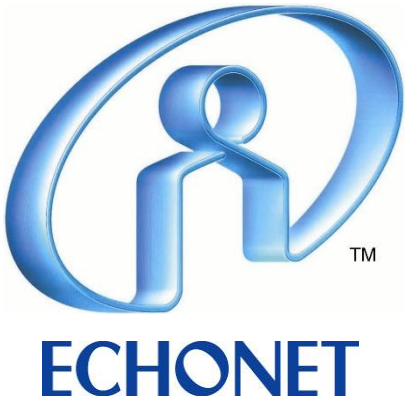
ECHONET Lite 機器を用いたシステム全体の信頼性確保に関する指針

第 1 版



改定履歴

・第 1 版 Draft	2019 年 12 月 26 日	制定，コンソーシアム会員内公開。
・第 1 版	2020 年 2 月 25 日	一般公開。

目次

第 1 章 はじめに

本書では、ECHONET2.0 実現に向けて、ECHONET Lite 機器が IoT 社会に資するものであることを明確化することを目的に、インターネットを含めた ECHONET Lite 機器を用いたシステム全体において、信頼性を確保するための考え方を整理し、システム全体としての信頼性確保に関する指針をまとめる。

1． 1 ECHONET2.0 の概要

日本政府は、科学技術基本計画の第 5 期計画において、我が国の目指すべき理想の未来社会を Society5.0 と名付け、デジタル革新、イノベーションを最大限活用して実現する方針を掲げている。「Society 5.0」で実現する社会では、サイバー空間とフィジカル空間が高度に融合し、両空間を跨いで、様々なモノやデータが動的につながり、必要な人に対して、必要な時に、必要なモノやサービスを提供することになる。

エコーネットコンソーシアムでは、「エネルギーマネジメント」に加え「ヘルスケア」を第 2 の基軸サービスとし、システムの信頼性の考え方の整理、サーバ間連携の技術検討、サービス事業者への普及促進などを通じて IoT 社会／Society 5.0 実現に貢献していく「ECHONET2.0」に向けた活動を進めている。

サイバー空間とフィジカル空間が高度に融合する Society 5.0 産業社会では、サプライチェーンに関わる全要素について、部分的ではなく全体的な対応を通じて信頼性を確保することが重要である。

この新たな産業社会環境において、ECHONET2.0 では、従来の ECHONET1.0 における規格拡張に加え、ECHONET Lite 機器が IoT 社会に資するものであることを明確化するために、インターネット含めたシステム全体の信頼性指針策定を検討している。（図 1-1）

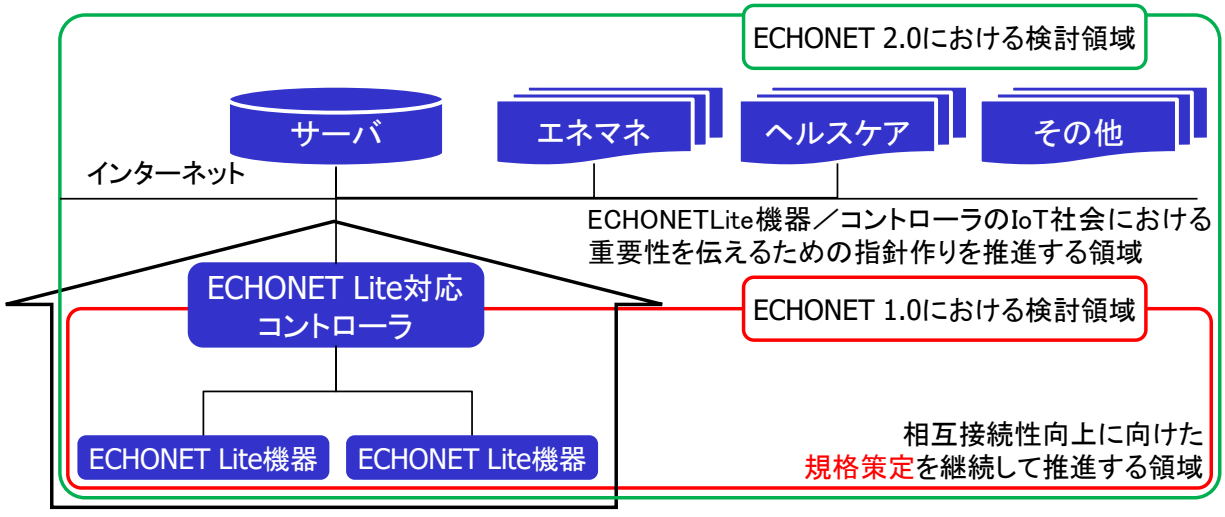


図 1-1　ECHONET2.0 検討領域

ECHONET2.0 の基本方針は、ECHONET Lite 機器の普及台数を武器にニーズに対応するサービス創造を推進すること、標準化団体などとの連携や新規事業者の容易な参入により仲間作りを強化することの 2 点である。

サービス創造推進に関する具体的な活動として、まず、ECHONET Lite 機器を用いたサービス普及に向け、サービス事業者の事業企画／マーケティングの認知度向上を図ることでサービス事業者との連携を強化し、サービス事業者等が多種多様なサービスをサーバ間連携する際に利用可能な、応用アプリ開発用の WebAPI を検討している。そして、サーバ、コントローラ、ECHONET Lite 機器の組合せで構築可能なシステムにおける、高い相互接続性と信頼性の確保について検討し、考え方を整理している。本書は、本検討結果により策定された指針である。

