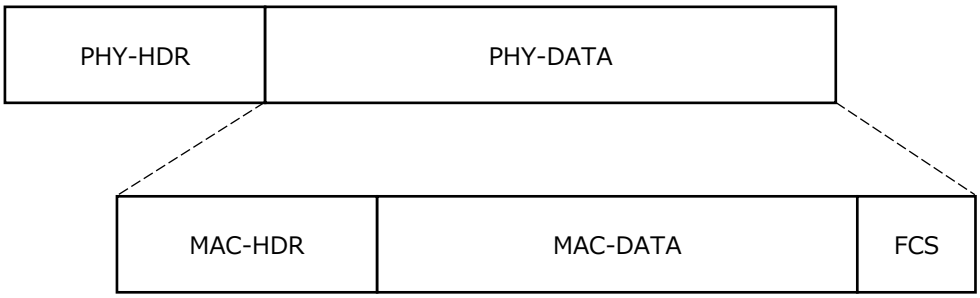


図 3-2　MAC フレームフォーマット

MAC-HDR領域のManagementフレーム（Beaconフレーム）には、ネットワーク情報としてSSIDが含まれる。

Beaconフレーム含めその他のフレームの詳細はIEEE802.11「9.3.3 Management frames」を参照のこと。

3.4 ネットワーク層

インタフェース部におけるネットワーク層は、[IPv6]で定義するIPv6プロトコルをベースに表3-3に示す項目を実装しなければならない。

表 3-3 IPv6 プロトコル

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	-	Y
IP1.2	Extension Header Order	[IPv6] 4.1	Y
IP1.3	Options	[IPv6] 4.2	Y
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	[IPv6-SAA]	O
IP1.10	ESP Header	[IPv6-MIB]	O
IP2	Deprecation of Type 0 Routing Headers	[IPv6-RH]	Y
IP3	Path MTU Discovery	[IPv6] 5	Y
IP4	Flow Labels	[IPv6] 6	Y
IP5	Traffic Classes	[IPv6] 7	Y

※1: Y:サポート必要、N:サポート不要、O:オプション(任意)

また、表3-4に示すICMPv6をサポートしなければならない。メッセージ種別としては、エコー要求(タイプ128)およびエコー応答(タイプ129)に加え、宛先未到達(タイプ1)、時間超過(タイプ3)およびパラメータ問題(タイプ4)の各エラーメッセージもサポートしなければならない。パケットサイズ超過(タイプ2)メッセージに関しては、送信機能を持たなくてもよいが受信した際は適切に処理されなければならない。

表 3-4 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
ICMP6	Packet Too Big Message	[ICMP6] 3.2	Y
ICMP7	Time Exceeded Message	[ICMP6] 3.3	Y
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: Y:サポート必要、N:サポート不要、O:オプション(任意)

3.5 IP アドレス

表 3-5に示す項目を実装しなければならない。本方式で定義するネットワークでは、プレフィックスとしてwell known link-local prefix FE80::0/64を使用する。なお、グローバルアドレスとユニークローカルアドレスは、本標準内では使用しない。

IPv6については、表 3 5に従い、ICMPv6については、表 3 6に従うこと。リンクローカルアドレスのインタフェースID(下位64ビット部分)については、任意とする。その際、プレフィックスとしてwell known link-local prefix FE80::0/64を使用する。

表 3-5 IPv6 アドレス

項番	概要	参照番号	サポート有無 ※1
IPAD1	IPv6 Addressing	[IP6ADDR]	Y (#1)
IPAD1.1	Global Unicast Address	[IP6ADDR] 2.5.4	N
IPAD1.2	Link Local Unicast	[IP6ADDR]	Y

	Address	2.5.6	
IPAD1.3	Unique Local Unicast Address	[ULA]	N
IPAD1.4	Anycast Address	[IP6ADDR] 2.6	N
IPAD1.5	Multicast Address	[IP6ADDR] 2.7	Y (#2)
IPAD1.6	Prefix Length		/64
IPAD2	Stateless Address Autoconfiguration	[SLAAC]	Y
IPAD2.1	Creation of Link Local Address	[SLAAC] 5.3	Y
IPAD2.2	Creation of Global Addresses	[SLAAC] 5.5	N

※1: Y:サポート必要、N:サポート不要、O:オプション(任意)

(#1) (#2) 一部機能は使用しない

3.5.1 ユニキャストアドレス

スマートメーター及びコントローラーは、自装置アドレスとしてリンクローカルアドレスを生成し、リンクローカルアドレスを使用したIPv6通信を行う。リンクローカルアドレスのインタフェースID(下位64ビット部分)については、任意とする。

3.5.2 マルチキャストアドレス

IPv6の近隣探索で要請ノードマルチキャストアドレス(solicited-node multicast address)を使用する。また、ECHONET Lite電文のマルチキャスト送信時は、ECHONET Lite仕様[EL]の規定に従いff02::1を宛先として設定する。なお、エニーキャストアドレス(anycast address)は使用しない。

3.6 近隣探索

近隣探索は、IPv6向けに定義されたRFC 4861 [ND]を使用する。[ND]を使用する場合、実装しなければならないIPv6のNeighbor discoveryの必須項目を表3-6に示す。[ND]が定義する機能のうち、本方式規定に従うノードがサポートしなければならない機能は、アドレス解決、重複アドレス検出の2機能である。また、[ND]に定義されているICMPv6メッセージのうち、本方式規定に従うノードがサポートしなければならないメッセージは、近隣要請メッセージ(Neighbor Solicitation message: Type = 133)と近隣応答メッセージ(Neighbor Advertisement message: Type = 134)の2つである。なお、近隣探索のエントリ数は、３以上とすること。

表 3-6 近隣探索

Item number	Item description	Support (Y:Yes, N:No, O:Option)	Notes

ND1	Router and Prefix Discovery	[ND]6	N
ND2	Address Resolution	[ND] 7.2	Y
ND3	Neighbor Unreachability Detection	[ND] 7.3	N
ND4	Duplicate Address Detection	[SLAAC] 5.4	Y
ND5	Redirect Function	[ND] 8	N
ND6	Router Solicitation Message	[ND]4.1	N
ND7	Router Advertisement Message	[ND] 4.2	N
ND8	Neighbor Solicitation Message	[ND] 4.3	Y
ND9	Neighbor Advertisement Message	[ND] 4.4	Y
ND10	Redirect Message	[ND] 4.5	N
ND11	Source/Target Link-layer Address Option	[ND] 4.6.1	Y
ND12	Prefix Information Option	[ND] 4.6.2	N
ND13	Redirected Header Option	[ND] 4.6.3	N
ND14	MTU Option	[ND] 4.6.4	N

※1: Y:サポート必要、N:サポート不要、O:オプション(任意)

3.7 トランスポート層

トランスポート層として、UDPとTCPをサポートする。表3-7と表3-8にサポートするポート番号を示す。

表 3-7 UDP ポート番号

プロトコル	ポート番号	概要
UDP	3610	ECHONET Lite で使用するポート番号

表 3-8 TCP ポート番号

プロトコル	ポート番号	概要
HTTP	80	WEB 認証で使用するポート番号(HTTPS は未サポート)

3.8 セキュリティ処理

本仕様では、通信セキュリティとして認証方式にWPA2-PSKおよびWPA3-SAE※、暗号化方式にAESを用いた通信の保護を実施する。

※WPA3への対応は任意とする。2022/12/01以降に取得するすべてのWi-Fi認証機器は、WPA3の取得が必須（WPA2はオプションとして追加取得可能）となっている。

3.9 認証・暗号

認証方式での必須項目を表 3-9に示す。WPA2-PSKを必須とし、WPA3-SAEを任意で採用する。WPA3をサポートする場合、WPA2/WPA3のどちらも選択できるようにすること。

表 3-9 認証方式

認証方式	サポート有無※1
オープン認証	N
SHARED認証	N
WPA-PSK	N
WPA-Enterprise	N
WPA2-PSK	Y
WPA2-Enterprise	N
WPA3-SAE	O ※
WPA3-Enterprise	N
IEEE802.1X認証	N

※1: Y:サポート必要、N:サポート不要、O:オプション(任意)

※2022/12/01以降に取得するすべてのWi-Fi認証機器は、WPA3の取得が必須（WPA2はオプションとして追加取得可能）となっている。

暗号方式での必須項目を表 3-10に示す。AES暗号を必須とする。

表 3-10 暗号方式

暗号方式	サポート有無※1
WEP暗号	N
TKIP暗号	N
AES暗号	Y

※1: Y:サポート必要、N:サポート不要、O:オプション(任意)

3.9.1 WPA2-PSK(AES)

IEEE802.11iに準拠したWPA2認証かつAES暗号化をサポートする。ユニキャスト鍵(PTK)およびマルチキャスト鍵(GTK)ともに4WAYハンドシェイクにて交換される。さらに、マルチキャスト鍵については定期更新を行うことでセキュリティが高められ、マルチキャスト用の鍵更新シーケンスとして2WAYハンドシェイクが定期的に繰り返される。WPA2-PSK認証の接続シーケンスを以下に示す。

