M2M ネットワークにおける簡便かつセキュアな機器ペアリング方式

中嶋　純　　八百　健嗣
福井　潔

近年、健康機器（例：血圧計）や住設機器（例：電力メーター）などの機器が、通信モジュールを搭載してネットワークシステムに組み込まれるようになってきた。

こうした機器を相互に連携させるためのシステムは、M2M（Machine-to-machine）システムと呼ばれ、その具体的なアーキテクチャがETSI TC M2MやoneM2Mといったフォーラムの場で審議されている。

機器に組み込まれる通信モジュールは、一般に低コスト化が要求されることから、処理能力や、メモリ容量、ユーザーインタフェースに乏しい。そのため、通信モジュールを搭載した機器をM2Mシステムのネットワーク（以下、M2Mネットワークと呼ぶ）に追加するとき、暗号鍵のような機密性の高い情報を、どのように簡便かつ安全に設定するかが問題となる。本稿では、この問題を考察すると共に、その一解決方法を提案する。

無線ネットワークへの参加におけるセキュリティ

無線ネットワークでは、有線ネットワークと異なり、配線による接続機器の分離ができない。そのため、機器は、ユーザーが所望するネットワークにのみ参加し、親機は、ユーザーが承認した機器のみ参加させるようにすることが望ましい（**図 1** ）。

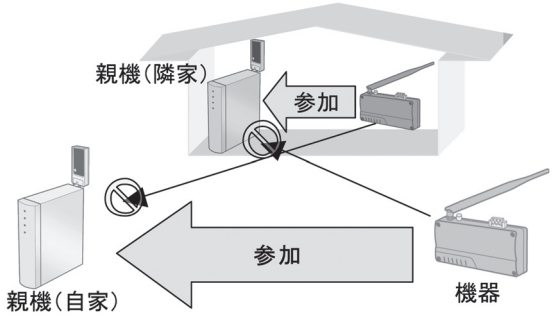

図 1　機器の参加管理の必要性

ネットワークへの参加機器を管理する手法の一つにMACアドレスフィルタリング法がある。この方法では、各機器が、受信したパケットのヘッダ情報に含まれている送信元MACアドレスを参照し、予め登録されているMACアドレスを含む受信パケットのみを受け入れることで、ネットワークへの参加機器を制限する。しかしMACアドレス情報は、電波をモニタリング（電波盗聴）することで簡単に分かってしまうため、MACアドレスフィルタリング法では、なりすましによる不正接続を防げないという問題がある。

このようなアドレスなりすましにより、具体的な脅威が想定される場合には、機器の参加に際して暗号技術を用いた認証を行う方法が有効である。

例えばOKIが提唱しているIP統合モデル[1]では、IPネットワーク上の認証サーバーを利用して機器の参加を管理する方法（以下、認証サーバ利用型認証）がオプションとして用意されている。認証サーバー利用型認証では、予め各参加機器に、認証サーバーで認証を受けるための情報（認証情報）をインストールしておき、各参加機器は、親機を経由して上位の認証サーバーに認証されることにより、その親機への接続が許可される。

一方、認証サーバーを利用できない個別のネットワークでは、予め認証情報をインストールすることができないため、機器の設置時に、ユーザーによる設定が必要になる。以下、本稿では、このユーザーによる設定を、機器と親機とを結び付けるという意味で、「機器ペアリング」と呼ぶ。ここまでに説明してきた機器の参加管理手法を **図 2**にまとめる。以下では、機器ペアリングにおける問題について考察する。

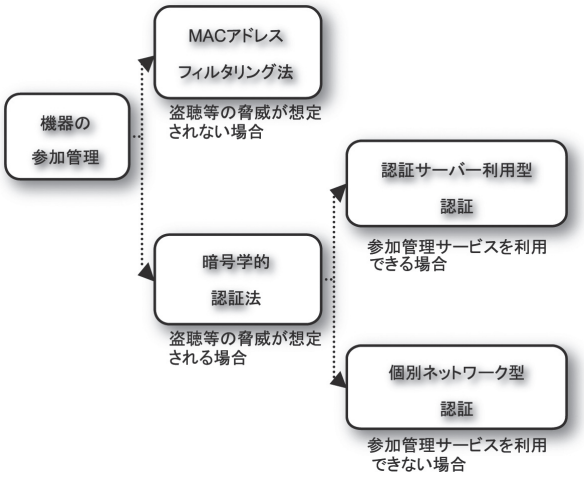

図2　ネットワーク参加管理の形態

機器ペアリング問題のモデル化

機器ペアリングにおける問題は、機器の関連付け操作と鍵共有の、二つの要素からなると考えられる。

機器の関連付け操作では、機器を所望の親機（ネットワーク）に参加させたいというユーザーの意図を、如何に簡便な操作でシステムに伝えるかが課題である。ここには、機器ペアリング後に、機器が確かにネットワークに参加できていることをユーザーが確認することも含まれる。