仲間作り強化に関する具体的な活動としては、ヘルスケアを中心にサービス拡張するにあたっての新規事業者の参入を想定し、試験センターの横展開や開発環境のオープン化について検討し、新規参入者向け環境整備を図っている。

また、従来からの活動である ECHONET Lite 機器の拡張と国際標準化および国際展開についても引続き強力に推進していく。

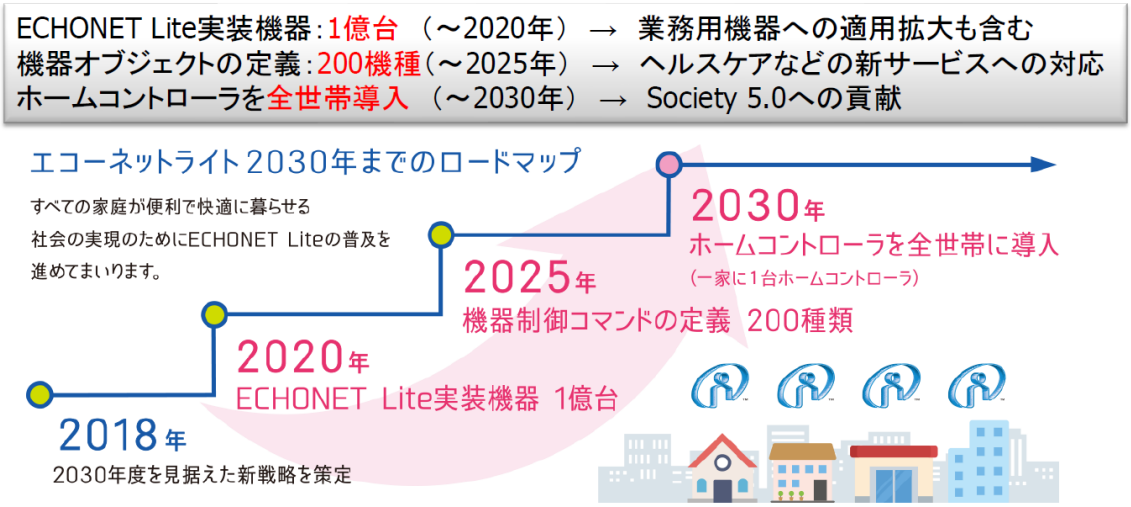


図 1-2　ECHONET2.0 の目指す姿

図 1−2 は、ECHONET2.0 の 2030 年までのロードマップである。ECHONET2.0 では、全ての人が Society5.0 のメリットを享受出来るよう、2020 年までに 1 億台の ECHONET Lite 搭載機器の普及、2025 年までに 200 種類の機器制御コマンドの定義、2030 年までに、全世帯に信頼できるホームコントローラの導入を目指す計画である。

1．2 用語

サービスサーバ	本書では、サービス事業者が運用し、機器管理サーバと連携することで各種サービスを提供するサーバを指す。
機器管理サーバ	本書では、コントローラと任意のプロトコルで通信し、家庭内の機器の情報の収集や各種サービスに必要な機器の制御指示を行うサーバを指す。
コントローラ	本書では ECHONET　Lite にて機器と通信し、各種制御、動作情報の取得を行うノードを指す。
機器	本書では ECHONET　Lite にてコントローラと通信し、各種制御、動作情報を提供するノードを指す。
Web API	HTTP(S)プロトコルを用いたシステム間のインタフェースであり、リクエスト／レスポンス方式でデータをやりとりする。本書では、特に呼び出される側のシステム（サーバ側）で提供されるものを指す。
Society5.0	サイバー空間（仮想空間）とフィジカル空間（現実空間）を高度に融合させたシステムにより、経済発展と社会的課題の解決を両立する、人間中心の社会（Society）。狩猟社会（Society 1.0）、農耕社会（Society 2.0）、工業社会（Society 3.0）、情報社会（Society 4.0）に続く、新たな社会を指す。
IoT 社会	これまで単独で存在していた端末／キーデバイス群が通信やプラットフォーム／ネットワークで相互につながりはじめ、集積されたデータを分析・制御することによる新たなサービス・アプリケーションを享受できる社会

1．3 参照規格及び参考文献

本書で参照する規格及び参考文献を以下に挙げる。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。

・参照規格

[EL]　The ECHONET Lite Specification
[APPENDIX]　APPENDIX 機器オブジェクト詳細規定
[AIF]　アプリケーション通信インタフェース（AIF）仕様書　※機器毎に仕様を規定

・参考文献

[1] Takashi Murakami et al., “COMPARISON OF IOT DEVICES ARCHITECTURE IN HOME NETWORK”, The 5th International Conference on Connected Smart Cities 2019 (CSC 2019)
[2] "サイバー・フィジカル・セキュリティ対策フレームワーク Version1.0", 経済産業省 商務情報政策局 サイバーセキュリティ課, 平成 31 年 4 月 18 日
[3] "IoTセキュリティガイドライン ver1.0", IoT推進コンソーシアム, 総務省, 経済産業省, 平成28年 7 月