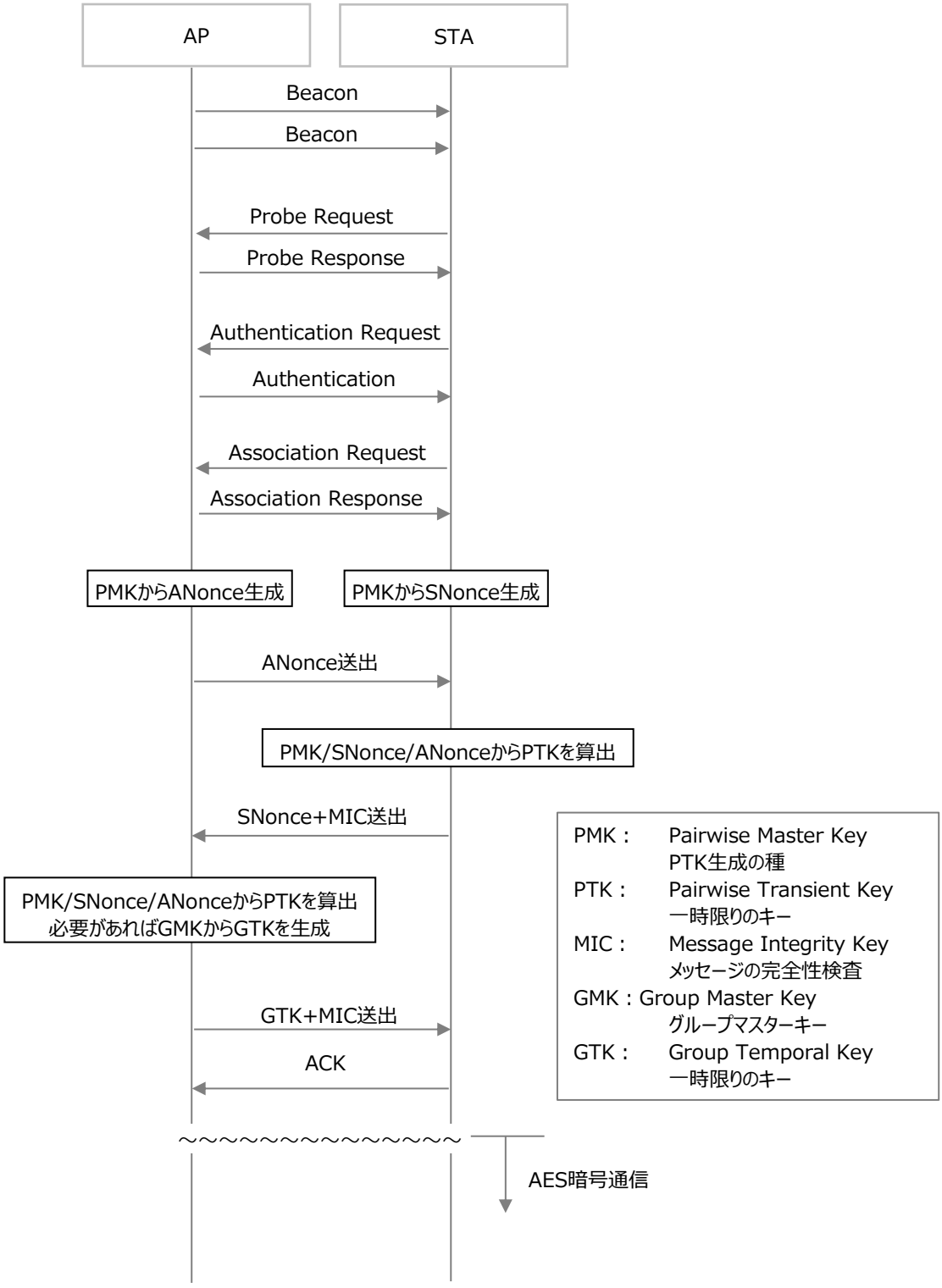


図 3-3WPA2-PSK 認証の接続シーケンス

グループ鍵更新2WAYハンドシェイクのシーケンスを以下に示す。

本シーケンスの処理は、APに接続中の全端末について個別に実施され、全ての端末から応答が返った後に鍵を更新する。

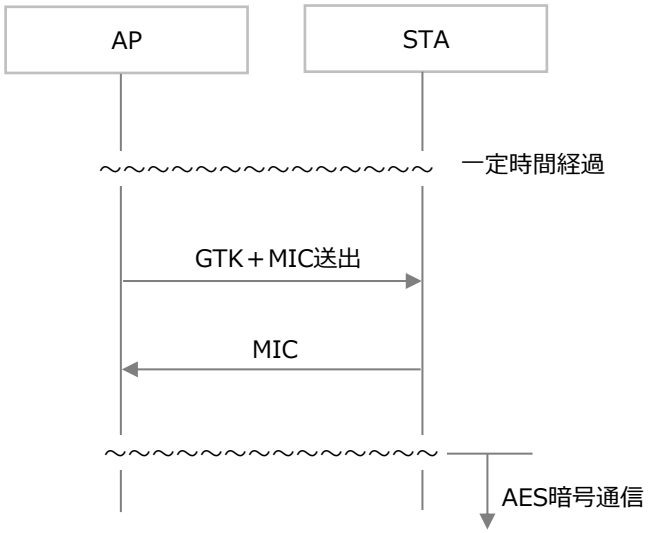


図 3-4WPA2-PSK 2WAY シーケンス

3.9.2 WPA3-SAE(オプション)

WPA3 認証かつ AES 暗号化をオプションとする。本方式では、SAE handshake を実施し、ユニキャスト鍵(PTK)およびマルチキャスト鍵(GTK)ともに 4WAY ハンドシェイクにて交換される。WPA3 認証(SAE 認証)の接続シーケンスを以下に示す。

