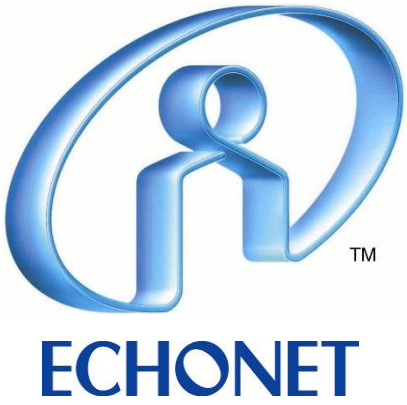
ECHONET Lite システム設計指針

第 2 版



改定履歴

・第 1 版 Draft　　2018 年 5 月 23 日　　制定，コンソーシアム会員内公開。
・ECHONET Lite 規格書 Ver.1.12 第 5 部を改編し本書を策定
・「メーカコードプロパティの搭載の考え方」を 2.9.3 項に追記
・「送信専用機器の扱いに関する指針」を 2.10 節に移動
・「TCP に関する指針」を 2.11 節に移動
・第 6 章として「スマート電力量メータ AIF 仕様に関する実装事例と指針」を追記

・第 1 版　　2018 年 7 月 6 日　　一般公開。
・高圧スマート電力量メータ・EMS 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の名称誤記を修正

・第 2 版 Draft　　2019 年 4 月 5 日　　会員公開。
・2.4.2 項 IGMP 規格に関する補足説明を追記
・2.8 節 識別番号プロパティに関する補足説明および図 2-4 を追記
・2.12 節を新規作成
・第 6 章の文言を全体的に修正
・6.2 節、6.3 節のタイトルを修正
・6.2.1 項 (2)において、事例を追記

・第 2 版　　2019 年 6 月 24 日　　一般公開。

目次

第１章 はじめに

本書では、ECHONET Lite 規格、及び各機器のアプリケーション通信インタフェース仕様の相互接続性向上を目的として、規格や仕様の解釈に関する指針や、これまで市場やプラグフェスト等で発生した不具合を未然に防止するためシステム構築や実装に関する指針をまとめる。

１．１ 参照規格

本書で参照する規格を以下に挙げる。本書に明示的な説明がない事柄については、規格文書に従う。

[EL]　The ECHONET Lite Specification
[APPENDIX]　APPENDIX 機器オブジェクト詳細規定
[LSM_AIF]　低圧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　※会員にのみ公開
[HSM_AIF]　高圧スマート電力量メータ・EMS 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　※会員にのみ公開

第２章 ECHONET Lite の実装に関する指針

本章では、プラグフェストなどを通じて受けた仕様の解釈に関する問合せについて、以下に指針という形でまとめる。

２．１ プロパティ値の扱いに関する指針

本項では、設定されたプロパティ値が、ECHONET プロパティの定義範囲内であるが、対応する実機器の稼動範囲外である場合のプロパティ値の扱いについて指針を記す。

⑴ECHONET プロパティが対応する実機器の連続値の稼動範囲が、ECHONET プロパティ定義範囲より狭い場合に、ECHONET プロパティに、ECHONET プロパティの上限値および下限値の範囲内で、実機器の上限値および下限値の範囲外の値を設定した時、ECHONET Lite ノード上のアプリケーションは、ECHONET プロパティの上限値と、実機器の上限値との間の値を設定した場合は、実機器の上限値を実機器のプロパティ値及び ECHONET プロパティ値とすることを推奨する。また、ECHONET プロパティの下限値と、実機器の下限値との間の値を設定した場合は、実機器の下限値を実機器のプロパティ値及び ECHONET プロパティ値とすることを推奨する。

例えば、ECHONET プロパティ定義範囲が、0x00～0xFD（0℃～253℃）で、対応する実機器の値の稼動範囲が、0x0A～0x32（10℃～50℃）の場合に、ECHONET プロパティに、実機器の上限値と ECHONET プロパティの上限値との間の値（60℃）を設定した場合には、実機器の稼動範囲の上限値 0x32（50℃）を ECHONET プロパティ値とすることを推奨する。また、実機器の下限値と ECHONET プロパティの下限値との間の値（5℃）を設定した場合には、実機器の稼動範囲の下限値 0x0A（10℃）を ECHONET プロパティ値とすることを推奨する。参考図を図 2-1 に示す。

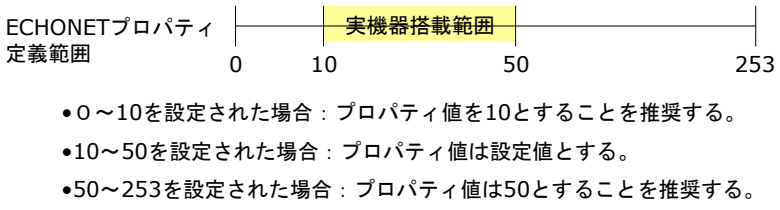


図 2-1　プロパティ値設定例１

⑵ECHONET プロパティが対応する実機器の値の稼動段階が、ECHONET プロパティ定義範囲より少ない場合に、ECHONET プロパティに、ECHONET プロパティの範囲内で、実機器が保持しない段階値を設定した場合に、ECHONET Lite ノード上のアプリケーションは、設定したプロパティ値に近い値を、実機器のプロパティ値および ECHONET プロパティ値とすることを推奨する。

例えば、ECHONET プロパティ定義範囲が、8 段階 0x31～0x38 で、対応する実機器の値の稼動範囲が、3 段階 0x31, 0x35, 0x38 の場合に、ECHONET プロパティに、8 段階のうち、いずれの値を設定した場合でも、ECHONET Lite ノード上のアプリケーションは、ECHONET プロパティ定義範囲が、8 段階 0x31～0x38 と、実機器の稼動範囲、3 段階 0x31, 0x35, 0x38 間のマッピングに従い、設定したプロパティ値に近い値を、実機器のプロパティ値および ECHONET プロパティ値とすることを推奨する。

参考図を図 2-2 に示す。

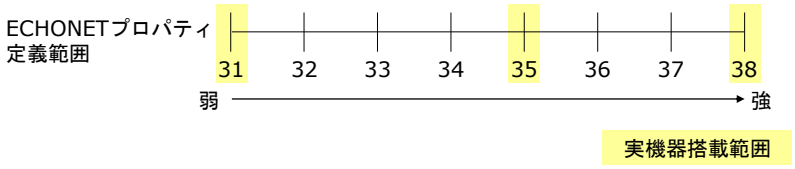


図 2-2　プロパティ値設定例 2

(3)ECHONET プロパティが対応する実機器の値の実装機能が、ECHONET プロパティ定義範囲より少ない場合に、ECHONET プロパティに、ECHONET プロパティの範囲内で、実機器が保持しない段階値を設定した場合に、ECHONET Lite ノード上のアプリケーションは、設定したプロパティ値を無視することを推奨とし、現在の実機器のプロパティ値を ECHONET プロパティ値とすることを推奨とする。