第２章 想定するシステム構成と検討範囲

本章では、本書において想定しているシステム構成と検討範囲について記載する。

２．１ コントローラを用いたシステム

本節では、本書において想定しているシステム構成を記す。宅内にある各機器をインターネット上のサービスと接続するにあたり、システム構成としては大きく二通りが考えられる。

一つ目は、機器自身は直接インターネット上のサービスと接続せずに、宅内に設置するコントローラを経由してインターネット上のサービスと接続するシステム構成である。コントローラは各機器を制御したり、情報を取得したりする機能を持ち、インターネット上の機器管理サーバに接続する。インターネット上の機器管理サーバが様々な事業者のサービスサーバと連携して、ユーザにサービスを提供することが可能になる。

二つ目は､機器自身が直接インターネット上のクラウドサービスに接続するシステム構成である。機器は、自社の機器管理サーバに接続する。接続方法は、宅内に設置しているルータを経由して機器管理サーバに接続する方法や、LPWA や LTE などの通信網を介して接続する方法などがある。各社の機器管理サーバはそれぞれサービス事業者のサービスサーバと連携して、ユーザにサービスを提供する。

ECHONET2.0 における ECHONET Lite システムでは、図 2-1 に示すようなコントローラを用いたシステム構成を想定している。ただし、一部の機器は直接インターネット上のクラウドサービスに接続することも想定している。ホームネットワーク等、制御の対象となる機器や、機器を制御するサービスの多様性が高い場合には、前者のコントローラを用いたシステム構成は、後者の機器がクラウドサービスに接続するシステム構成と比較して、「システム構築」、「多種多様なサービスの実現」、「導入・運用コスト」といった観点でメリットが大きいと考えられる[1]。

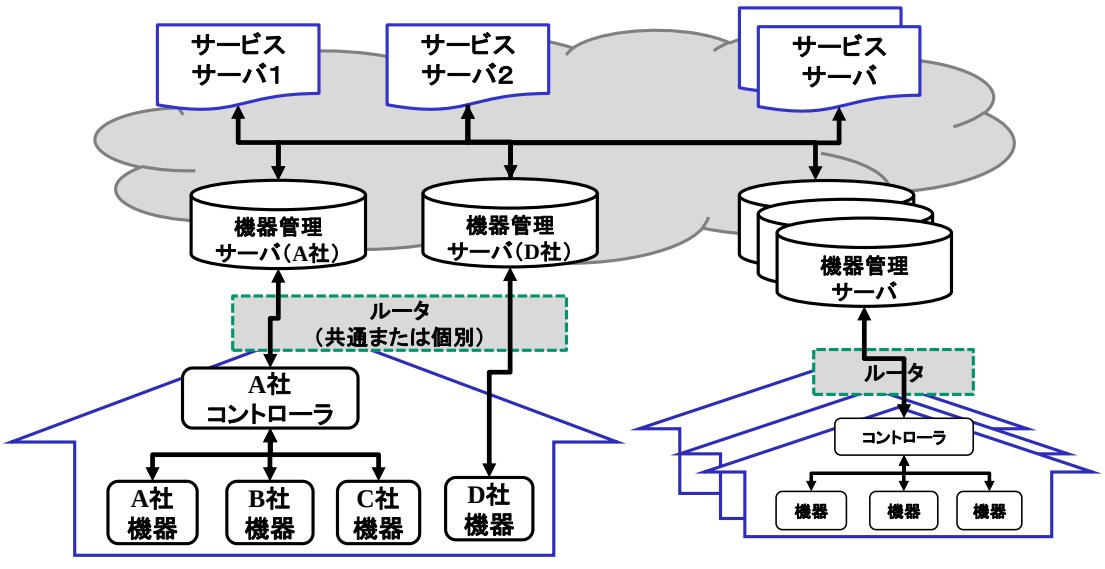


図 2-1　想定するシステム構成

2．2 検討範囲

ECHONET2.0 において、ECHONET Lite 機器が持つ情報をより活用し、クラウド上のエネマネ・ヘルスケア・その他サービスを実現するためには、様々な機器やサーバがつながるシステム全体での信頼性確保が必要となる。本節では、ECHONET Lite システム全体の信頼性確保に関する検討範囲を記す。

図 2-2 は、本指針における検討範囲の概略図である。本書では、ECHONET Lite 規格に関わる通信インタフェースを検討範囲とし、サーバの保守・運用、及び機器本体やコントローラ本体の製品安全対策などは検討範囲外とする。具体的には、図 2-2 に示されるように、各サービス事業者のサービスサーバと各社機器管理サーバとの間の通信インタフェース「I/F① サービスサーバ～機器管理サーバ間」、各社機器管理サーバと各社コントローラとの間の通信インタフェース「I/F② 機器管理サーバ～コントローラ間」、及び、各社コントローラと各社機器との通信インタフェース「I/F③ コントローラ～機器間」を、本書では検討範囲とする。

図 2-2 に示されるように、本書では、様々な企業から提供される機器を 1 つのコントローラで制御する、マルチベンダ環境を想定している。さらに、サービスサーバと機器管理サーバ及びコントローラを提供するベンダも異なる環境を想定している。上記のようなマルチベンダ環境において信頼性確保のためには、安定して安全につながる事、つまり相互接続性とセキュリティ対策が重要である。そこで、本書では、相互接続性とセキュリティ対策に焦点を当てて、システム全体の信頼性確保のための指針について述べる。