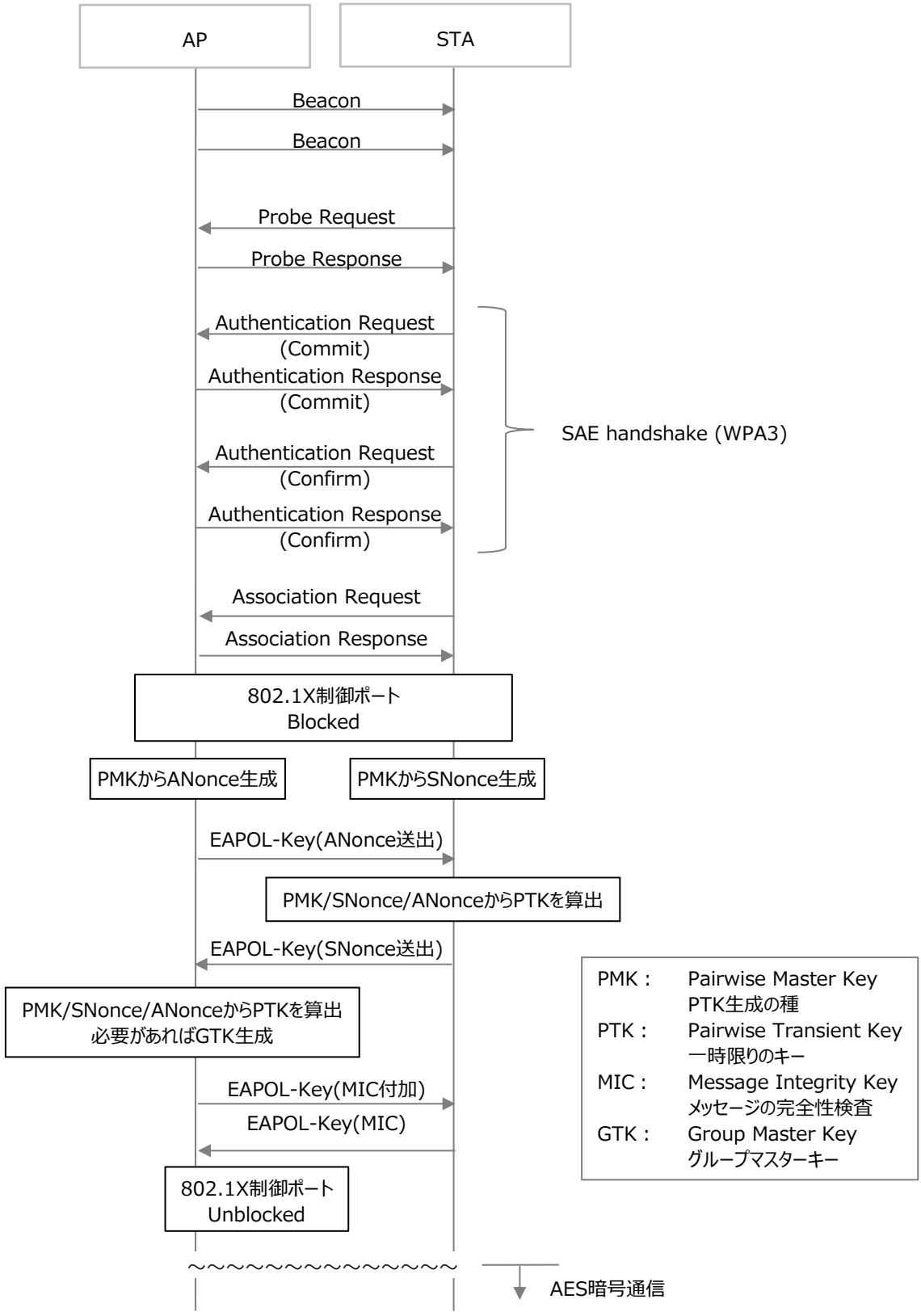


図 3-5WPA3-PSK 認証の接続シーケンス

グループ鍵更新 2WAY ハンドシェイクのシーケンスを以下に示す。

一定時間経過後、接続中の全てに対して個別に更新を行い、すべての端末から応答が返れば鍵を更新する。

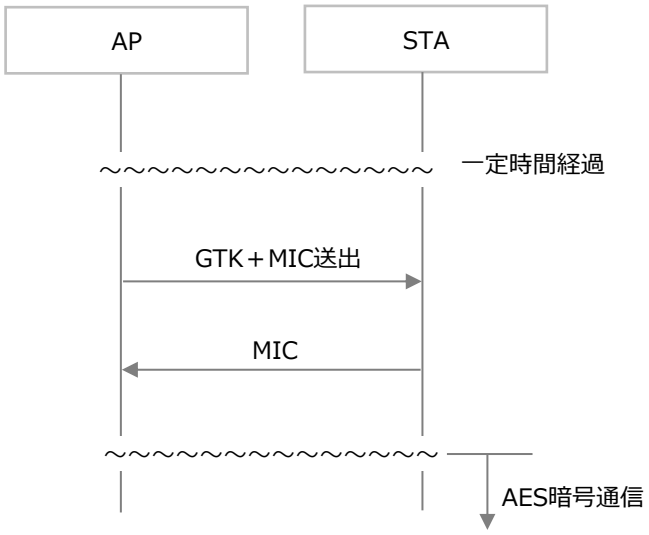


図 3-6WPA3-SAE 2WAY シーケンス

3.10 鍵更新

3.10.1　AP機能

セキュリティ侵害リスクの削減のため、GTKおよびPTKは定期的に更新することを推奨し、GMKおよびPMKの更新に関しては任意とする。

3.10.2　STA機能（クライアント機能）

グループ鍵（GMK）の更新条件は標準規格では規定されていないため、ルータや中継機の実装依存となっており、ECHONET Liteノード間におけるGTKの不一致が発生することがある。このため、スマートメーター側でGTKが古くなっていることを検知し、GTKを再取得することを推奨する。

3.11 暗号化と改ざん検知

WPA2/WPA3の暗号化方式には[IEEE802.11]に基づくAES (CCMP: Counter mode with Cipher-block chaining Message authentication code Protocol)を使用し、MAC Dataフレームの暗号化を実施すること。CCMPは改ざん検知をCounter with CBC-MAC(CCM）で行う。CCMは、WPA2の一部として規定されるCCMP(無線LANに使用される暗号化プロトコルの標準規格)で使用されるブロック暗号の暗号利用モードの一つです。暗号化にカウンター(CTR)モードを、認証にCBC-MACモードを組み合わせたものである。

3.12 リプレイアタック対策

リプレイ検出機構は、他のSTAからデータフレームを受信したSTAが、そのデータフレームが不正な再送であるか否かを検出する手段として[IEEE802.11]に定義されるAES(CCMP)を使ってMICの計算を行うことで、Packet Numberを偽造したリプレイアタック対策を実施する。

3.13 DoS 対策

1.3.1項アプリケーションレベルにおける要求頻度を参照すること。

3.14 各種動作処理

2.4GHz帯無線LAN方式でのBルート通信における動作処理を示す。スマートメーターがAPとして動作する際のBルート認証ID/PASS(SSID/PASS)の情報、IPv4リンクローカルアドレスはスマートメーターに設定済みであるとする。

IP層以降の接続シーケンスに関しては、[SHIF-L1.10]を参照する。

3.14.1　BルートWi-Fi接続開始／終了処理

需要家がBルートサービスを開始し、宅内2.4GHz帯無線LAN方式ネットワークにスマートメーターを参加させる処理(宅内APとスマートメーター間の接続)と、Bルートサービスを停止した際の処理について示す。スマートメーターは、APモード稼働時のみにおいてIPv4での接続を行う。コントローラーと通信するスマートメーターのSTAモードはこれまで通り、IPv6対応する。

尚、コントローラー側が一般的なブラウザで問題なくスマートメーターへアクセスできることを目的としてスマートメーターのIPv4リンクローカルアドレスをBルート認証ID/PWの通知と併せてユーザー側に伝えることとする。

3.14.1.1　B ルート Wi-Fi 接続開始処理例

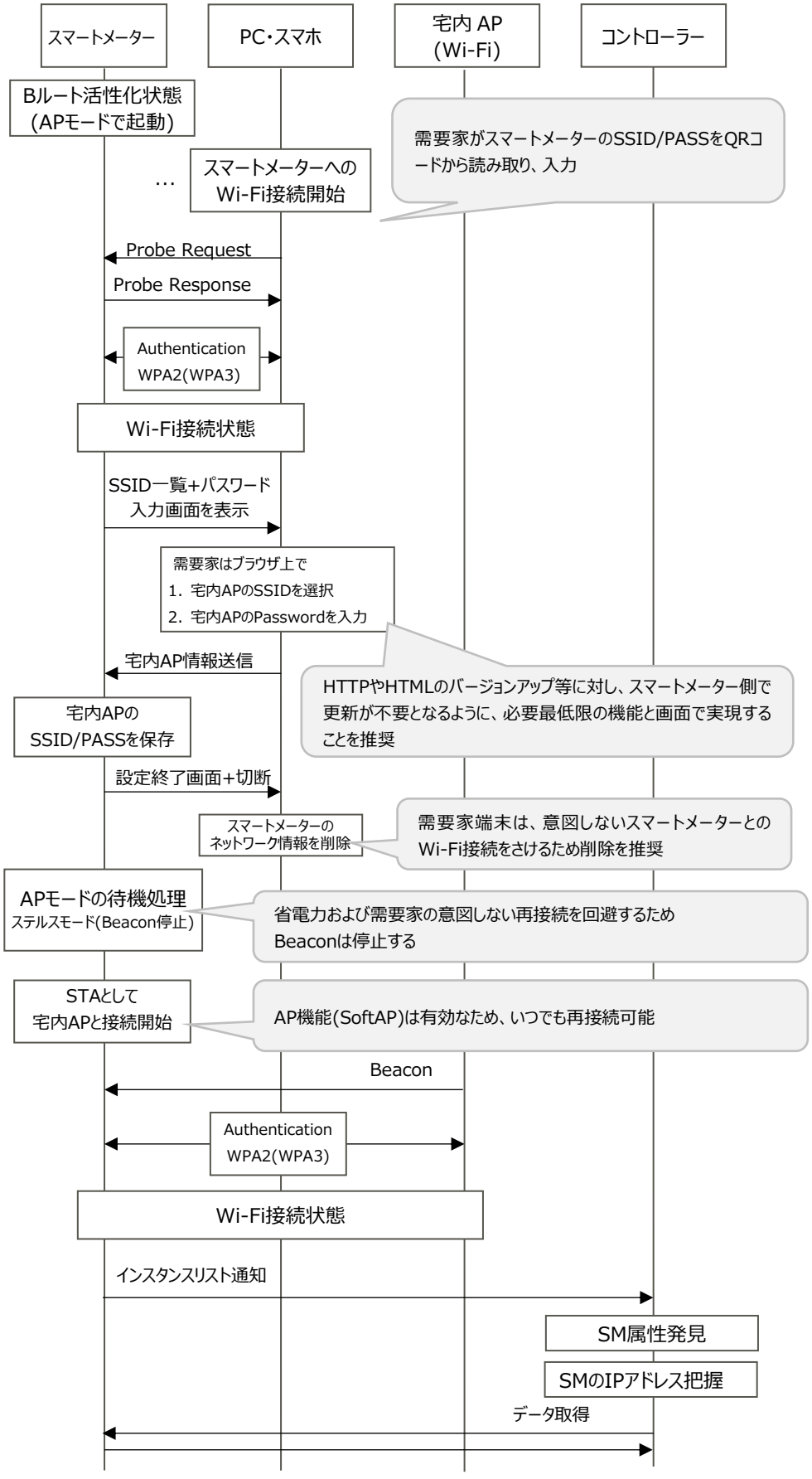


図 3-7B ルート(Wi-Fi)接続開始シーケンス

図 3-7のシーケンスは、以下のように記述できる

① スマートメータは SSID を広報しない。ユーザーは、自身が保有する STA モードで稼働する WI-Fi 機器を用いて予め入手した B ルート認証 ID（スマートメーターの AP モードにおける SSID に相当）、入手パスワードを用いて AP モードで稼働するスマートメーターに接続する