参考図を図 2-3 に示す。

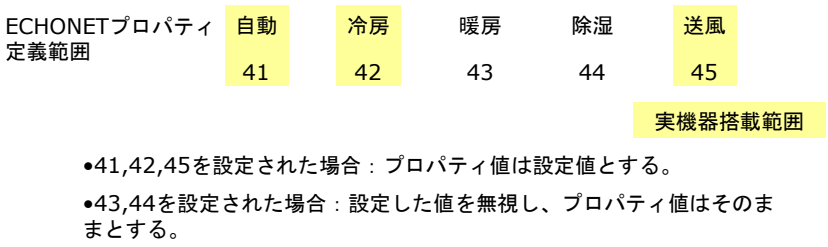


図 2-3　プロパティ値設定例 3

2．2 応答の扱いに関する指針

プロパティ値書き込み要求(ESV=0x60,61)およびプロパティ値書き込み読み出し要求(ESV=0x6E)の設定値として、以下のような値が指定された場合の応答については、処理を受理したものとして取り扱うことを推奨する。すなわち、ESV=0x60 の場合は、応答を行わない。また、ESV=0x61,0x6E の場合はプロパティ値書き込み応答(ESV=0x71)またはプロパティ値書き込み読み出し応答(ESV=0x7E)を返信する。

ただし、実機器における対応範囲の確認処理、または、実機器への設定処理などを実行してから応答を返信するように実装している場合は不可応答(ESV=0x50,0x51,0x5E)を返してもよいものとする。

- ECHONET プロパティ定義範囲外の値が指定された場合
- ECHONET プロパティが対応する実機器の連続値の稼動範囲が、ECHONET プロパティ定義範囲より狭い場合に、ECHONET プロパティに、ECHONET プロパティの上限値および下限値の範囲内で、実機器の上限値および下限値の範囲外の値が指定された場合
- ECHONET プロパティが対応する実機器の値の稼動段階が、ECHONET プロパティ定義範囲より少ない場合に、ECHONET プロパティに、ECHONET プロパティの範囲内で、実機器が保持しない段階値が指定された場合
- ECHONET プロパティが対応する実機器の値の実装機能が、ECHONET プロパティ定義範囲より少ない場合に、ECHONET プロパティに、ECHONET プロパティの範囲内で、実機器が保持しない段階値が指定された場合

2．3 OPC に関する指針

他の ECHONET Lite 機器に対してプロパティ値書き込み要求(ESV=0x60,0x61)、プロパティ値読み出し要求(ESV=0x62)、プロパティ値書き込み読み出し要求(ESV=0x6E)、プロパティ値通知要求(ESV=0x63)を送信する機器（コントローラなど）は、OPC に 2 以上の値 A を設定した要求送信に対して、A よりも小さい値 B が OPC に設定された不可応答を受信した場合、以降の要求送信では、OPC に値 B（以下）を設定することを推奨する。

なお、このとき制御対象機器の OPC 処理可能数がわからない場合、OPC に 1 を設定して要求電文（ESV=0x6*）を送信することで期待する応答の受信可能性が高まる。

2．4 一斉同報に関する指針

2．4．1 基本的な考え方

一斉同報は、その使用方法によっては、ECHONET Lite ノードの処理過負荷やネットワーク輻輳発生を引き起こす可能性がある。一斉同報宛メッセージの送受信に関する指針を示す。

- 宛先が一斉同報宛、かつ、ESV がプロパティ値通知要求（0x63）であるメッセージの送信は、行わないことが望ましい。同メッセージは、それを受信した全てのノードからの、応答による更なる一斉同報宛送信を引き起こす。
- 宛先が一斉同報宛、かつ、ESV がプロパティ値書き込み要求（応答要）（0x61）、読み出し要求（0x62）、通知要求（0x63）、書き込み・読み出し要求（0x6E）のいずれかであるメッセージを受信したノードは、送信元への応答集中を緩和するため、その応答メッセージの送信までに、ノードごとに異なる時間だけ待つのが望ましい。待つ時間は、例えば、ノードごとに異なる固定値、または、ランダム時間を用いる。

・ 各ノードのアプリケーションは、一斉同報による通知や、通知要求を使用する場合、システムや通信メディアの特性を考慮した上でトラフィックに大きな影響がないように使用することが望ましい。例えば、マルチホップを行う通信メディアである場合、多量の一斉同報メッセージを送信するとネットワーク負荷が高まり、システム全体の通信信頼性が落ちることがある。このため、予想されるトラフィックを考慮して送信頻度を設計することを推奨する。

２．４．２ IPv4 環境下での考え方

IP マルチキャストグループを制御する為のプロトコル「IGMP（Internet Group Management Protocol)」規格に対応したルータ（以下、マルチキャストルータと呼ぶ）が、同一ネットワーク上にある場合、ECHONET Lite ノードが送信した一斉同報は、マルチキャストルータを介した先の ECHONET Lite ノードが IGMP 規格に未対応であると、転送されないことがある。このため、IPv4 を用いてシステム構築する場合、ECHONET Lite ノードは、IGMP 規格に対応する事を推奨する(特に、IGMP クエリア対応ルータからの Membership Query 受信時に IGMP Membership Report を送信する機能を保持すること）。

また、以下のケースで IGMP Membership Report を送信することは IGMP に規定されていないが、ルータの実装仕様の差異を吸収しマルチキャスト通信の成功率を高めるために、IGMP Membership Report を送信することが望ましい。マルチキャストに必要な情報を管理しているテーブルからその情報を削除するタイミングがルータの実装仕様によって異なるため、以下のケースで IGMP Membership Report を送信することによって、マルチキャストに必要な情報がテーブルに残る可能性が高くなる。

1. 起動時の IP アドレス取得後
2. リンクダウンからリンクアップ時の IP アドレス取得後
3. IP アドレスの切り替わり時 (DHCP から Static、DHCP リースアウト時など)

また、IGMP Membership Report を監視し、ポート毎に IP マルチキャストパケットの転送を判断する IGMP Snooping 機能を搭載したマルチキャストルータまたは、スイッチがある。このうち、IP マルチキャストパケットの転送期間を管理するマルチキャストルータ／スイッチでは、IGMP Membership Report を受信できず転送期間が経過した場合、マルチキャストルータ／スイッチを介した先の ECHONET Lite ノードに一斉同報の IP マルチキャストパケットが転送されないことがある。このため、ルータの実装仕様の差異を吸収しマルチキャスト通信の成功率を高めるために、ECHONET Lite ノードは定期的に Membership Report を送信し、一斉同報の転送可能状態を維持することを推奨する（例えば 2 分間隔以内)。

ECHONET Lite ノードが Membership Report の定期送信を実装せず、かつ使用するマルチキャストルータが定期的な IGMP Membership Query を送信しない場合には、転送期間を管理する IGMP Snooping 機能を持たない他のマルチキャストルータ／スイッチを選択するか、IGMP Snooping 機能の設定を変更（例：転送期間設定の無効化、IGMP Snooping 機能 OFF など）して ECHONET Lite のシステムを構築する事を推奨する。

OSI Layer3 で IPv4 を使用する場合のアドレスや UDP/TCP のポート規定は、「第 2 部 ECHONET Lite 通信ミドルウェア仕様」の 1.2 節に定義している。IGMP は、RFC1112（Version1）、RFC2236（Version2）、RFC3376（Version3）で規定されている。