本節以降の第３章から第５章では、これら通信インタフェースごとに、通信の特性と信頼性の考え方について述べる。

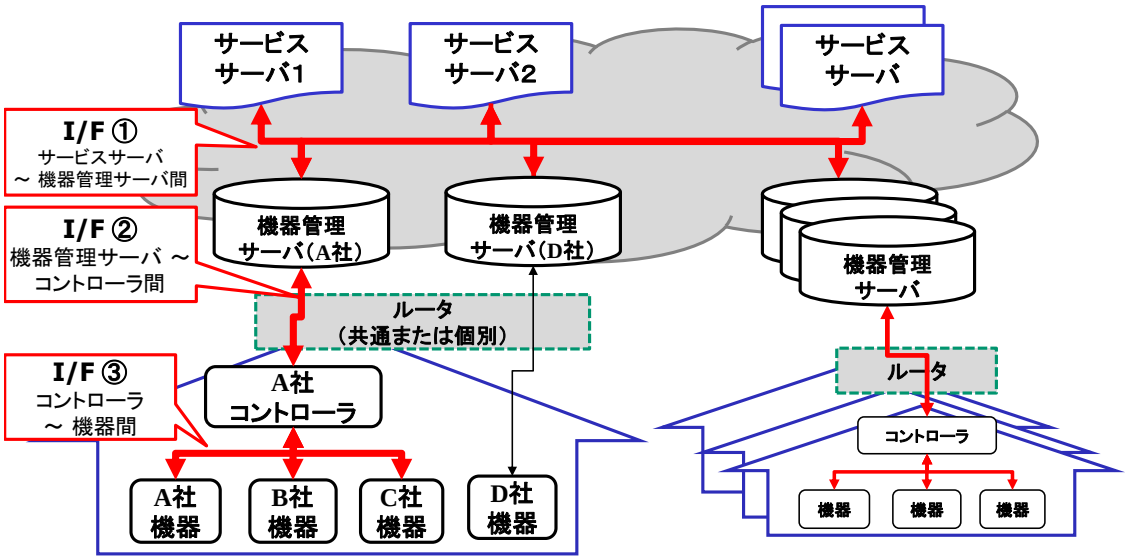


図 2-2　検討範囲

第３章 サービスサーバと機器管理サーバ間の通信のあり方

本章では、図 2-2 に記載のインタフェース「I/F① サービスサーバ～機器管理サーバ間」における通信のあり方について記載する。サービス事業者（サービスサーバ）は、各サービス（エネルギーマネジメント、ヘルスケア、他）を実現するために各種機器と接続している各社機器管理サーバと連携する。また、スマートスピーカーなどとの連携もインタフェース「I/F① サービスサーバ～機器管理サーバ間」によって実現される。

３．１ 想定するシステムにおけるサービスサーバと機器管理サーバ間通信の特性

様々なサービスサーバと各社機器管理サーバが連携するシステムでは、両者間で実現したいサービスに基づき、様々なデータの連携や共有が必要となる。本書では特に各社機器管理サーバが提供するリソース (データやサービスなど) に対して、サービスサーバから利用するモデルを対象に、要求される通信の特性について言及する。

本書では、一般的なモデルとして、サービスサーバと各社機器管理サーバの所有者が異なり、各々がインターネット上のサーバにて構築されるケースを想定する。

（a）各社機器管理サーバの所望リソースへのアクセス公開は、許可されたサービス事業者のサービスサーバに限定される。

インターネット上の機器管理サーバは、外部から（攻撃を含む）任意のアクセスを受けうるため、強固なセキュリティ対策を実施することが求められる。特定の信頼関係を結んだ相手のみにリソースアクセスを許可し、その他の不要なアクセスから各社機器管理サーバを守る仕組みが必要となる。

（b）各社機器管理サーバとサービスサーバの間でなんらかの認証機能や通信暗号化機能が適用される。

サービス事業者が各社機器管理サーバのリソースを利用するには、各社機器管理サーバがサービスサーバを認証・認可する仕組みが必要となる。また、逆にサービス事業者側のリソースも利用される場合は、双方向にて認証・認可する仕組みが必要となる。認証後に開始される通信内容について、適切な暗号強度を持った暗号化処理が実施されるべきである。さらに、各社機器管理サーバは、連携先の各サービス事業者に応じて、提供するリソースの範囲や種類を個別に設定できることが望ましい。

（c）各社機器管理サーバから提供されるリソースが適切なルール・スタイルに基づき利用可能となる。

提供リソースへのアクセス方法として、その手順やデータ形式・API 形式などのモデルについて、定式化された指針が構築・提示されていることが望ましい。統一性のないモデルが複数混在する機器管理サーバを利用する場合、同サーバのリソースへアクセスするサービス事業者側のプログラミングが煩雑化し、保守性や拡張性などの面で信頼性が劣化する恐れがある。

なお、高い信頼性を実現するためには、高信頼なストレージや冗長化サーバなどを用意するハードウェア面での検討や、障害回避（負荷問題回避）やシステム二重化、万一のシステムダウンや故障時に迅速な再開をするといった仕組みやシステム構成の検討など、稼働率を向上させるといった面（可用性）も考慮すべきだが、本書ではこうしたハードウェア面や運用面での特性については言及しない。

