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。
	2011 年 12 月 21 日	一般公開。

- 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プロパティ値の扱いに関する指針

本章では、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℃～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 1-1 に示す。

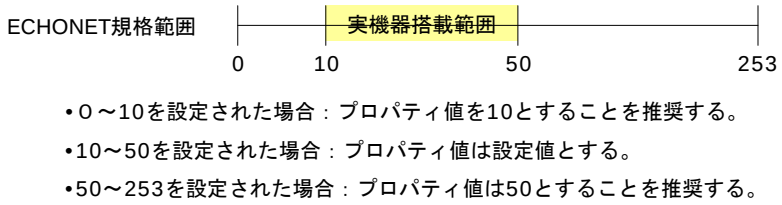
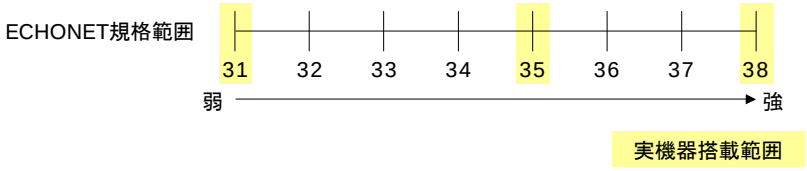


図 1-1　プロパティ値設定例１

(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 １-３３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

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３章 ECHONET Liteにおける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。