２．５ インスタンス数に関する指針

一つの ECHONET Lite ノードが保持する機器オブジェクトのインスタンス数は、原則 84 個以下とする。

実体として 85 個以上のインスタンスを持つノードであっても、84 個以下のインスタンスのみを解釈するノードの存在を考慮し、インスタンスリスト通知(EPC=0xD5)では 84 個までのインスタンスのみを通知するのが望ましい。

85 個以上のインスタンスを含めたインスタンスリスト通知を行いたい、または、それを解釈したい場合、OPC 値を 2 以上、各 EPC 値を 0xD5 とした、一つのメッセージを用いるのが望ましい。ただし、メッセージの送信ノードは、それを解釈しない受信ノードがいることに留意すること。

２．６ プロパティ値書き込み・読み出しサービスに関する指針

プロパティ値書き込み・読み出しサービスの実装指針を示す。

- 他ノードから、プロパティ値書き込み・読み出し要求（ESV=0x6E）を受信するノードは、どのようなプロパティの組み合わせに対しても、まず書き込み要求処理を行い、その完了後の自ノードの状態に基づいた値を、読み出し要求への応答として格納するよう、実装する。任意のプロパティの組み合わせに対し、この順番での処理が保証できない（書き込み処理と機器状態変化とが非同期であるなど）ノードの場合、プロパティ値書き込み・読み出し要求に対して、OPCSet に 0、OPCGet に 0 を格納した不可応答（ESV=0x5E）を返すよう、実装する。

- ある相手ノードに対し、プロパティ値書き込み・読み出し要求（ESV=0x6E）を送信するノードは、その正常応答（ESV=0x7E）を受信した場合、相手ノードへの書き込み要求処理が完了し、かつ、完了後の相手ノードの状態に基づいた値が読み出し要求への応答として得られている、と見なして処理を行うよう、実装する。

２．７ 電文の送信に関する指針

ECHONET Lite 機器には、設備機器、センサ類などのようにメモリ容量が小さく演算処理能力が低い機器が多く存在する。このため、同一の ECHONET Lite 機器に対して短時間で連続して要求電文や通知電文の送信を行う場合や、ECHONET Lite 機器が応答を送信する前に新たな要求電文を同一 ECHONET Lite 機器に送信する場合は、該当する ECHONET Lite 機器からの応答が無くなったり、各電文に対する処理が反映されないなどの恐れがある。ECHONET Lite 機器の中には、秒オーダーかそれ以上の間隔をあける必要がある機器も存在する。同一の ECHONET Lite 機器に対して連続して電文を送信す

る際、多様な ECHONET Lite 機器の処理能力を考慮して送信間隔を設計することを推奨する。

2．8 ECHONET Lite 機器の管理に関する指針

同一の ECHONET Lite ノード上には、2 つ以上の機器オブジェクトを搭載することが可能である。このとき、ECHONET Lite ノードを一意に特定するだけでなく、同一の ECHONET Lite ノード上に搭載している機器単位で、一意に特定したい場合には、機器オブジェクトに「識別番号プロパティ（0x83）」を搭載し、下位通信層のプロトコル種別を 0xFE とする事を推奨する。「識別番号プロパティ（0x83）」は機器オブジェクトをドメイン内で一意に識別するための番号であり、「APPENDIX ECHONET 機器オブジェクト詳細規定」の機器オブジェクトスーパークラスに定義している。ここで「識別番号プロパティ（0x83）」のメーカ規定形式（0xFE）において、ユニーク ID 部は、同一クラスにおいて重複しないように、各ベンダで担保する必要がある。

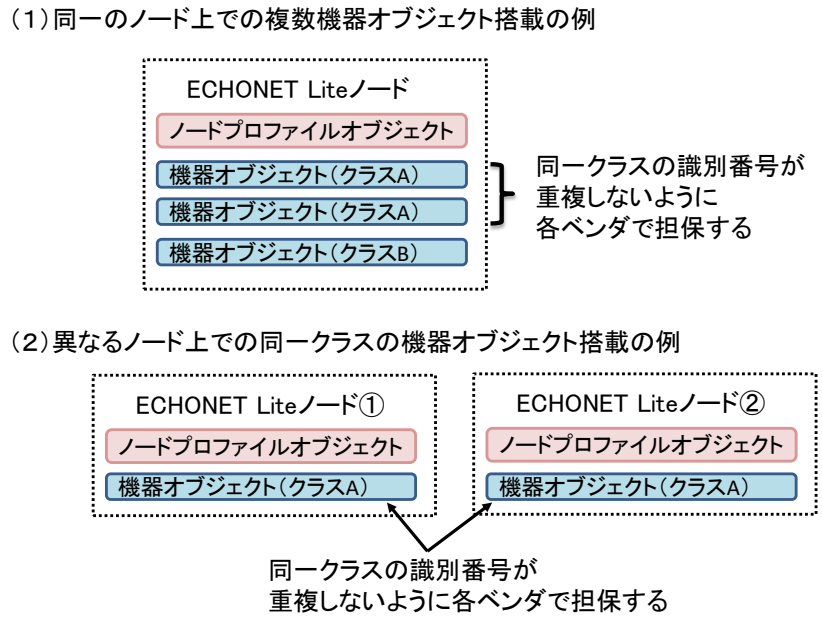


図　2-4　搭載機器オブジェクトと識別番号プロパティ

2．9 ECHONET プロパティの搭載に関する指針

本節では、ECHONET プロパティの搭載に関する指針を示す。

2．9．1 ECHONET Lite ミドルウェアアダプタの搭載オブジェクトの考え方

ECHONET Lite レディ機器と ECHONET Lite ミドルウェアアダプタとの組合せによ

り ECHONET Lite ネットワークに接続する場合、機器オブジェクトのプロパティは ECHONET Lite レディ機器に関連する情報を示し、ノードプロファイルオブジェクトのプロパティは、ECHONET Lite ミドルウェアアダプタに関連する情報を示す。

例えば、機器オブジェクトの製造番号、商品コード、メーカコードのようなプロパティは、ECHONET Lite レディ機器に関連する情報を示し、ノードプロファイルオブジェクトの製造番号、商品コード、メーカコードのようなプロパティは ECHONET Lite ミドルウェアアダプタに関連する情報を示す。

２．９．２ 動作状態プロパティの搭載の考え方

機器オブジェクトの各クラスを搭載するノードにおいて、ノードの動作開始とともに、各クラス固有の機能が、稼動を開始する場合は、「動作状態プロパティ（0x80）」を固定値 0x30 で実装することが可能である。その場合、アクセスルールは Get のみとすることを推奨する。「動作状態プロパティ（0x80）」は、実機器における、各クラス固有の機能が稼動状態であるか否か(ON/OFF)を示すプロパティであり、「APPENDIX ECHONET 機器オブジェクト詳細規定」の機器オブジェクトスーパークラスに定義している。

２．９．３ メーカコードプロパティの搭載の考え方

ECHNONET Lite 規格適合性認証および AIF 仕様適合性認証を取得した ECHONET Lite 機器の各機器オブジェクトのメーカコードプロパティには、認証取得時に使用したメーカコードを搭載しなければならない。なお、認証取得時に使用したメーカコードと異なるメーカコードへ変更する場合には、認証を再取得する必要がある。

