

## 第5部 ECHONET Lite システム設計指針

## 改定履歴

- Version1.00 Draft 2011年3月9日 制定, コンソーシアム会員内公開。
- Version1.00 2011年6月30日 コンソーシアム会員内公開。
- Version1.01 Draft 2012年1月25日 コンソーシアム会員内公開。

変更のある目次項目は以下の通り

	変更部位 (目次項目)	追加・変更概要
1	第1章	図1-1、図1-2、図1-3を修正
2	第3章	送信専用機器に関する記述を追記

- Version1.01 2012年3月5日 一般公開。
- Version1.10 Draft 2013年1月7日 コンソーシアム会員内公開。

変更のある目次項目は以下の通り

	変更部位 (目次項目)	追加・変更概要
1	1.2	新規に項目を作成し、応答の扱いに関する指針を記述
2	1.3	新規に項目を作成し、OPCに関する指針を記述
3	1.4	新規に項目を作成し、一斉同報に関する指針を記述
4	1.5	新規に項目を作成し、インスタンス数に関する指針を記述
5	1.6	新規に項目を作成し、プロパティ値書き込み・読み出しサービスに関する指針を記述
6	第4章	新規に項目を作成し、ノード検出・発見手順の指針を記述
7	第5章	新規に項目を作成し、TCPに関する指針を記述

- Version1.10 2013年5月31日 一般公開。

変更のある目次項目は以下の通り

	変更部位 (目次項目)	追加・変更概要
1	1.3	OPCに関する記述を修正
2	4.3	ノード発見に関する記述を修正

- エコーネットコンソーシアムが発行している規格類は、工業所有権(特許, 実用新案など)に関する抵触の有無に関係なく制定されています。エコーネットコンソーシアムは、この規格類の内容に関する工業所有権に対して、一切の責任を負いません。
- この書面の使用による、いかなる損害も責任を負うものではありません。

## 目次

第1章 ECHONET Lite の実装に関する指針.....	1-1
1. 1 プロパティ値の扱いに関する指針.....	1-1
1. 2 応答の扱いに関する指針.....	1-2
1. 3 OPC に関する指針.....	1-3
1. 4 一斉同報に関する指針.....	1-3
1. 5 インスタンス数に関する指針.....	1-4
1. 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.....	1-4
第2章 ECHONET Lite におけるセキュア通信の実現指針.....	2-1
2. 1 概要.....	2-1
2. 2 下位レイヤにおけるセキュア機構.....	2-1
2. 2. 1 DTLS.....	2-1
2. 2. 2 IPsec.....	2-2
2. 2. 3 RFC5191.....	2-2
2. 2. 4 AES-CCM.....	2-2
2. 2. 5 WEP.....	2-2
2. 2. 6 WPA.....	2-2
2. 2. 7 WPA2.....	2-3
2. 2. 8 IEEE802.1X.....	2-3
第3章 送信専用機器の扱いに関する指針.....	3-1
第4章 ノード検出・発見手順の指針.....	4-1
4. 1 概要.....	4-1
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.....	4-1
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.....	4-1
第5章 TCP に関する指針.....	5-1

## 第1章 ECHONET Lite の実装に関する指針

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、以下第1章に、指針という形でまとめる。

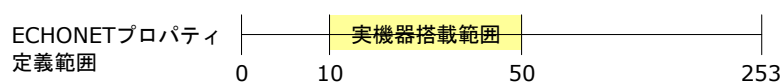
### 1. 1 プロパティ値の扱いに関する指針

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。

- (1) 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°C~253°C) で、対応する実機器の値の稼動範囲が、0x0A~0x32 (10°C~50°C) 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°C) を設定した場合には、実機器の稼動範囲の上限値 0x32 (50°C) 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°C) を設定した場合には、実機器の稼動範囲の下限値 0x0A (10°C) を ECHONET プロパティ値とすることを推奨する。

参考図を図 1-1 に示す。

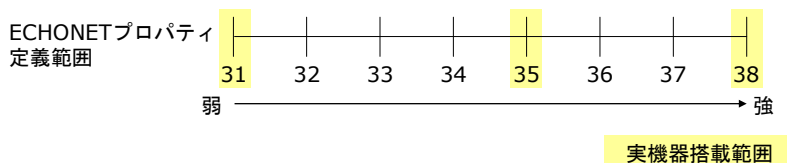


- 0~10を設定された場合：プロパティ値を10とすることを推奨する。
- 10~50を設定された場合：プロパティ値は設定値とする。
- 50~253を設定された場合：プロパティ値は50とすることを推奨する。

図 1-1 プロパティ値設定例 1

- (2) 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 1-2 に示す。

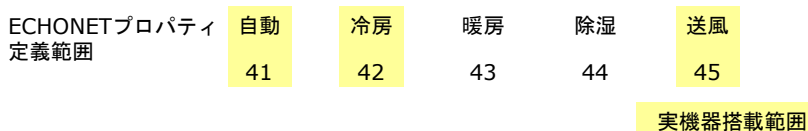


- 31,35,38を設定された場合：プロパティ値は設定値とする。
- 32,33,34,36,37を設定された場合：設定された値31,35,38の近い値にマッピングを行い、プロパティ値とする。

図 1-2 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 1-3 に示す。



- 41,42,45を設定された場合：プロパティ値は設定値とする。
- 43,44を設定された場合：設定した値を無視し、プロパティ値はそのままとする。

図 1-3 プロパティ値設定例 3

## 1. 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

### 1. 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。

### 1. 4 一斉同報に関する指針

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。

## 1. 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。

## 1. 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。

## 第2章 ECHONET Lite におけるセキュア通信の実現指針

### 2. 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。

### 2. 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 2-1 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

#### 2. 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。

## 2. 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。

## 2. 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。

## 2. 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。

## 2. 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。

## 2. 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。

## 2. 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。

## 2. 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。サブリカント（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（サブ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3章 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。

## 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、インスタンス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。

## 第5章 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、既に接続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。