３．２ サービスサーバと機器管理サーバ間通信の信頼性の考え方

各社機器管理サーバがインターネット上に配置される場合、外部からの侵入やシステムダウン・レスポンス低下などを防ぐなど、機器管理サーバ上のリソースを保護する仕組みの導入が必須となる。一般的な構成としては、ファイアウォール（ネットワーク層への攻撃：ポートスキャンなどへの対策）、IPS/IDS（不正アクセス攻撃：DoS 攻撃、DDoS 攻撃など OS やアプリの脆弱性を狙ったものなどへの対策）、WAF（Web アプリケーションの脆弱性を利用した攻撃：SQL インジェクション、XSS など）をサーバプログラム（Web アプリケーション）の前段に配置する対策がとられるケースが多い。また、機器管理サーバが一般公開するリソースと特定相手先のみに限定公開するリソースの両方を持つケースでは、リソース単位でアクセス可能な相手やその範囲を指定できるシステムが必要となる。

サービスサーバと機器管理サーバ間でなりすましや否認防止、漏洩対策、改ざん防止といったセキュリティ対策を実施する場合、認証や通信暗号化の仕組みが必須となる。認証・通信暗号化には標準的な方式が複数存在し、サーバ間で VPN を張る方法など複数考えられるが、ここでは一般的な手法として HTTPS 通信（以降、SSL/TLS）を用いたケースについて触れる。議論を簡単にするために、本節では各社機器管理サーバ側をサーバ、サービスサーバ側をクライアントと呼ぶ。SSL/TLS では、サーバ認証とクライアント認証が可能となっているが、サーバ認証には証明書を用い、クライアント認証にはクレデンシャル（ID やパスワードといった認証情報）を用いる事例が多い。具体的には、サーバの証明書と公開鍵から暗号化した共通鍵を両者で共有し、その鍵で暗号化通信を実施する処理までを SSL/TLS にて実施し、サーバがクライアントからのリソースアクセスへの許可を（クレデンシャルを用いて）確認することになる。サーバが自身のリソースを単純にクライアントへ提供するケースであれば良いが、モバイルサービスのように、クライアントを経由してサーバリソースを利用するモバイルユーザの場合、クレデンシャルの扱いが問題になりうる。モバイルユーザがクライアントに対してクレデンシャルを提示したくない場合、別途許可サーバを用意し、アクセストークンの発行・やりとりによってサーバリソースを提供する仕組みが存在する。これは OAuth と呼ばれ、権限の許可を付与するオープンスタンダードであり、クラウドサービスの多くでサポートが広まっている。OAuth では、スコープを適切に設定することで、リソースに対するアクセス権の範囲を制限することも可能となっている。

昨今のサーバリソース利用に関しては、何らかの Web API を介して実現されるケースが多い。通常 Web API では、リソースの読み込み、書き込み、その他の操作などをサポートしている。データ伝送には主に HTTPS（HTTP）を用い、SOAP（通信プロトコル）や XML（メッセージ記

述）を用いるケースもあるが、近年では、REST（Web サービスの設計モデル）に基づき JSON（データ記述言語）を用いるケースが多い。サーバリソースは複数種から構成されるモデルも多く、個々に独立した設計思想にて実装・構築してしまうと、メンテナンスがしづらく、クライアントからの利用も煩雑化するなど、サーバプログラムの管理・品質面で信頼性を損ねる状況に陥る可能性もある。

サーバリソースの設計や利用に関して、なんらかの指針（ガイドライン）が統一的なスタイルにて規定され、これに準拠したサーバが構築されることが望ましい。また、サービス事業者（クライアント）の視点からは、同ガイドライン準拠のサーバであれば、異なる各社機器管理サーバであっても同様のインタフェースでプログラムを実装することができるため、コードの再利用性や複数の各社機器管理サーバのサービスリソースを跨った複合サービスの構築も容易になると考えられる。

エコーネットコンソーシアムでは、ECHONET で定義している豊富な機器の情報をベースにクラウドサーバ向きのインタフェース（Web API）を規定している。これは、ECHONET Lite Web API と呼ばれ、各社機器管理サーバが提携しているユーザ宅内の機器リソースを機器管理サーバ経由で（さらに統一的なスタイルで）扱うことを可能にしている。具体的には、機器の一覧取得、機器に対する SET 操作・GET 操作・通知操作などについて、Web API ガイドラインとして規定している。

この他、サービスサーバと機器管理サーバ間通信の信頼性に関連する事項として、通信品質（通信速度や帯域、データ欠損率など）、ミッションクリティカル性（パケット到達・順序保証、トランザクションなど）といった主にトランスポート層以下に関わる視点も重要となるが、本書では特に言及しない。

第４章 コントローラと機器管理サーバ間の通信のあり方

本章では、図 2-2 に記載のインタフェース「I/F② 機器管理サーバ ~ コントローラ間」における通信のあり方について記載する。各社機器管理サーバは宅内のコントローラを介して各種機器と接続し連携する。
ただし、ルータの設定や機能については本検討の対象外としている。

４．１ 想定するシステムにおけるコントローラと機器管理サーバ間の通信の特性

ECHONET Lite 機器を用いたシステムでは、通常、各社機器管理サーバは、自社のコントローラを介して各種機器を管理している。また、ECHONET Lite 規格では、コントローラと機器管理サーバ間の通信方式については規定していないため、この部分の通信方式の実装に関しては、各ベンダに任されている。