２．１０ 送信専用機器の扱いに関する指針

常時通電されており通信可能な機器だけではなく、電池駆動の機器など、消費電力を極力抑えたい機器も ECHONET Lite に対応させるため、ECHONET Lite では送信のみ可能な機器として、送信専用機器を定義する。特殊な機器であるため、その取扱い指針について記述する。

- 送信専用機器をシステムに参入させる場合は、その機器が送信専用機器であることをシステム内の送信専用機器以外の機器に手動で設定すること。
- 送信専用機器が存在するシステムにコントローラを参加させる場合、既存の送信専用機器情報をコントローラに手動で設定すること。
- 送信専用機器は、第２部４．３．１のインスタンスリスト通知アナウンスを定期的に同報することを推奨とする。

２．１１ TCP に関する指針

・ 他ノードへ応答メッセージを送信するノードは、その送信処理時、既にコネクションが切断している場合の対応は実装依存（応答しなくてもよい）とする。

・ 他ノードへ要求メッセージを送信するノードは、通信相手が TCP を使えないケースを考慮し、TCP での接続失敗時、必要に応じて UDP ユニキャストにて送信しなおすのが望ましい。

２．１２ 無線 LAN ネットワークに関する注意事項

通信の安全性を高めるために、マルチキャスト通信で使用するグループ鍵を定期的に更新するルータや中継機が存在する。グループ鍵の更新条件は 802.11i などの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いる。従って、そのようなルータや中継機が同一ネットワーク上にある場合、ECHONET Lite ノード間におけるグループ鍵の不一致が発生することがある。このため、無線 LAN を搭載する ECHONET Lite ノードは、グループ鍵が古くなっていることを検知し、再取得する事を推奨する。

例えば、ECHONET Lite ノードからルータに対して broadcast flag を True(RFC2131 参照)に設定した DHCP のリクエスト(例えば Discover や T2 Request など)を定期送信することによりグループ鍵更新の監視を行うことができる。ルータからのブロードキャストのレスポンス(例えば Offer や Ack)を受信できなくなった場合にグループ鍵が更新されたと判断し、無線を再接続して 4-way handshake を実施することにより新しいグループ鍵を取得することができる。また、UI 上に ECHONET Lite ノードやルータ・中継機の再起動を促すメッセージを示し、手動にて無線 LAN を再接続して 4-way handshake を実施することによりグループ鍵の不一致を解消させてもよい。

あるいは、ルータや中継機のいずれかのキー更新間隔を変更(例えば 10 分など)する事により、グループ鍵不一致の発生を防ぐことも可能である。

第３章　ECHONET Lite におけるセキュア通信の実現指針

３．１ 概要

ECHONET Lite を用いるシステムにおけるセキュリティの課題として、通信内容の改ざんの防止、認証による不正アクセス防止、暗号化による盗聴防止が挙げられる。ECHONET Lite における通信ミドルウェアは、その下位レイヤにおいて、既存のセキュア通信の標準技術を適用することで、ECHONET Lite からは透過的にセキュリティを確保可能となる。本章では、下位レイヤのセキュア通信機構の例と、その適用指針について記述する。

３．２ 下位レイヤにおけるセキュア機構

通信ミドルウェアの下位レイヤにおいて提供される、セキュア機構の一例を示す。下記に限らず、各社独自で提供されているセキュア機構などを用いてセキュリティを確保してもよい。暗号アルゴリズムのネゴシエーション、ECHONET Lite ノード間の通信の暗号化、ECHONET Lite ノード間の認証などの実施手段については、各セキュア機構の仕様に従う。

表 3-1　下位レイヤのセキュア機構

下位レイヤ	セキュア機構
トランスポート	DTLS (Datagram Transport Layer Security)
ネットワーク	IPsec(Security Architecture for Internet Protocol) RFC5191
データリンク	WEP(Wired Equivalent Privacy) WPA(Wi-Fi Protected Access) WPA2(Wi-Fi Protected Access2) AES-CCM(Advanced Encryption Standard Counter with CBC-MAC) IEEE802.1X

３．２．１ DTLS

DTLS は、データグラム向けにセキュア通信機能を提供するプロトコルであり，TLS(Transport Layer Security)とほぼ同様の機能を備える。UDP 上での DTLS 利用について、RFC4347 にて規定されている。ECHONET Lite のトランスポート層において UDP を用い、かつ、トランスポート層において ECHONET Lite 伝送フレームの暗号

化および改ざん防止を実施する際に適用しうる。

3．2．2 IPsec

IPsec は暗号技術を用いて、IP パケット単位でデータの改竄防止や秘匿機能を提供するプロトコルである。IPv4 ではオプションとして使用することができる。IPv6 では標準で実装されている。ECHONET Lite のネットワーク層において IP を用い、かつ、ネットワーク層において ECHONET Lite 伝送フレームの暗号化および改ざん防止を実施する際に適用しうる。

3．2．3 RFC5191

あらかじめ決められた機器以外がネットワークに参加しないよう、認証によって接続を規制するための規格。任意のデータリンク層上での利用が可能。認証要求を発行するクライアントを ECHONET Lite ノード、認証要求を受ける認証エージェント・認証サーバを ECHONET Lite ノードと通信可能な機器が実施する形態を推奨とし、認証方式としては、機器の筐体に記載されるシリアルキーなどを用いた ID・パスワードによる認証（PEAP）、または、機器に格納されたデジタル証明書による認証（EAP-TLS）を推奨とする。

3．2．4 AES-CCM

米国商務省標準技術局(NIST)によって制定された、米国政府の新世代標準暗号化方式。暗号化はカウンタモードで行い、改竄検知は改竄防止コード（MIC：Message Integrity Code）を利用し、MIC 生成には CBC-MAC で行う。

3．2．5 WEP

無線通信における暗号化技術。RC4 アルゴリズムをベースにした秘密鍵暗号方式で、IEEE によって標準化されており、IEEE 802.11b のセキュリティシステムとして採用されている。

3．2．6 WPA

無線 LAN の業界団体 Wi-Fi Alliance が発表した、無線 LAN の暗号化方式の規格。WEP の弱点を補強し、セキュリティ強度を向上させたもの。WPA は、SSID と WEP キーに加えて、ユーザ認証機能を備え、暗号鍵を一定時間毎に自動的に更新する「TKIP」(Temporal Key Integrity Protocol)暗号化プロトコルを採用している。

3．2．7 WPA2

WPA の新バージョンである。米標準技術局(NICT)が定めた暗号化標準の「AES」を採用しており、128～256 ビットの可変長鍵を利用した強力な暗号化が可能となっている。

3．2．8 IEEE802.1X

あらかじめ決められた機器以外がネットワークに参加しないよう、認証によって接続を規制するための規格。有線・無線のどちらでも利用可能。サプリカント（認証クライアント）を ECHONET Lite ノード、オーセンティケータ（認証装置）・認証サーバ（サプリカントの参加許可を判断するサーバ）を ECHONET Lite ノードと通信可能な機器が実施する形態を推奨とし、認証方式としては、機器の筐体に記載されるシリアルキーなどを用いた ID・パスワードによる認証（PEAP）、または、機器に格納されたデジタル証明書による認証（EAP-TLS）を推奨とする。