② ユーザー側機器に IPv4 リンクローカル（169.254.146.239 等）が生成される

③ ユーザーは、スマートメーターの IPv4 リンクローカルアドレスを入手し、ユーザ側機器のブラウザでスマートメーターのリンクローカルアドレス上（http://169.254.8.117/等）の Web ページを開く

④ ユーザー自身の AP モードで稼働する WI-Fi 機器に STA モードで稼働するスマートメーターを Ipv6 リンクローカルアドレスでアクセスし、ECHONET Lite 通信を開始する

※スマートメーターの設定に使用した需要家の端末は一度スマートメーターのAPモードに接続するとAPの接続情報を保存しているため、他に優先接続されるWi-Fiが無い場合、意図せず再接続される可能性があるため、需要家の端末からスマートメーターへの接続情報を削除（または自動接続をOFF）することを推奨する」

3.14.1.2　宅内 AP 情報の入力誤り（接続開始時）

PC・スマートフォンからスマートメーターに誤った宅内AP情報を送信した場合の処理を記載する。

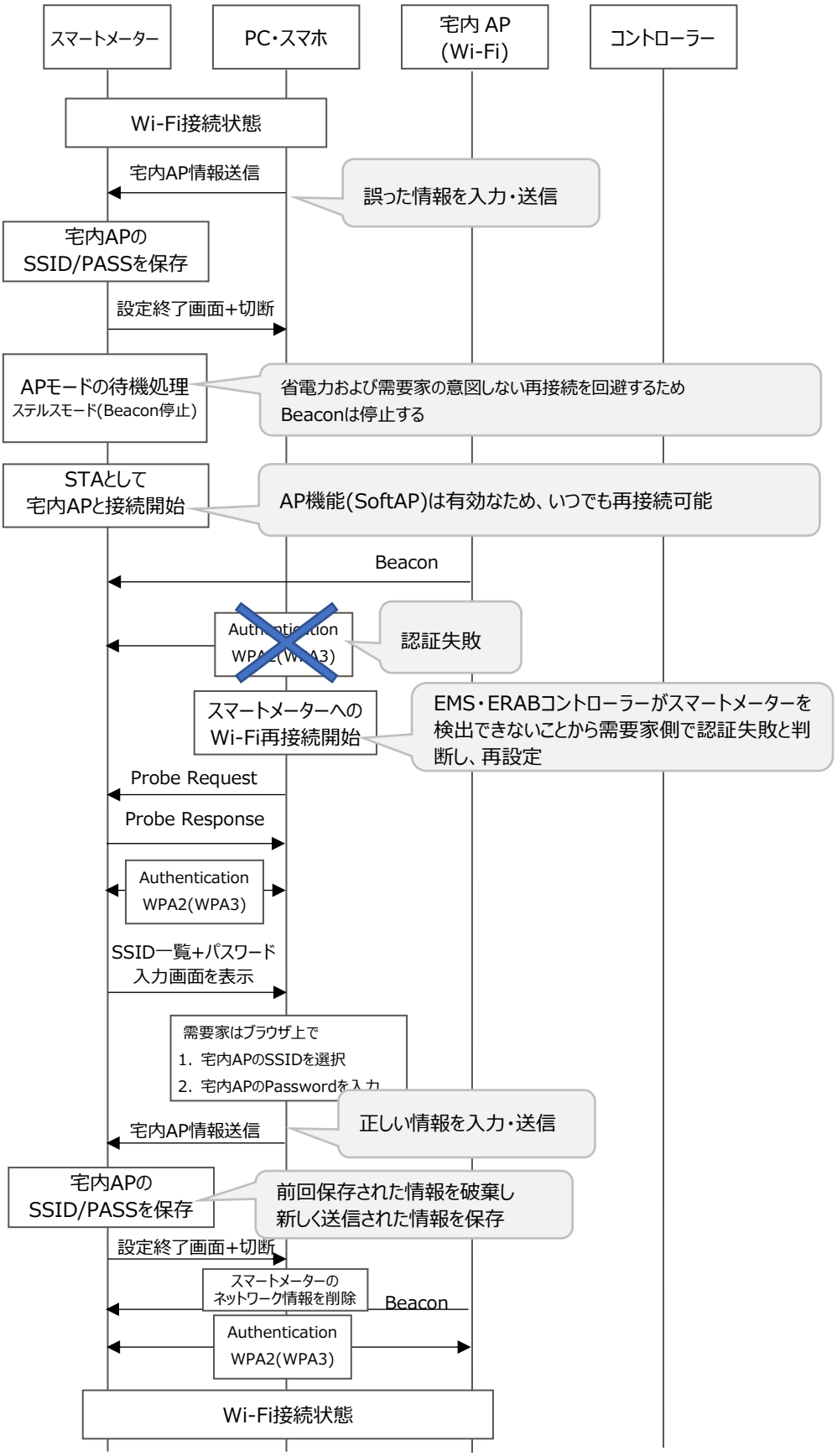


図 3-8B ルート(Wi-Fi)接続開始(宅内情報入力誤り時)シーケンス

3.14.1.3　B ルート Wi-Fi 接続終了処理

Bルートサービスの停止指示を受けた場合、Bルートの非活性化と認証情報の初期化を行う。

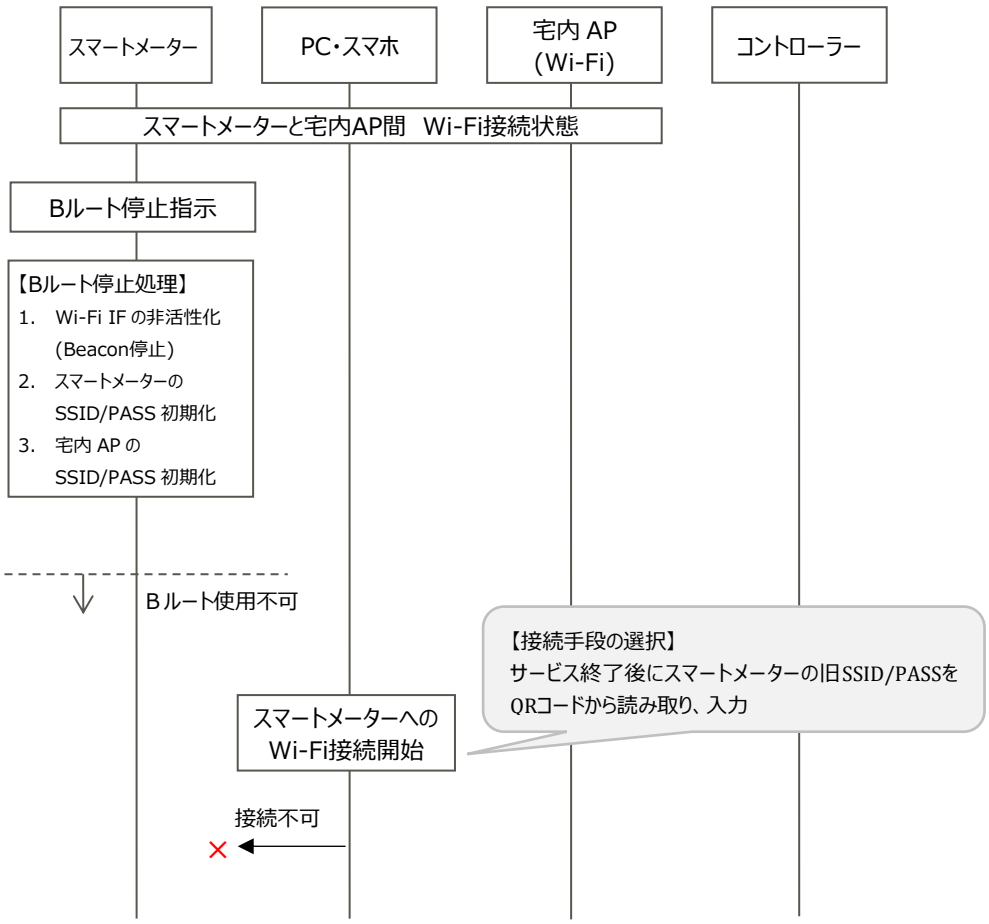


図 3-9B ルート(Wi-Fi)接続停止シーケンス

3.14.2　宅内AP交換（再設定）

Bルート運用開始済みの宅内APが交換または故障等により、スマートメーターに宅内AP情報(SSID/PASS)の再設定が必要な場合の処理を記載する。APモードはスタンバイ状態のため、Probe Requestを受付、Probe Responseを応答することが可能である。