従って、本項では、コントローラと機器管理サーバ間の通信方式において信頼性を確保するために取り得る手段について、①通信経路、②通信プロトコル、③セキュリティ対策、④コントローラによる効果に関して、一般的な観点で記載する。

実際のシステム構築においては、それぞれの観点で、どのような方式を選択し、組み合わせるかにより、全体的な信頼性が影響を受けることとなる。一般的な傾向として、より信頼性の高い方式ほど、システムに要求される性能レベルも高くなるため、実際のシステムで、どの程度の信頼性を担保するかは、信頼性とシステム性能とのトレードオフの中で、各ベンダの判断に任されることとなるが、この部分のセキュリティ対策を高めることで、システム全体の信頼性を高めることが可能である。また、昨今のネットワーク環境におけるクラウド側の機能の高度化に伴い、コントローラの機能を宅内のコントローラ機器内ではなく、クラウド側 (機器管理サーバ内) に配置することも、技術的には可能となりつつある。ただし、この場合であっても、コントローラ機器とサーバを接続する構成自体は変わらないため、基本的には、本項で記載する内容で包含されるもの考え、このケースについては、ここでは言及しない。

４．２ コントローラと機器管理サーバ間の信頼性の考え方

① 通信経路

コントローラと機器管理サーバ間の代表的な通信経路構成を、図 4-1 に示す。

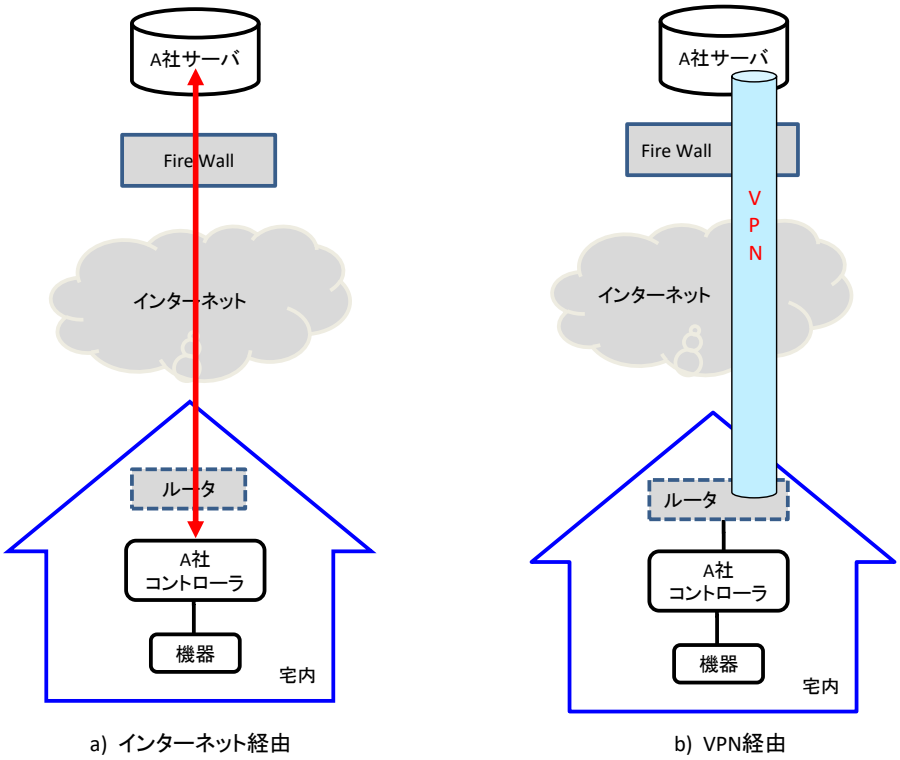


図 4-1　コントローラと機器管理サーバ間の代表的な通信経路構成

a) インターネット経由

対象システムが、一般ユーザを対象としたもので、コントローラが、一般家庭等、企業ネットワーク外に存在する場合には、インターネット経由で、コントローラと機器管理サーバが接続されることとなる。一般的に、インターネットにおいては、セキュリティは担保されないため、この場合には、何らかのセキュリティ対策を検討することが望ましい。

b) VPN 経由

通信経路としてインターネットを用いる場合等に、よりセキュリティを高める方法として、通信経路上に VPN を構築し、これを経由してコントローラと機器管理サーバを接続する方法が考えられる。VPN には、前述のようにインターネット VPN と ISP が提供する閉域網を利用する IP-VPN がある。VPN では、SSL/TLS、SSH、IPsec、PPTP、L2TP、MPLS といったセキュリティ技術が用いられており、信頼性の高い通信路となっている。

② 通信プロトコル

ECHONET Lite 規格では、OSI 参照モデルの第 3 層（ネットワーク層）および第 4 層（トランスポート層）に関しては規定がない。その一方、実際のシステムにおいては、この部分の通信プロトコルとして、UDP/IP または TCP/IP が用いられるのが一般的である。そこで、この場合に、第 7 層（アプリケーション層）で用いられる通信方式について比較する。

a) 標準的な通信方式を利用する場合

コントローラと機器管理サーバ間の通信では、通常、インターネット経由での接続を考慮し、Fire Wall(FW)を経由してセッションを張ることも想定してシステムを設計することが多いと考えられる。また、その場合、標準的な通信方式として、WebSocket や MQTT 等を用いて通信機能部を作成するケースが多い。