第４章 ノード検出・発見手順の指針

４．１ 概要

他 ECHONET Lite ノードの制御や状態取得を行いたい ECHONET Lite ノード(以降、本章ではコントローラと呼称）は、常に固定の相手と通信する場合を除き、ノード検出・発見により相手の通信アドレスを知ったのち、通信を行う。

ECHONET Lite では、ノード検出・発見用のメッセージは定義していないが、一斉同報送信、および、搭載必須プロパティの取得や通知の組み合わせにより、これを実現することができる。本章では、その手順の指針を示す。

４．２ ノードからコントローラへのメッセージ送信による検出

ECHONET Lite ノードは、新たにネットワークに参入（通信アドレス変更時も含む）した場合、第２部４．３．１「ECHONET Lite ノードスタート時の基本シーケンス」に従い、インスタンリスト通知メッセージを一斉同報送信しなければならない。コントローラは、新たなノードの参入を即座に検出するために、同メッセージの受信を待ち受け、処理してもよい。

停電復帰時など、全ノードが同時に起動した場合、同時送信によるネットワーク輻輳が発生しうる。その緩和のため、ノードは、新たにネットワークに参入してからインスタンスリスト通知メッセージを送信するまでに、ノードごとに異なる時間だけ待つのが望ましい。待つ時間は、例えば、ノードごとに異なる固定値、または、ランダム時間を用いる。

４．３ コントローラからノードへのメッセージ送信による発見

コントローラは､ネットワーク内に存在する ECHONET Lite ノードを発見するために、任意のタイミングで、ノード発見用メッセージを一斉同報送信してもよい。送信専用機器を除く、全ての ECHONET Lite ノードは、同メッセージを待ち受け、自身が備えるオブジェクトやプロパティに該当する要求であった場合、応答メッセージをコントローラに返送しなければならない。ノード発見用メッセージは、以下のパラメータを用いるのが望ましい。

- 宛先アドレス：一斉同報宛
- TID：任意値
- SEOJ：コントローラが保有しているオブジェクトのいずれか
- DEOJ：ノードプロファイルオブジェクト（0x0EF001）
- ESV：プロパティ値読み出し要求（0x62）
- OPC：1
- EPC：自ノードインスタンスリスト S（0xD6）

特定の機種（ある機器オブジェクトを保有するノード）を発見するために、以下のパラメータを用いてもよい。

- 宛先アドレス：一斉同報宛
- TID：任意値
- SEOJ：コントローラが保有しているオブジェクトのいずれか
- DEOJ：発見したいノードが保有する機器オブジェクト
- ESV：プロパティ値読み出し要求（0x62）
- OPC：1
- EPC：DEOJ に指定したオブジェクトが保有するプロパティ（動作状態(EPC=0x80)など、必須プロパティの指定が望ましい）

ノード発見用メッセージの ESV は、プロパティ値通知要求（0x63）は使用しないことが望ましい。宛先が一斉同報宛、かつ、ESV がプロパティ値通知要求であるメッセージの送信は、それを受信した全てのノードから応答による更なる一斉同報宛送信が発生することから、ノードの処理過負荷やネットワーク輻輳発生を引き起こす可能性がある。コントローラは、ノード発見メッセージの送信後、各ノードからの応答を一定時間待つ。待つ時間は、固定値でも、ネットワーク状況に応じた変動値でもよい。

4．4 ECHONET Lite 機器の接続確認

ECHONET Lite 規格において、機器がネットワークへ接続し続けていることを他ノードへ通知するための仕様は規定していない。しかし、ECHONET Lite ノードの中には、送信専用機器のように、ネットワークへ接続していることを通知するために、定期的にインスタンスリスト通知メッセージを送信する場合がある。受信した ECHONET Lite 機器は、送信元の機器を新規に登録する必要性の有無を判断し、処理を分岐することを推奨とする。また、インスタンスリスト通知メッセージを送信する機器についても、受信した機器が、新規機器の登録処理を行うケースがあることを考慮して、送信間隔の設計を行うことを推奨する。

第５章 遠隔操作に関する指針

５．１ 基本的な考え方

本項では、制御要求電文（ESV=0x60, 0x61, 0x62, 0x63, 0x6E）を送信するノードを「コントローラ」と定義し、制御要求電文を受信するノードを「機器」と定義する。APPENDIX ReleaseC 以降で規定された遠隔操作設定プロパティ(0x93)の目的は、公衆回線経由で制御されたことを「機器」が識別可能にすることを目的としている。

また、コントローラから、該当する機器が、

・公衆回線経由で制御を受けたと認識(0x42)している状態

・公衆回線未経由で制御を受けたと認識(0x41)している状態

のいずれの状態であるかを取得できるように定義している。

公衆回線経由で制御を行うコントローラ、及び公衆回線経由で制御される機器(公衆回線経由での制御操作を認める機器)は「遠隔操作設定プロパティ(0x93)」を実装することを推奨する。

ただし、APPENDIX ReleaseB 以前の ECHONET 機器オブジェクトに対応したシステム及び、APPENDIX ReleaseC 以降でも遠隔操作設定プロパティ(0x93)を付与して制御要求電文を送信する機能を実装していないコントローラを含むシステムにおいては、機器としては、公衆回線経由で制御されたこと、公衆回線未経由で制御されたことを、識別・判断する事はできない。

このような公衆回線経由で制御されたこと、公衆回線未経由で制御されたことを識別できないシステムにおいては、機器としては、安全側に立ち、全ての制御を公衆回線経由で制御されたとして動作することを推奨する。

５．２ ミドルウェアアダプタを用いる場合

オブジェクト生成タイプのミドルウェアアダプタとレディ機器を使用して遠隔操作を行なう場合の指針について記述する。

APPENDIX ReleaseC では公衆回線経由の制御をする場合、遠隔操作設定プロパティを含む複数のプロパティを同一電文に格納して、制御要求電文を送信すること、その際、必ず先頭のプロパティに遠隔操作設定プロパティを付与し、EDT=0x42(公衆回線経由操作)として送信することと定められている。また、公衆回線未経由で制御する場合は、遠隔操作設定プロパティを付与せず、制御要求電文を送信することと定められている。

上記の制御要求電文を受信したミドルウェアアダプタが、レディ機器に制御要求電文の内容を伝達する方法として 2 つの方法を示す。遠隔操作対応のミドルウェアアダプタ、および、遠隔操作対応のレディ機器はいずれかの方法を実装することを推奨する。

なお、いずれの場合も遠隔操作設定プロパティのアクセスルールは、IASetup, IAGetup とする。また、制御元が公衆回線経由か公衆回線未経由かを区別したいプロパティについても、アクセスルールは IASetup, IAGetup とする。