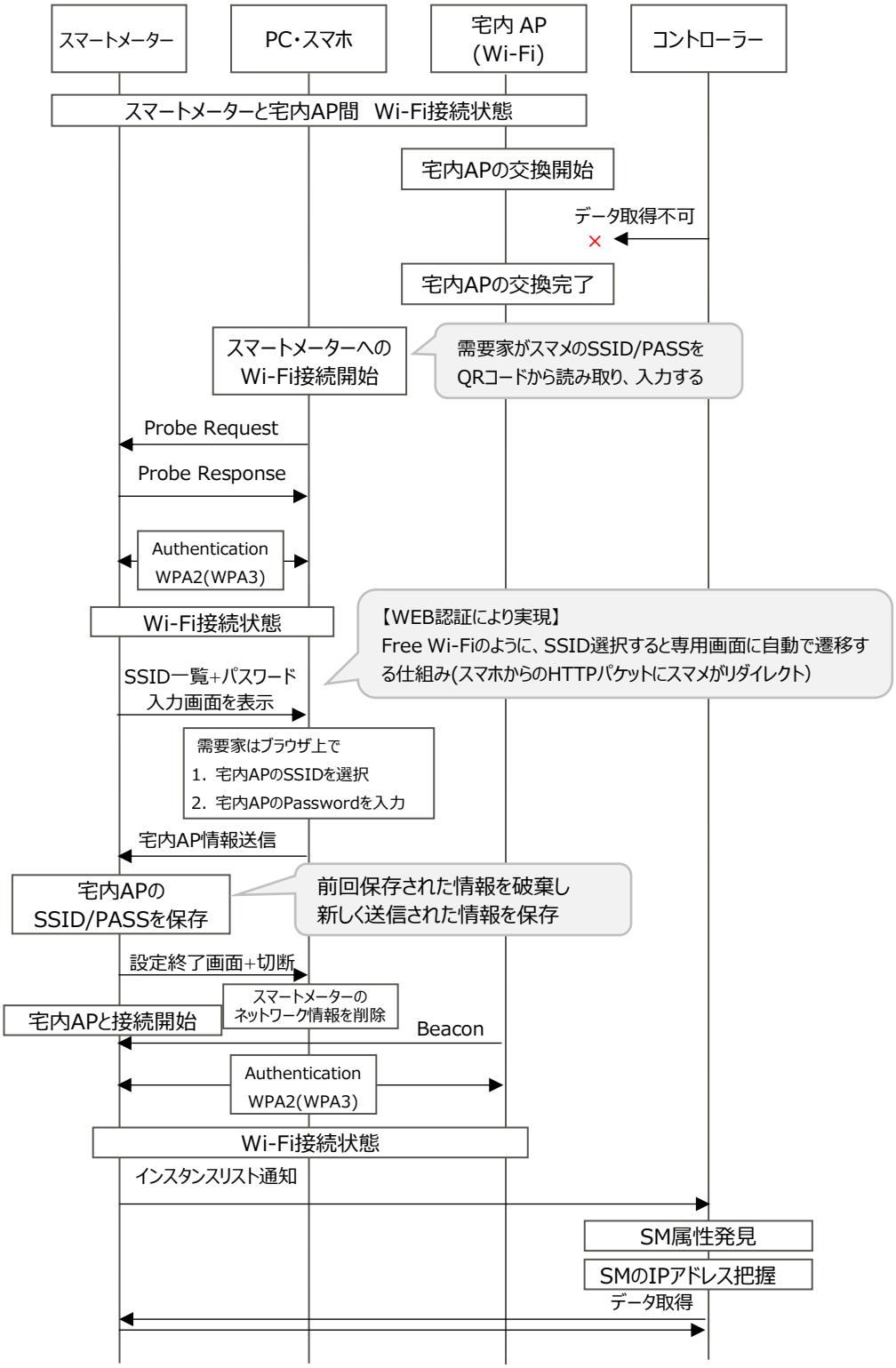


図 3-10 宅内 AP 交換シーケンス

3.14.3　宅内AP故障時（接続完了後）

Bルート運用開始済みの宅内APが故障交換によりスマートメーターへの宅内AP情報再設定が必要となった場合の処理を記載する。

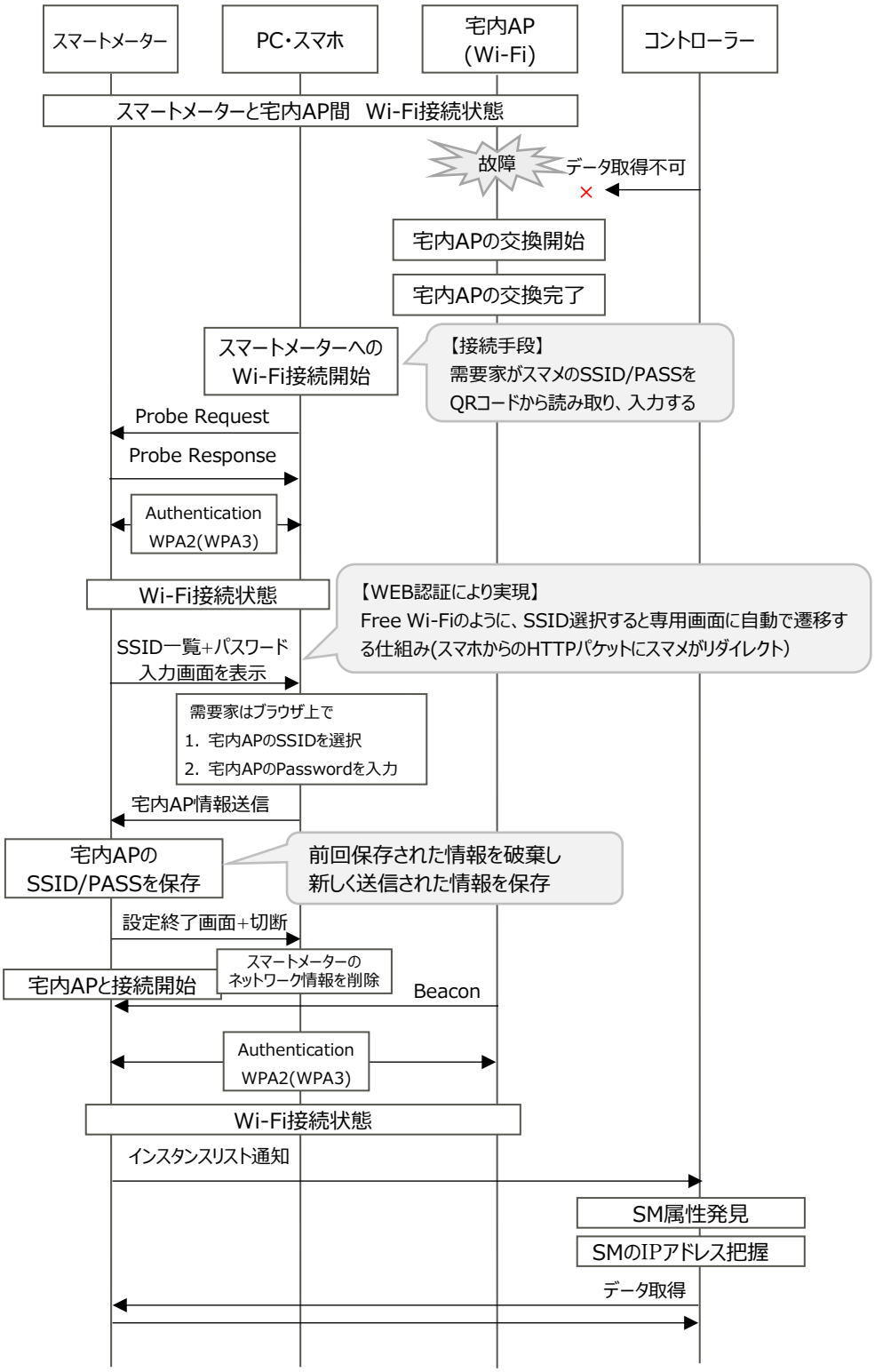


図 3-11 宅内 AP 故障交換シーケンス

3.14.4　EMS・アグリゲーションコントローラー交換

Bルート運用開始済みのコントローラーの交換が発生した場合の処理を記載する。

