1F-5

Managed M2M システム技術(2)
－インターネットを介した安全な即時制御を実現－

釜坂　等　　道下　学　金子　洋介
三菱電機株式会社　情報技術総合研究所

1. はじめに

近年、ブロードバンド環境の浸透により、ネットワークに接続し統合的に制御・監視が可能な制御機器を、インターネットから遠隔で制御・監視するニーズが高まってきた。

しかし、システム構築は高価であったり、インターネット接続環境が制限されたり、制御機器側にサーバ機能を持たせためにブロードバンドルータの設定変更が必要であるなどいくつかの課題がある。

そこで、インターネット接続環境に依存せず、安全でかつ即時制御を用いた遠隔制御・監視するため必要なセッション確立技術を開発したので報告する。

2. Managed M2M システム技術

2.1. 機能と特長

Managed M2M システム技術[1]とは、インターネットを活用してビル内の設備機器を遠隔から集中的に管理するための技術である。

本稿では、図 1に示す本システム技術のアーキテクチャの内、セッション管理層について述べる。

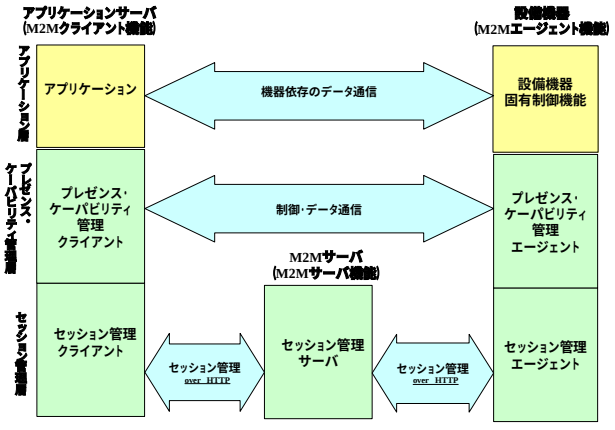

図 1 Managed M2M システム技術アーキテクチャ

Managed M2M System (2)-Session Management-.
HITOSHI KAMASAKA, MANABU MICHISHITA, and YOSUKE KANEKO
Information Technology R&D Center, Mitsubishi Electric Corporation

3. セッション管理層

セッション管理層では、ISP(Internet Service Provider)やルータなどのインターネットへの接続環境に非依存で、安全かつ即時制御可能なセッション確立を実現する。

3.1. セッション確立の課題

インターネットを介して機器とセッションを確立するためには、いわゆる NAT(Network Address Translation)越え問題がある。具体的には、インターネットから制御対象機器の IP アドレス指定が出来ない、ルータのインバウンド設定が必要であるなどの課題がある。

また VPN (Virtual Private Network)による解決もあるが、高価であったり設定が複雑であったりなどの課題がある。

3.2. 環境非依存なセッション確立の実現方式

セッション確立には、設備機器からの HTTP のアウトバウンドによる通信のみを用いる事で、通常の Web ブラウジング環境がそのまま利用できる。したがって、ISP やルータに依存しない。また、グローバル IP アドレスが必須ではなく、Web プロキシーやファイアウォールが存在する環境でもセッション確立が可能である。さらに、ルータの NAT テーブルなどの設定が不要である。

3.3. 安全なセッション確立の実現方式

アウトバウンド通信だけを用いる方式により、IP アドレスの公開を不要とし、サーバ機能を持たないことによりアタックを受けにくい。また、通常の Web アクセス時に設定されている NAT あるいはファイアウォールによる安全性をそのまま利用できる。

3.4. 即時制御可能なセッション確立の実現方式

M2M サーバの中継方式により、即時性のある通信セッションを実現する。具体的なセッション確立のシーケンスを図 2に示す。

この図では、M2M クライアント機能（監視アプリケーション等）から M2M サーバを経由して M2M エージェント機能（設備機器等）に対して、セッションを確立して、遠隔制御を行うシーケン