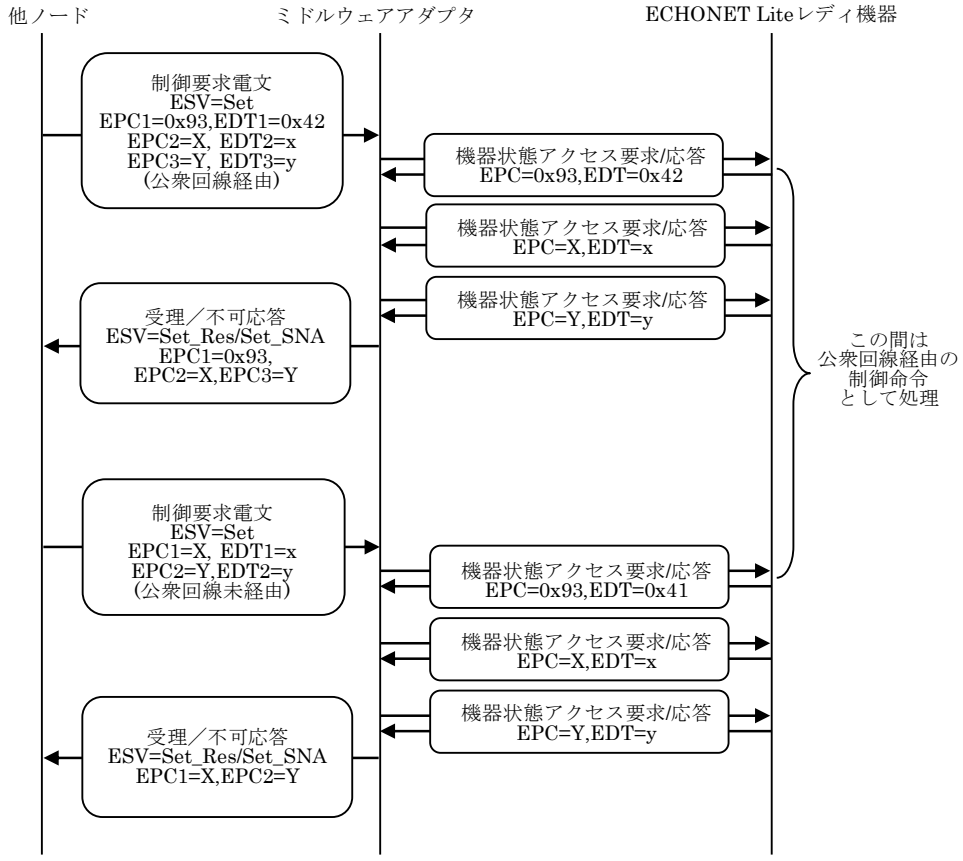
(1) 機器状態アクセス要求／応答コマンドを用いる方法

公衆回線経由の制御要求電文を受信したとき、ミドルウェアアダプタは第 3 部 3.8.5.8 の処理に従う。その際、機器状態アクセス要求／応答コマンドを用いる。

公衆回線未経由の制御要求電文を受信したとき、一つ前に公衆回線経由の制御要求電文を受け取っている場合、ミドルウェアアダプタは、機器状態アクセス要求を用いて、EPC として遠隔操作設定プロパティ(0x93)、EDT として公衆回線未経由操作(0x41)をレディ機器に送出する。レディ機器から受け取った遠隔操作設定プロパティに対する応答は破棄し、最終的な制御要求電文への応答には含めない。その後は、第 3 部 3.8.5.8 に従う。

上記の処理は、レディ機器に対して公衆回線経由の命令と公衆回線未経由の命令との境界を認識させるためである。

レディ機器は、遠隔操作設定プロパティ(EPC=0x93)を公衆回線経由操作(EDT=0x42)に設定する要求を受け取って以降は公衆回線経由の制御命令として処理する。遠隔操作設定プロパティ(EPC=0x93)を公衆回線未経由操作(EDT=0x41)に設定する要求を受け取って以降は公衆非回線経由の制御命令として処理する。この様子を図に示す。

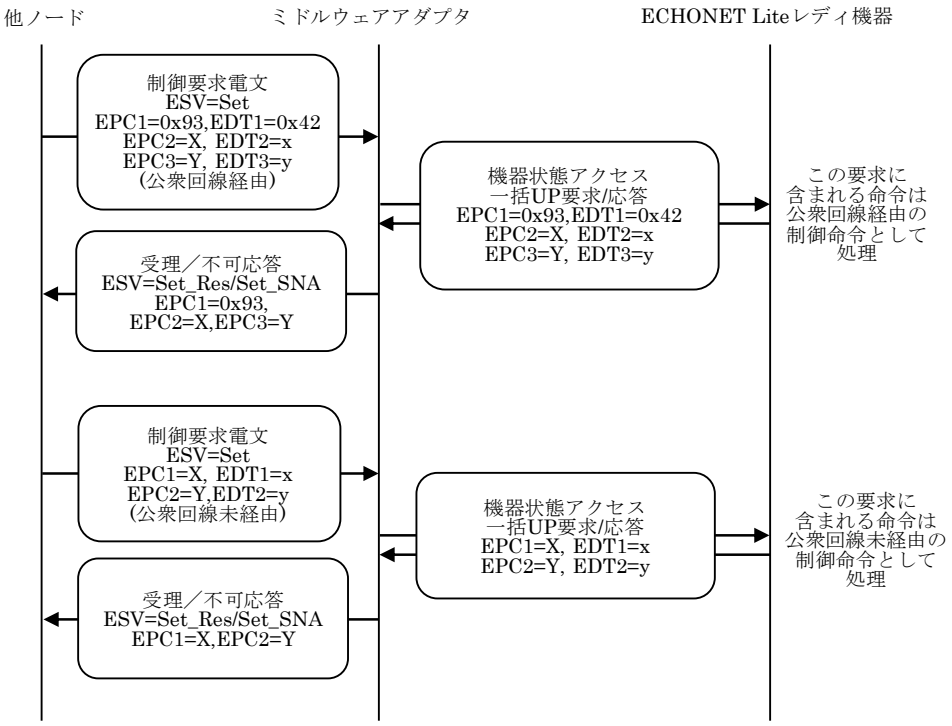


上記の制御要求電文の処理を行なっている間、すなわち、ミドルウェアアダプタが制御要求電文を受け取り、最初の機器状態アクセス要求をレディ機器に送出してから、最後の機器状態アクセス応答をレディ機器から受け取るまでの間は、ミドルウェアアダプタは何らかの排他制御の仕組みを用いて他の機器状態アクセス要求や機器状態アクセス一括 UP 要求のコマンドが割り込まないようにすること。

(2) 機器状態アクセス一括 UP 要求／応答コマンドを用いる方法

ミドルウェアアダプタは第 3 部 3.8.5.8 に従う。この際、機器状態アクセス一括 UP 要求／応答コマンドを用いる。

機器状態アクセス一括 UP 要求を受け取ったレディ機器は、要求の中に遠隔操作設定プロパティ(EPC=0x93)を公衆回線経由操作(EDT=0x42)に設定する要求が含まれていれば公衆回線経由操作として処理する。含まれていなければ公衆回線未経由操作として処理する。この様子を図に示す。