コントローラーが宅内APに接続された際、スマートメーターを検出する処理はEMS・アグリゲーションコントローラーで実施することとし、方法については任意とする。

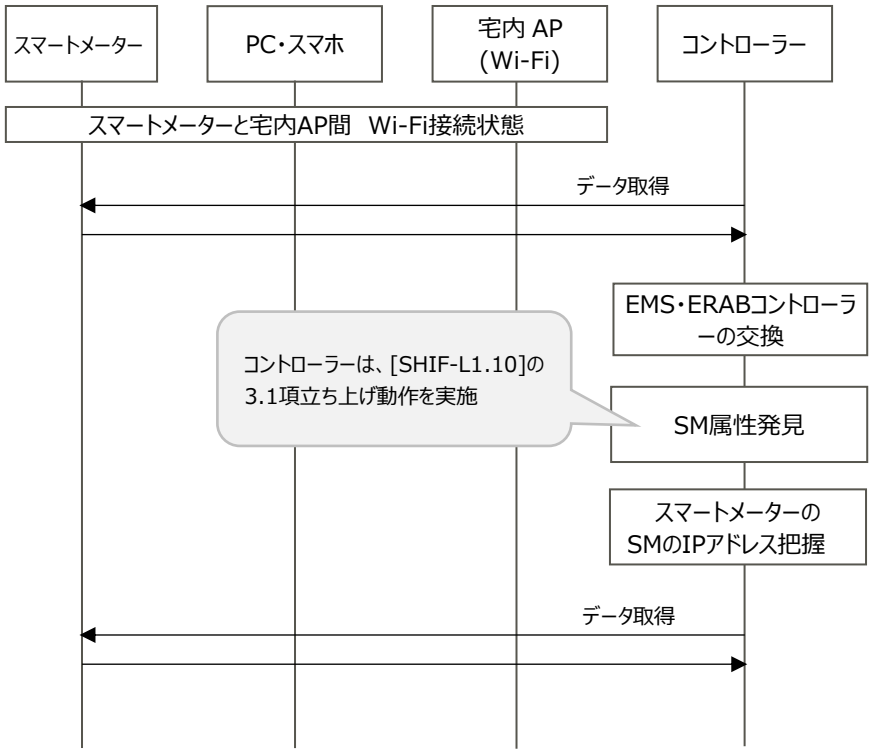


図 3-12EMS・アグリケーションコントローラー交換シーケンス

3.14.5　スマートメーターが複数台の場合

スマートメーターを2台接続する場合のシーケンスを記載する。

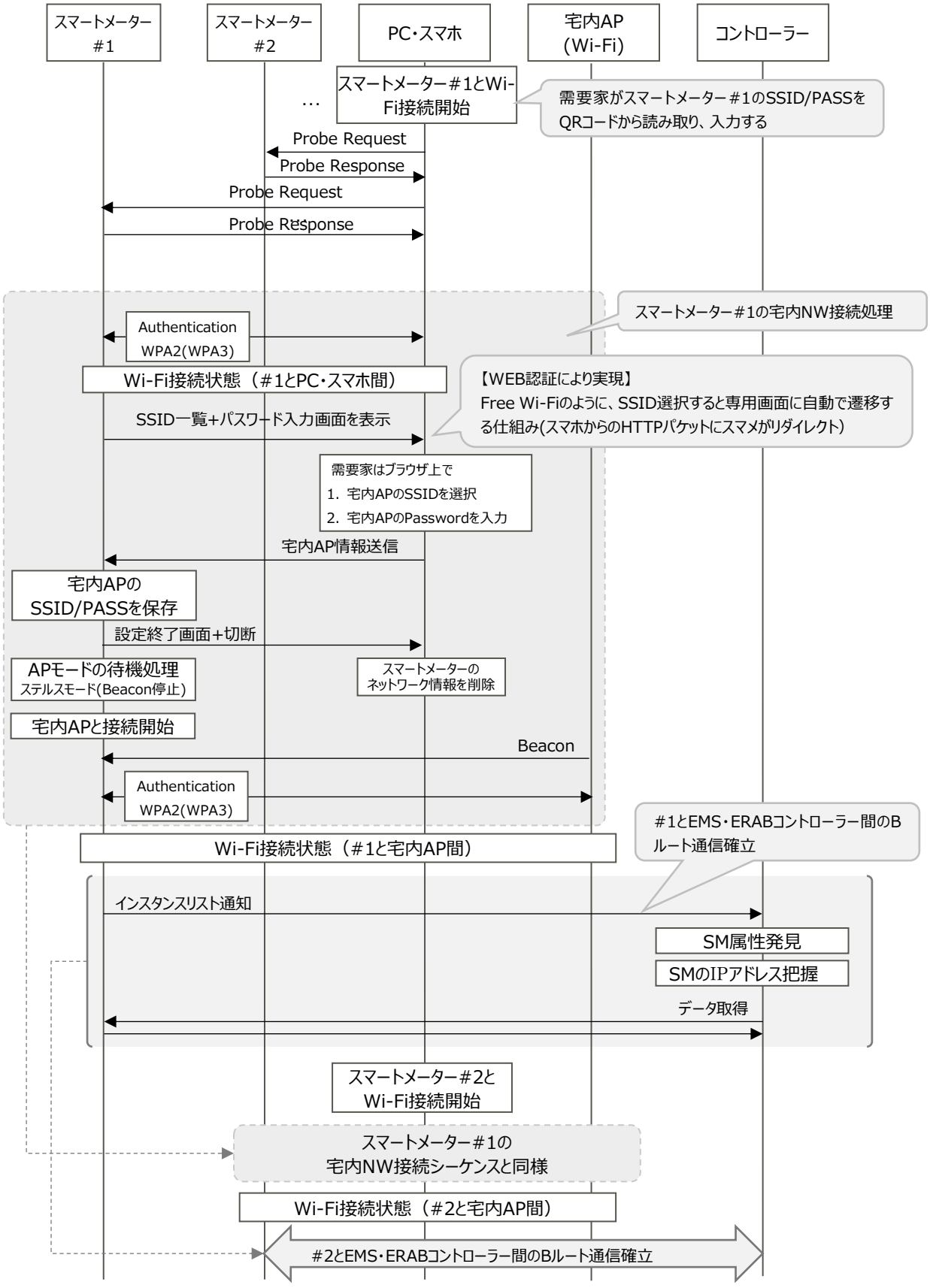


図 3-13 スマートメーター2 台接続時のシーケンス

3.14.6　EMS・アグリゲーションコントローラーが複数台の場合

コントローラーが複数台存在する場合のBルート通信の流れについて記載する。"