スを示している。

セッション確立は、シグナリングフェーズと制御フェーズから構成される。

(1)シグナリングフェーズ：即時に接続要求をM2Mエージェントに通知する部分である。

- M2Mエージェント：常時、M2Mサーバに対して、接続要求の確認要求を投げる。
  - タイムアウトを受信：再度、同リクエストを投げる
  - 制御要求を受信：制御フェーズに移る。
- M2Mサーバ：M2Mエージェントからの接続要求の確認要求を、M2Mクライアントから該当M2Mエージェントへの制御要求があるまで、あるいは別途規定したタイムアウト時間待つ。
  - タイムアウトが発生：タイムアウトをM2Mエージェントに返す。
  - 制御要求を受ける：接続要求をM2Mエージェントに渡す。

(2)制御フェーズ：M2Mクライアントから M2Mエージェントへの遠隔制御の実行を行う

- M2Mエージェント：接続要求を受けると認証等を行い、接続許可を発信する。そのリプライとして、コマンドを受信・実行し、その結果をM2Mサーバに送付する。
- M2Mサーバ：M2Mクライアントからの接続要求・コマンドをM2Mエージェントへ、M2Mエージェントからの接続許可・コマンド処理結果をM2Mクライアントへ、中継する。
- M2Mクライアント：接続要求およびコマンドをサーバに渡し、その処理結果をそのレスポンスで得る。

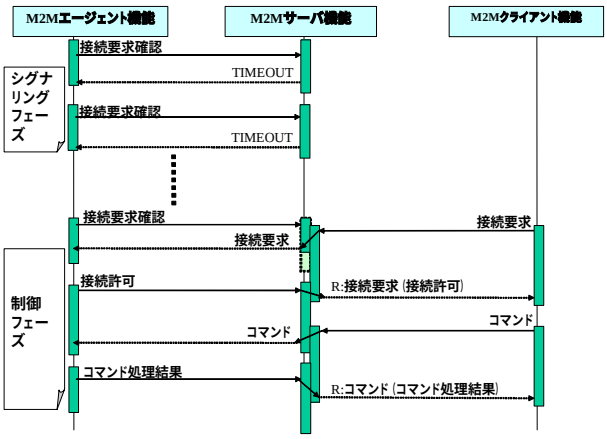

図 2　シーケンス図

3.5.　他のリモート制御方式との比較

一般的な NAT 越え問題を解決するリモート制御方法として、機器からサーバに HTTP ポーリングする方法や DDNS(Dynamic Domain Name System)を利用する方法などがある。これら方式との比較を行ったのが、表 1である。

これより、本方式は、環境への依存性が少なくかつ、安全で即時制御が出来る方式であるといえる。

表 1　比較表

	DDNS	HTTP ﾎﾟｰﾘﾝｸﾞ	本方式
環境非依存性	△ (*1)	○	○
安全性	△ (*1)	○	○
即時性	○	△(*2)	○

*1)機器（正確には機器に接続されたルータの）の不定グローバル IP アドレスを DDNS サーバに登録し、ルータでは、特定ポートを開けておく。機器側ではその特定ポートからアクセスを待つ。端末からは DDNS で機器を指定してアクセスする方法。この方法では、アドレスの公開やポートを開くなどセキュリティ上で問題がある。またローカル IP アドレスを付与する ISP では使えない。

*2)端末からコマンドをサーバに送る。機器から定期的にサーバにコマンドの有無を確認する。コマンドがあれば実行し、次のポーリングで結果を返す。ポーリング間隔が、制御されるまでの遅延に影響する。

3.6.　効果

本方式ではネットワーク環境に非依存であるため、既存の Web 環境がそのまま利用して、安全でかつ即時制御が可能なセッション管理が実現できる。また、M2Mエージェント機能は WWW プロトコルのクライアント機能のみを利用しているため、軽い実装が可能となる。

4.　おわりに

本システムのプロトタイプシステムを構築し、ブロードバンドルータ経由の ADSL 及び FTTH 回線を用いた環境や、企業内の Web プロキシー経由の Web ブラウジング可能な環境において、ルータ等の設定を変更せずに、既存の安全な環境の状態で、即時制御できることを確認した。

今後は M2M エージェント機能の制御機器への実装検討を行う。

参考文献

[1]金子他:"Managed　M2M システム技術(1)－複数の機器の統一的な遠隔制御と遠隔監視を実現－",情報処理学会 第 68 回全国大会,2006/3