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

本章では、低圧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[LSM_AIF]、および高圧スマート電力量メータ・EMS 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[HSM_AIF]に関して相互接続性に問題が生じる実装事例と期待する動作について記載する。

６．１ 単方向メータに関する実装事例

⑴ 対象機器

低圧スマート電力量メータ

⑵ 事例

低圧スマート電力量メータにおいて、双方向計量部との組み合わせを想定した通信部と単方向計量部を組み合わせた場合、逆方向に関わるプロパティの処理や EDT データが正しく処理されておらず、[LSM_AIF]仕様違反になっている場合がある。ここで、双方向計量部は正・逆両方の電力を計測し、単方向計量部は正方向のみ計測する。

仕様違反の実装例：

・双方向計量部との組み合わせを想定した通信部を単方向計量部と組み合わせた場合に、通信部は逆方向の積算値のプロパティ値として 0x00000000 を応答する。

⑶ 期待する動作

通信部と組み合わせる計量部が、単方向仕様なのか双方向仕様なのかを予め確認する。単方向仕様の場合は、以下のような対応を行うべきである。

・単方向計量部と組み合わせる場合、逆方向のプロパティはプロパティマップに含まない様にすることで、単方向メータであることを示す。

・単方向計量部と組み合わせて、逆方向のプロパティをプロパティマップに含める場合、Get 応答を返す場合は必ず 0xFFFFFFFE（計測値なし）を返す。

尚、市場にて仕様違反が発覚した場合は、認証が取り消される事がある。

６．２ 積算履歴収集日プロパティに関する実装事例

⑴ 対象機器

低圧／高圧スマート電力量メータ

⑵ 事例

スマート電力量メータによっては、Set された積算履歴収集日プロパティの値が Get される積算電力量計測値履歴１プロパティに即座に反映されないケースが確認されている。例えば、同収集日プロパティへの Set と同履歴１プロパティの Get との間に B ルート通信異常が発生し再接続されると、Set された収集日と異なる日の履歴データが返信されるケースがある。また、停電が発生した日付を積算履歴収集日プロパティに設定した場合、取得された積算電力量計測値履歴１プロパティの先頭２バイトで表される積算履歴収集日が不定（0x00FF）となっているケースがある。

⑶ 期待する動作

スマート電力量メータに関しては、積算電力量計測値履歴１プロパティ（EPC=0xE2、0xE4）の先頭２バイトの積算履歴収集日は、再接続、停電などの状況に関わらず、積算履歴収集日プロパティ（EPC=0xE5）で設定されたプロパティ値と一致しなければならない。

６．３ 計測データが無い場合の積算電力値に関する実装事例

⑴ 対象機器

低圧／高圧スマート電力量メータ

⑵ 事例

積算値履歴（あるいは、直近の積算値）を取得した際に、停電で「データの無い期間」の値として、 0xFFFFFFFE（計測データ無し）とすべき箇所が、0x00000000 となっている仕様違反のスマート電力量メータがある。

関連する EPC（プロパティ名）

履歴：

0x E2（積算電力量計測値履歴１(正方向計測値)）
0x E4（積算電力量計測値履歴１(逆方向計測値)）
0x E5（積算履歴収集日１）
0x EC（積算電力量計測値履歴２（正方向、逆方向計測値））
0x ED（積算履歴収集日２）

直近：

0x E0（積算電力量計測値(正方向計測値)）
0x E3（積算電力量計測値(逆方向計測値)）
0x EA（定時積算電力量計測値(正方向計測値)）
0x EB（定時積算電力量計測値(逆方向計測値)）

⑶ 期待する動作

停電時等、計測値が取得できなかった場合は、0x00000000 ではなく、0xFFFFFFFE（計測データ無し）とするべきである。

尚、市場にて仕様違反が発覚した場合は、認証が取り消される事がある。

６．４ 生存確認方法に関する実装事例

⑴ 対象機器

低圧／高圧スマート電力量メータ、HEMS／EMS コントローラ

⑵ 事例

ECHONET Lite では、相手側が接続状態を保っているかを周期的に確認する「生存確認（Keep Alive）」のための手順が規定されていないため、様々な実装が混在しており、相互接続性上、問題になる可能性がある。

これまでに、以下の実装例が、報告されている。

1）IPv6 層の Neighbor Solicitation - Advertisement
2）Wi-SUN の MAC 層（802.15.4e）の Enhanced Beacon Request - Enhanced Beacon
3）ECHONET Lite 層の SetC/Get コマンド – Set_Res/Get_Res
4）ICMPv6 の Echo Request – Echo
5）Universal Plug and Play (UPnP)用の Simple Service Discovery Protocol (SSDP) UDP Port = 1900

（補足）PANA Notification Request (AUTH, P-bit) : PANA 認証の一部として、生存確認用通信（TR-1052 2.8.3.1.2 節）が規定されている。

⑶ 期待する動作

生存確認は、必須機能を用いて実現することが一般的であり、低圧スマート電力量メータの場合には、Wi-SUN もしくは ECHONET Lite の必須機能を用いることが望ましい。また、高圧スマート電力量メータの場合には、ECHONET Lite の必須機能を用いることが望ましい。

６．５ 再接続試行に関する実装事例

⑴ 対象機器

HEMS コントローラ

⑵ 事例

低圧スマート電力量メータの中には、PANA 認証の Session Life Time に関係なく、毎日ある時刻になるとＢルートの ECHONET Lite 通信を停止するような実装をしているものがある。ここで、MAC 層や IPv6 層などの下位層では応答するが、PANA や ECHONET Lite 通信には応答しないことが確認されている。

また、低圧スマート電力量メータの生存を確認できなくなった場合や、ECHONET Lite による通信が不能となった場合、HEMS コントローラが Active Scan からやり直してしまうと、再接続までに長い時間がかかってしまうため、再接続までの間、データが欠落してしまう事例が報告されている。

⑶ 期待する動作

HEMS コントローラは、上記事例のように低圧スマート電力量メータが離脱することを踏まえて設計し、低圧スマート電力量メータの生存を確認することができなくなった場合、低圧スマート電力量メータに対して、再接続をするべきである。再接続は、下記の 1) から 4) 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 4)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) 全 Channel の Active Scan

（補足）再接続の詳細については、「TTC 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 実装詳細ガイドライン」に記載されている。

６．６ ECHONET Lite 通信開始に関する実装事例

(1) 対象機器

低圧スマート電力量メータ、HEMS コントローラ

(2) 事例

PANA 認証完了後の、ECHONET Lite 通信開始シーケンスが例として[LSM_AIF]に図示されているが、相手側が必ずその例の通りに通信を行なうと期待し、図例以外のシーケンスを認めなかった場合、PANA 認証は成功しても ECHONET Lite 通信ができなくなる。

これまでに、以下のような実装例が報告されている。

・相手からの起動時 INF（EPC=0xD5）を受けないと ECHONET Lite 通信を始めないため、何らかの理由で、起動時 INF を受信できなかった場合に ECHONET Lite 通信を開始しない。

・相手からの起動時通信を受信する際、受信タイミングに寛容でないため、互いの送受信タイミングがずれると ECHONET Lite 通信を開始しない。

・HEMS コントローラが、PANA 認証完了後間髪を入れず INF_Req を出し、スマート電力量メータは受信準備が間に合わないため応答できず、ECHONET Lite 通信を開始しない。