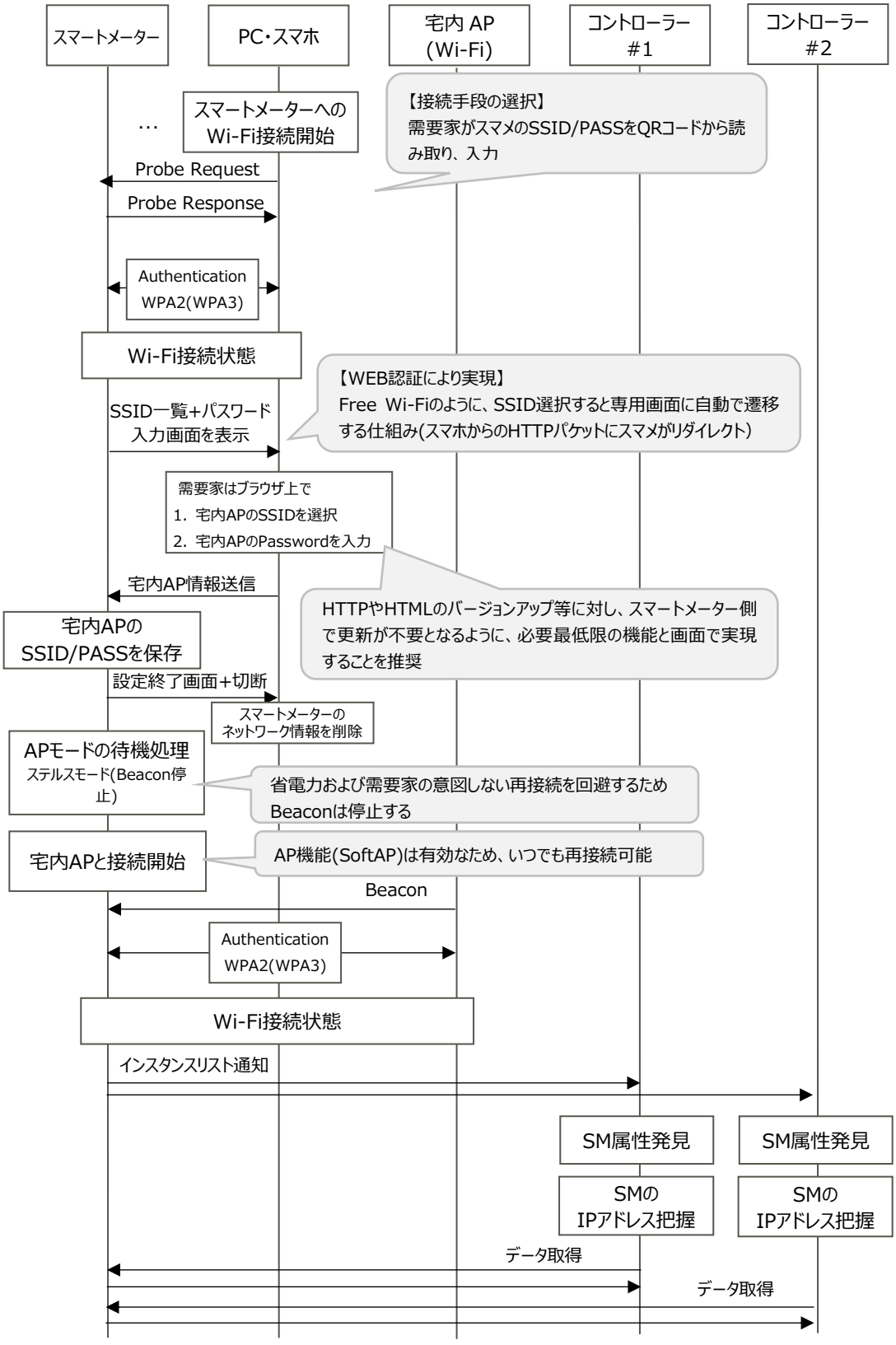


図 3-14　EMS・アグリケーションコントローラーが複数台の場合の通信シーケンス

スマートメーターがSTAモードに切り替わった後は、需要家のスマートフォンが意図しないタイミングでスマートメーターに再接続(※)回避のためスマートメーターがBeaconを停止する省電力化を行う。

※需要家の端末側は、一度登録されたAPの接続情報を覚えているため、スマートメーターからのBeaconを取得した時点で再接続する可能性が存在する。

3.15 処理シーケンス

インスタンスリスト通知の処理シーケンスを図3-15に示す。

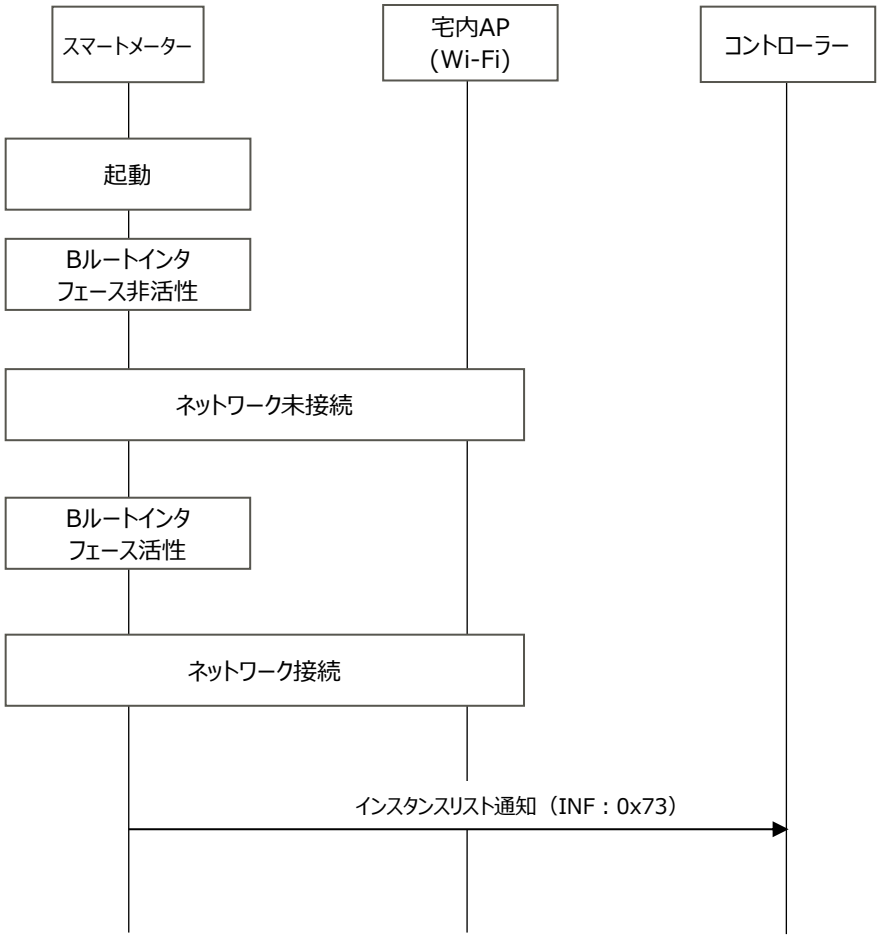


図 3-15 起動からインスタンスリスト通知までのシーケンス

表 3-11 状況別のふるまい

シーン	ふるまい
1 台目の EMS･アグリゲーションコントローラーの 2.4GHz 帯無線 LAN 方式での接続	「コントローラーは、図 3-12 EMS･アグリケーションコントローラー交換シーケンスの”SM 属性発見”以降の手順を実施する」
2 台目の EMS･アグリゲーションコントローラーの 2.4GHz	「コントローラーは、図 3-12 EMS･ア

帯無線 LAN 方式での接続	グリケーションコントローラー交換シーケンスの”SM 属性発見”以降の手順を実施する」
3 台目の EMS・アグリゲーションコントローラーの 2.4GHz 帯無線 LAN 方式での接続	「コントローラーは、図 3-12 EMS・アグリケーションコントローラー交換シーケンスの”SM 属性発見”以降の手順を実施する」
EMS・アグリゲーションコントローラーが一度接続をしながらネットワークから離脱し、再接続する機器を接続したとき	「コントローラーは、図 3-12 EMS・アグリケーションコントローラー交換シーケンスの”SM 属性発見”以降の手順を実施する」

第4章　IEEE802.3下位レイヤ実装

4.1 概要

本仕様で述べるスタック図を示す。IEEE802.3u規格上にIPv6を動作させ、UDPおよびHTTPによるデータ通信、アプリケーションプロトコルとしてECHONET Liteを動作させる。

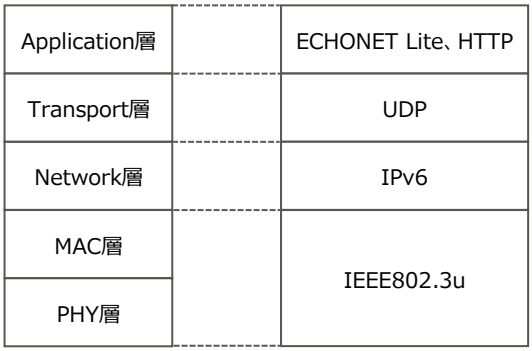


図 4-1IEEE802.3 方式スタック図

4.2 物理層

IEEE802.3u規格上における物理層仕様を示す。本仕様はIEEE802.3uで定義されたPHY仕様を採用し、技術基準適合証明の取得を前提とする。

表 4-1 物理層機能

項目	仕様
準拠規格	IEEE802.3u(100Base-TX)
伝送媒体	UTPケーブル(CAT5以上)
コネクタ	RJ-45
最大長	100m
トポロジー	スター

4.3 MAC 層

MAC層の仕様については、IEEE802.3u仕様に準拠する。なお、スマートメーターおよびコントローラーは、IEEE802.3u準拠に限定する。

4.3.1 フレームフォーマット概要

MACフレームフォーマット概要を以下に示す。

表 4-2 MAC フレームフォーマット

プリアンブル	7オクテット(56ビット)
Start Frame Delimiter	1オクテット(8ビット)。パターンは10101011
送信先アドレス	6オクテット(48ビット)。最初の24ビットがIEEE登録メーカ固有番号。残りの24ビット部分は製造メーカー管理
送信元アドレス	6オクテット(48ビット)。最初の24ビットがIEEE登録メーカ固有番号。残りの24ビット部分は製造メーカー管理
データ長	2オクテット(16bit)
Data and PAD	データが格納されるフィールド。可変フィールド、46オクテット～1,500オクテット。
Frame Check Sequence	通信途上でデータに誤りが生じていないか調べるため、送信時にデータに付加(4オクテット【32bit】受信したフレームに誤りがないかどうかを調べるために付加されるデータ

4.4 ネットワーク層

インタフェース部におけるネットワーク層は、[IPv6]で定義するIPv6プロトコルをベースに表4-3に示す項目を実装しなければならない。

表 4-3 IPv6プロトコル

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	-	Y
IP1.2	Extension Header Order	[IPv6] 4.1	Y
IP1.3	Options	[IPv6] 4.2	Y
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	[IPv6-SAA]	O
IP1.10	ESP Header	[IPv6-MIB]	O
IP2	Deprecation of Type 0 Routing Headers	[IPv6-RH]	Y
IP3	Path MTU Discovery	[IPv6] 5	Y
IP4	Flow Labels	[IPv6] 6	Y
IP5	Traffic Classes	[IPv6] 7	Y

※1: Y:サポート必要、N:サポート不要、O:オプション(任意)