もっとも、コントローラと機器管理サーバ間の通信部分は、ECHONET Lite 規格で規定されていないため、通信プログラム自体は、ベンダ個別のものとなると想定される。とは言え、将来的に、この部分の通信機能部に関して、他社製通信機能部との連携を実現しようとした場合に改造規模を小さくできる可能性はある。

b) 独自方式を使用する場合

ECHONET Lite を用いたシステムでは、通常、コントローラと機器管理サーバは、同一ベンダにより構成される。そのため、この部分の通信プロトコルとして、当該ベンダの独自方式を実装することは可能である。この場合には、仮にコントローラが、外部から不正アクセスされたとしても、通信プロトコルが独自のものであれば、通信内容の流出は起きにくい可能性がある。

ただし、逆に、汎用性は低下することになるため、将来的にこの部分の通信機能部を他社製通信機能部と相互接続させる可能性を考慮するような場合には、適さないと考えられる。

③ セキュリティ対策

TCP/IP 通信におけるセキュリティ対策としては、一般的に、以下の方式が考えられる。基本的には、サービスサーバと機器管理サーバ間通信の場合と同様の手法が適用可能である。

a) 認証方式

サービスサーバと機器管理サーバ間通信の場合と同様に、コントローラと機器管理サーバの接続時にも、不正なアクセスを排除するため、双方とも、相手が正しいコントローラまたは機器管理サーバであるかを認証し、アクセスを制御することが望ましい。

b) データの暗号化

システムの信頼性を高める意味では、万一、外部から不正なアクセスがあった場合でも、データの外部流出を防ぐため、データに暗号化処理を施しておくことは有効と考えられる。

ただし、データの暗号化を行う場合、その分、システム全体の処理性能が低下することが懸念されるため、データ保全とシステム性能とのバランスを取ることが重要となる。

④ コントローラによる効果

ECHONET Lite を用いたシステムでは、機器管理サーバが、直接、機器を管理・制御するのではなく、間にコントローラを設置し、コントローラが機器を管理・制御したうえで、必要な情報のみを機器管理サーバに送信している。これにより、機器の持つ情報のうち、不必要な情報は機器管理サーバへは送られないこととなり、その分、信頼性が高いシステムを構築することができる。

第５章 コントローラと機器間の通信のあり方

本章では、図 2-2 に記載のインタフェース「I/F③ コントローラ ~ 機器間」における通信のあり方について記載する。機器管理サーバより各種要求を受けた宅内のコントローラはマルチベンダ機器と連携し、各種サービスを実現する。

５．１ 想定するシステムにおけるコントローラと機器間の通信の特性

信頼性について、本文書が対象とする相互接続性と通信のセキュリティについて検討する際に考慮すべき、コントローラと ECHONET Lite 機器間の通信の特性を以下に説明する。

(a)　コントローラ、および、機器はマルチベンダ機器と接続する必要がある。
コントローラと機器のベンダは必ずしも同じとは限らない。また、1 台のコントローラと通信する複数の機器のベンダが異なる場合がある。

(b)　ユニキャスト通信だけでなくマルチキャスト通信も使用する。
マルチキャストによる INF 通知、ネットワークに存在する機器を発見するためのマルチキャストによる Get 要求など、マルチキャスト通信を使用する場合がある。

(c)　コントローラと機器間の通信に対して認証、秘匿、改竄防止の対策を行う場合、現状はレイヤ 4（Layer4、トランスポート層）以下のメディアの規定に従う。

５．２ コントローラと機器間の相互接続性

コントローラと機器間の相互接続性を検討する上で、5.1 の(a)で説明したマルチベンダ環境を考慮することが必要となる。マルチベンダ環境においてコントローラと機器間の相互接続性を向上させるために、ECHONET Lite は以下の 2 種類の手段を提供している。コントローラ、または、機器のベンダは、以下の手段の中から必要なものを利用することで、マルチベンダ環境での相互接続性を向上させることができる。

(1)　ECHONET Lite 規格、ECHONET Lite 認証試験、および、プラグフェスト

ECHONET Lite 規格は、ECHONET Lite に準拠するコントローラと機器が従うべき通信インタフェースを規定している。この規定に従うコントローラと機器を開発することで、コントローラと機器間の相互接続性を担保することが可能になる。

ECHONET Lite 認証試験仕様書は、コントローラと機器が、ECHONET Lite 規格に準拠していることを確認するための試験項目を規定している。コントローラ、または、機器のベンダは、ECHONET Lite 認証試験仕様書が規定する試験項目を実施・確認することで、自社製品が ECHONET Lite に準拠していることを確認可能となり、相互接続性を向上できる。

また、異なるベンダの ECHONET Lite 準拠のコントローラと機器の間の相互接続性を実際に確認するため、エコーネットコンソーシアムが定期的にプラグフェストを実施している。プラグフェストに参加することで自社製品と他社製品の相互接続性を確認し、相互接続性上問題となる箇所の検出・改善を行うことができる。