・低圧スマート電力量メータで、通電後の B ルート初回接続時しか起動時 INF を送信しないものがある。

(3) 期待する動作

・HEMS コントローラ及びスマート電力量メータは、PANA 認証完了後、各々が直ちに ECHONET Lite ノードとしての通信を開始し、インスタントリスト通知を送信する。特に、HEMS コントローラは、スマート電力量メータのインスタントリスト通知の受信を、自機器の ECHONET Lite 通信開始のトリガにすべきではない。

・低圧スマート電力量メータ用の HEMS コントローラは、PANA 認証完了後、一定時間待ってもインスタンスリストを受信出来ない場合、ユニキャストでの INF_Req[0x63]にて、相手機器のインスタントリスト通知を取得することが[LSM_AIF]において推奨されている。

・相手機器の処理性能が、自機器と異なることを考慮して実装する。特に、HEMS コントローラは、スマート電力量メータの処理速度が（通信に限らず）かなり遅い場合があることを考慮し、受信のタイミングや、送信間隔等に十分余裕を持つべきである。

６．７ コントローラの置き換えに関する実装事例

⑴ 対象機器

低圧／高圧スマート電力量メータ、HEMS／EMS コントローラ

⑵ 事例

古いHEMS/EMS コントローラを、新しいHEMS/EMS コントローラに置き換える際、スマート電力量メータが、何らかの制約や手続きが必要な仕様だった場合、ユーザに不必要な混乱を招く恐れがある。

スマート電力量メータが、何らかの制約や手続きを必要としていた例：

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 HEMS コントローラに接続できないケース。（一般的なユーザは、切断手続きをせずに、古いHEMS コントローラを外してしまうため、新しい HEMS コントローラに接続できないという事象となってしまう。）

2）スマート電力量メータの 1 次側電源を 10 秒以上切らないと、次の HEMS コントローラ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 HEMS コントローラを接続できないケース。（いつ新しいHEMS コントローラ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。）

⑶ 期待する動作

スマート電力量メータは、上記事例１）および２）のような実装はすべきではない。

また、上記事例３）のように、接続要求を受け付けられないタイミングがあることは、不適切と考えられるため、通常の動作時には、接続要求は、常に受け付けられるべきである。

ただし、複数のコントローラが同時に存在していた場合、複数のコントローラが、スマート電力量メータを交互に取り合うような事態が起きることが懸念される。従って、コントローラは、複数コントローラ存在時に、交互にスマート電力量メータ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）を持つことが望ましい。

６．８Ｂルート開通以前の積算電力量履歴値の応答方法に関する実装事例

⑴ 対象機器

低圧／高圧スマート電力量メータ

⑵ 事例

B ルートの開通が、A ルートから設定されるスマート電力量メータが存在し、B ルート開通以前の積算電力量履歴値を返信できるものと、返信できないものも存在する。後者の中には、Get コマンドに対して、0xFFFFFFFE（計測データ無し）で応答するものと、Get_SNA で応答するものがあるとの報告事例がある。

⑶ 期待する動作

B ルート開通以前の積算電力量履歴値を返信できないスマート電力量メータは、Get コマンドに対して、0xFFFFFFFE（計測データ無し）で応答することが望ましい。Get_SNA で応答することは、[LSM_AIF]/[HSM_AIF]仕様違反ではないが、Get コマンドの再送が繰り返される可能性があることに留意すべきである。

６．９ PANA 認証中の異常に関する実装事例

⑴ 対象機器

低圧スマート電力量メータ、HEMS コントローラ

⑵ 事例

PANA 認証シーケンス中に、HEMS コントローラから想定外の PANA パケットを受信した場合、低圧スマート電力量メータの B ルート通信が停止する事例がある。

PANA 認証の途中で、HEMS コントローラが Error 通知を発信すると、それを受けた低圧スマート電力量メータの通信モジュールが動作停止する事例がある。

⑶ 期待する動作

PANA 認証途中で認証エラーを検知した場合、HEMS コントローラ及び低圧スマート電力量メータは、TTC TR-1052 の記述に従った動作を行うことが望ましい。

また、低圧スマート電力量メータは、想定外の PANA パケットを受信しても動作停止せず、PANA 認証を破棄して、PANA 認証をやり直すべきである。

６．１０ 積算電力計測に関する実装事例

⑴ 対象機器

低圧/高圧スマート電力量メータ

⑵ 事例

積算電力量計測値（EPC=0xE0, 0xE3）の値が 30 分毎にしか更新されず、定時積算電力量計測値(EPC=0xEA, 0xEB)と同一になっているスマート電力量メータがある。現在値が取得できないため、デマンド・レスポンスの細かい制御ができない。

⑶ 期待する動作

スマート電力量メータは、EPC=0xE0, 0xE3 の値として現在値を応答するべきである。

６．１１ DoS 攻撃対策に関する実装事例①

⑴ 対象機器

低圧／高圧スマート電力量メータ、HEMS／EMS コントローラ

⑵ 事例

スマート電力量メータの中には、DoS（Denial of Services）攻撃対策として、1 分間あたり 60 回以上受信すると、10 分間通信不能となるケースが確認されている。ECHONET Lite コマンドだけでなく、Neighbor Solicitation 等の IPv6 コマンドなどを多用している HEMS／EMS コントローラとの通信であっても同様の症状が発生するケースも確認されている。

⑶ 期待する動作

スマート電力量メータに関しては、上記のような過度な動作制限を設けないよう実装することが望ましい。

HEMS／EMS コントローラに関しては、上記のような挙動となるケースを想定し、正常に通信可能なケースにおいても、Neighbor Solicitation 等下位層の通信も考慮した上で、余裕を持った時間間隔でスマート電力量メータへアクセスするべきである。また、データ応答が無い場合、AIF 認証仕様に基づく時間間隔や B ルートで用いられる下位通信層の仕様に準拠した再送処理や、一定期間通信不能な場合に再接続処理を行うなど、適切なリカバリ処理を実施するべきである。

６．１２ DoS 攻撃に関する実装事例②

⑴ 対象機器

低圧スマート電力量メータ

⑵ 事例

HEMS コントローラが低圧スマート電力量メータに Wi-SUN で B ルート接続する時に、低圧スマート電力量メータが、後から接続してくる HEMS コントローラに接続対象を切り替える後勝ち動作をする場合、以下のような DoS 攻撃が成立する可能性がある。

低圧スマート電力量メータが、新たな HEMS コントローラから Enhanced Beacon Request (EBR)を受信した時点で、現在接続中の HEMS コントローラの接続を解放する動作をする場合、悪意ある攻撃者が EBR を送信することで、HEMS コントローラと低圧スマート電力量メータの間の通信を妨害することが可能となる

⑶ 期待する動作

低圧スマート電力量メータは、既に接続済みの HEMS コントローラが存在する場合、EBR 受信時に既存の接続を解放せず、新たに接続を要求する HEMS コントローラの PANA 認証が済むまで、接続済みの HEMS コントローラとの接続を維持することが望ましい。