また、表 4-4に示すICMPv6をサポートしなければならない。メッセージ種別としては、エコー要求(タイプ128)およびエコー応答(タイプ129)に加え、宛先未到達(タイプ1)、時間超過(タイプ3)およびパラメータ問題(タイプ4)の各エラーメッセージもサポートしなければならない。パケットサイズ超過(タイプ2)メッセージに関しては、送信機能を持たなくてもよいが受信した際は適切に処理されなければならない。

表 4-4　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
ICMP6	Packet Too Big Message	[ICMP6] 3.2	Y
ICMP7	Time Exceeded Message	[ICMP6] 3.3	Y
ICMP8	Parameter Problem Message	[ICMP6] 3.4	Y
ICMP9	Echo Request Message	[ICMP6]	Y

		4.1	
ICMP10	Echo Reply Message	[ICMP6] 4.2	Y

※1: Y:サポート必要、N:サポート不要、O:オプション(任意)

4.4.1 IPアドレス

表 4-5　に示す項目を実装しなければならない。本方式で定義するネットワークでは、プレフィックスとしてwell known link-local prefix FE80::0/64を使用する。なお、グローバルアドレスとユニークローカルアドレスは、本標準内では使用しない。 IPv6については、表 4 5に従い、こと。本方式で定義するネットワークでは、リンクローカルアドレスのインタフェースID(下位64ビット部分)については、任意とする。その際、プレフィックスとしてwell known link-local prefix FE80::0/64を使用する。

表 4-5 IPv6アドレス

項番	概要	参照番号	サポート有無※1
IPAD1	IPv6 Addressing	[IP6ADDR]	Y (#1)
IPAD1.1	Global Unicast Address	[IP6ADDR] 2.5.4	N
IPAD1.2	Link Local Unicast Address	[IP6ADDR] 2.5.6	Y
IPAD1.3	Unique Local Unicast Address	[ULA]	N
IPAD1.4	Anycast Address	[IP6ADDR] 2.6	N
IPAD1.5	Multicast Address	[IP6ADDR] 2.7	Y ~~(#2)~~
IPAD1.6	Prefix Length		/64
IPAD2	Stateless Address Autoconfiguration	[SLAAC]	Y
IPAD2.1	Creation of Link Local Address	[SLAAC] 5.3	Y
IPAD2.2	Creation of Global Addresses	[SLAAC] 5.5	N

※1: Y:サポート必要、N:サポート不要、O:オプション(任意)

(#1) (#2)一部機能は使用しない

4.4.2 ユニキャストアドレス

スマートメーター及びEMS・アグリゲーションコントローラーは、自装置アドレスとしてリンクローカルアドレスを生成し、リンクローカルアドレスを使用したIPv6通信を行う。リンクローカルアドレスのインタフェースID(下位64ビット部分)については、任意とする。

4.4.3 マルチキャストアドレス

IPv6の近隣探索で要請ノードマルチキャストアドレス(solicited-node multicast address)を使用する。また、ECHONET Lite電文のマルチキャスト送信時は、ECHONET Lite仕様[EL]の規定に従いff02::1を宛先として設定する。なお、エニーキャストアドレス(anycast address)は使用しない。

4.4.4 近隣探索

近隣探索は、IPv6向けに定義されたRFC 4861 [ND]を使用する。[ND]を使用する場合、実装しなければならないIPv6のNeighbor discoveryの必須項目を示す。[ND]が定義する機能のうち、本方式規定に従うノードがサポートしなければならない機能は、アドレス解決、重複アドレス検出の2機能である。また、[ND]に定義されているICMPv6メッセージのうち、本方式規定に従うノードがサポートしなければならないメッセージは、近隣要請メッセージ(Neighbor Solicitation message: Type = 133)と近隣応答メッセージ(Neighbor Advertisement message: Type = 134)の2つである。なお、近隣探索のエントリ数は、３以上とすること。

表 4-6 近隣探索

Item number	Item description	Support (Y:Yes, N:No, O:Option)	Notes
ND1	Router and Prefix Discovery	[ND]6	N
ND2	Address Resolution	[ND] 7.2	Y
ND3	Neighbor Unreachability Detection	[ND] 7.3	N
ND4	Duplicate Address Detection	[SLAAC] 5.4	Y
ND5	Redirect Function	[ND] 8	N
ND6	Router Solicitation Message	[ND]4.1	N
ND7	Router Advertisement Message	[ND] 4.2	N
ND8	Neighbor Solicitation Message	[ND] 4.3	Y
ND9	Neighbor Advertisement Message	[ND] 4.4	Y
ND10	Redirect Message	[ND] 4.5	N
ND11	Source/Target Link-layer Address Option	[ND] 4.6.1	Y
ND12	Prefix Information Option	[ND] 4.6.2	N
ND13	Redirected Header Option	[ND] 4.6.3	N
ND14	MTU Option	[ND] 4.6.4	N

※1: Y:サポート必要、N:サポート不要、O:オプション(任意)

4.5 トランスポート層

トランスポート層として、UDPをサポートする。表 4-7にサポートするポート番号を示す。

表 4-7 UDP ポート番号

プロトコル	ポート番号	概要
UDP	3610	ECHONET Liteで使用するポート番号

4.6 処理シーケンス

インスタンスリスト通知の処理シーケンスを図4-15に示す。

IP層以降の接続シーケンスに関しては、[SHIF-H1.00]を参照する。

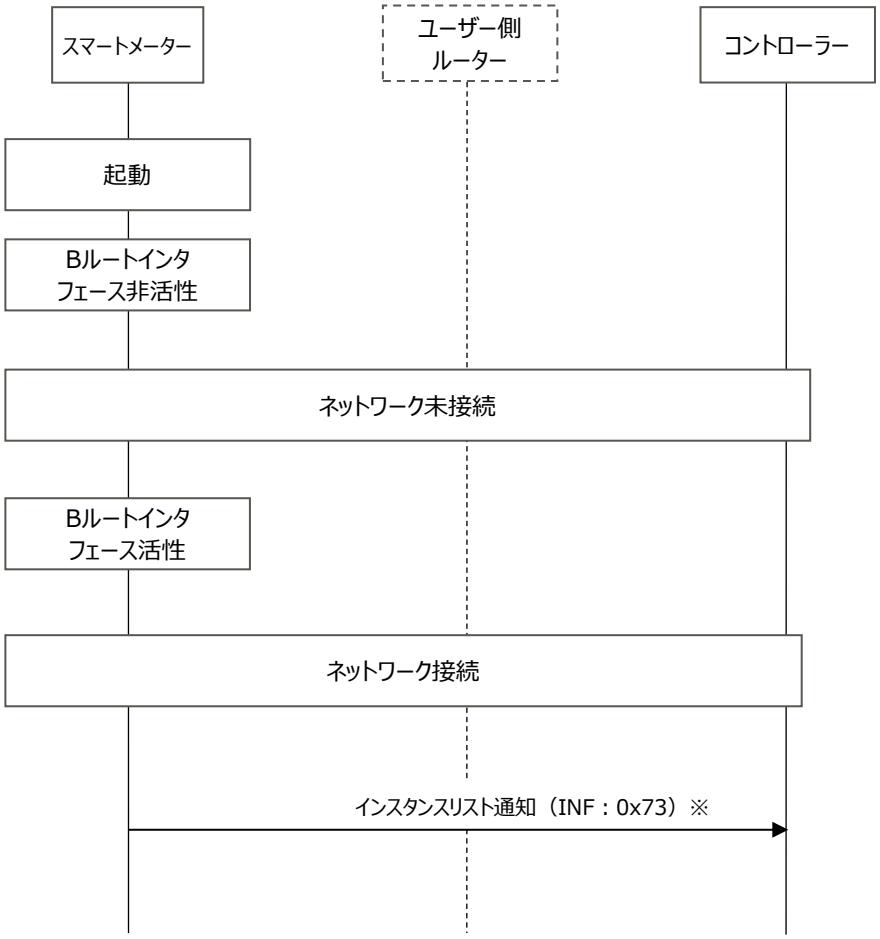


図 4-2 起動からインスタンスリスト通知までのシーケンス

※コントローラーは[SHIF-H1.00]の3.1 立ち上げ動作に従う。

表 4-8 状況別のふるまい

シーン	ふるまい
1 台目の EMS･アグリゲーションコントローラーの第 4 章 IEEE802.3 方式での接続	コントローラーは[SHIF-H1.00]の 3.1 立ち上げ動作に準じる
2 台目の EMS･アグリゲーションコントローラーの第 4 章 IEEE802.3 方式での接続	コントローラーは[SHIF-H1.00]の 3.1 立ち上げ動作に準じる
3 台目の EMS･アグリゲーションコントローラーの IEEE802.3 方式での接続	コントローラーは[SHIF-H1.00]の 3.1 立ち上げ動作に準じる
EMS･アグリゲーションコントローラーが一度接続をしながらネットワークから離脱し、再接続する機器を接続したとき	コントローラーは[SHIF-H1.00]の 3.1 立ち上げ動作に準じる