(2)　アプリケーション通信インタフェース（AIF）仕様、および、AIF 認証試験

AIF 仕様書は、重点 8 機種等の個々の機種に対して策定されており、ECHONET Lite を用いて通信するコントローラと機器の相互接続性をより高めるため、ECHONET Lite を用いる通信手順に関する機種固有の追加仕様を記述している。AIF 仕様書に従うコントローラと機器を開発することで、コントローラと機器間の相互接続性を担保することが可能になる。

AIF 認証試験仕様書は、コントローラと機器が、AIF 仕様に準拠していることを確認するための試験項目を規定している。コントローラ、または、機器のベンダは、AIF 認証試験仕様書が規定する試験項目に基づく AIF 認証を第 3 者機関から取得することで、自社製品が AIF 仕様に準拠していることを確認可能となり、相互接続性を向上できる。

5．3 コントローラと機器間の通信のセキュリティ

通信のセキュリティにおいて考慮すべき点に以下の 3 つが含まれる。

(1)　通信相手の認証（認証）
コントローラ、または、機器が通信する相手が、システムが想定する相手ではない状態の発生を防ぐために認証が必要となる。
(2)　通信内容の秘匿（秘匿）
通信内容が、通信の相手以外の第三者に知られることを防ぐために秘匿が必要となる。
(3)　通信内容の改竄防止（完全性）
通信内容が、通信の相手以外の第三者により改変されることを防ぐために完全性が必要となる。

ECHONET Lite 機器を用いたシステムでのコントローラと機器間の通信において、上記の認証、秘匿、完全性の 3 点を担保するための対策は、システムに対するリスク分析の結果に基づいて選択する性質のものであり[2][3]、対象システムにより適用する対策が異なる可能性がある。また、対策の選択にあたっては、5.1 の(b)と(c)で説明したコントローラと ECHONET Lite 機器間の通信の特性を考慮することが必要となる。以下に、いくつかの対策例を説明するが、以下に示す例以外の対策が適切な場合も有り得る。

5．3．1 ケース 1

ECHONET Lite におけるユニキャスト通信とマルチキャスト通信に、下位層での規定で認証、秘匿、完全性を適用するケースである。ユニキャスト通信とマルチキャスト通信の両方に認証、秘匿、完全性を適用する方法の例として、エコーネットコンソーシアムが、AIF 認証を取得した機器を対象に仕様を策定し適用方法を検討中の機器認証（DA: Device Authentication）仕様が挙げられる。

DA 仕様は、ユニキャスト通信とマルチキャスト通信の両方に認証、秘匿、完全性を提供するだけでなく、コントローラ、または、機器が AIF 認証を取得済みのものか否かを判別する機能も提供する。このため、DA 仕様を適用して、AIF 認証を取得したコントローラと機器間の通信のみを許可することで、コントローラと機器間の相互接続性を向上させる効果も期待できる。

５．３．２ ケース２

ECHONET Lite におけるユニキャスト通信に、下位層での規定で認証、秘匿、完全性を適用するケースである。システムにおける ECHONET Lite のマルチキャスト通信の使用方法を制限し、マルチキャスト通信については認証、秘匿、完全性を適用しなくてもリスク分析結果に対する対策がとれる場合を想定する。例えば、マルチキャストの INF で通知される内容をそのまま使用せず、INF を受信後、必ず INF の送信元にユニキャスト通信で Get を送信してプロパティ値を確認するようにして、マルチキャストの Get/SetC/SetI に対しては Get_SNA/SetC_SNA/SetI_SNA で応答することで機器の存在は知らせるが、ユニキャスト通信の Get/SetC/SetI のみ受理するようにすることが考えられる。ユニキャスト通信に認証、秘匿、完全性を適用する方法の例として、[EL]第 2 部 1.2 (1)に書かれている DTLS や IPSec が挙げられる。

５．３．３ ケース３

下位層の規定での通信の認証、秘匿、完全性を適用しないケースである。例えば、一般の家庭内に設置されるコントローラと ECHONET Lite 機器を接続するネットワークについて、家の施錠管理と、「無線 LAN の接続認証」＋「秘匿」＋「完全性」により、ネットワークに接続するコントローラと機器を限定可能で、かつ、コントローラと機器が不正動作をしないと、リスク分析の結果判断した場合を想定する。この場合、下位層の規定での通信の認証、秘匿、完全性を適用しないという対策を適用できる可能性がある。

第６章 おわりに

インターネットを含めた ECHONET Lite 機器を用いたシステムは、ECHONET Lite 規格に対応した各種機器とコントローラ、及び機器管理サーバとサービスサーバから構成される。これら構成要素は、全て異なる事業者により提供される可能性があり、このようなマルチベンダ環境において信頼性を確保するためには、相互接続性とセキュリティ対策が重要である。

本書では、各サービスサーバと各社機器管理サーバ間の通信インタフェース、各社機器管理サーバと各社コントローラ間の通信インタフェース、及び、各社コントローラと各社機器間の通信インタフェースを検討範囲として、相互接続性とセキュリティ対策に焦点をあてて、通信の特性と信頼性の考え方を整理した。

ECHONET Lite 機器を用いたシステムは、本書に示したように ECHONET Lite 規格、ECHONET Lite AIF 仕様等への準拠、Web API ガイドラインへの対応により相互接続性の向上を図ることができ、適切なセキュリティ対策を行うことでシステム全体での信頼性を確保可能なシステムである。このことから、ECHONET Lite 機器は今後の IoT 社会に資するものである。