一方鍵共有では、親機が機器を認証するのに使用する共通の秘密鍵情報（以下PSK : Pre-Shared Keyと呼ぶ）をどのように安全に共有するかが課題である。

機器ペアリングの既存方式

本節では、無線LAN等で利用される既存の機器ペアリング法を整理し、これらの既存方法をM2Mネットワークに適用したときの問題を考察する。

前節の機器ペアリング問題のモデル化を踏まえ、**図 3**に既存の機器ペアリング法を図式化する。機器ペアリング法は、上段の関連付け操作の方法と、下段の鍵共有の方法の組み合わせであり、既存の方式としては、以下の3通りが代表的と考えられる。

①手動入力　（上段）　×　手動入力　　（下段）
②押しボタン（上段）　×　PSK直接配送（下段）
③押しボタン（上段）　×　公開鍵暗号　（下段）

機器ペアリング法①は、例えば無線LAN親機のSSIDとキーを、無線LAN子機に直接入力する方法である。本手法を、本稿で想定するM2Mネットワークシステムに適用する場合、ユーザーが親機に参加機器のIDとキーを直接入力し、参加機器は認証に成功する親機を見つけることでネットワークに接続するものと想定される。この方法では、機器ごとにインストールされたIDとキー（文字や数字の羅列）をユーザーが親機に入力することが煩雑であり、また機器のキーは第三者による不正な漏洩を防ぐために人目の付かない所に保管する必要がある。

機器ペアリング法②は、現在の無線LAN向け簡易設定方式AOSS™[5]（AirStation One-Touch Secure System)*1) や、TVセットとリモコンをペアリングするZigBee RF4CE™*2) に代表される方法である。この方法では、親機と機器にボタンが備え付けられており、一定時間内にボタンを押している機器同士が関連付けられる。

鍵共有には、例えばZigBee RF4CEの場合、分散鍵配送方式[2] が利用される。分散鍵配送方式は、秘密分散技術を用いた符号化方式を利用することで盗聴に耐性

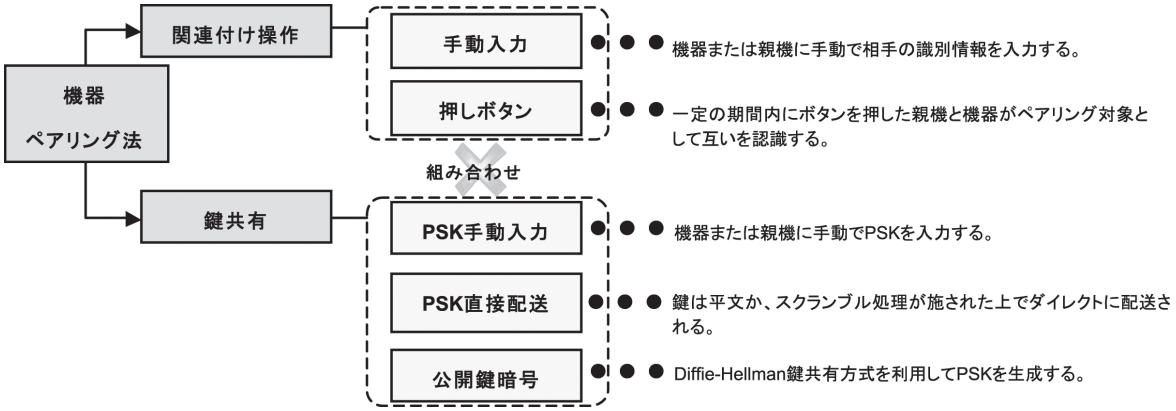

図3　機器ペアリングの既存技術

*1）AOSS は株式会社バッファローの登録商標です。　*2）ZigBee および ZigBee RF4CE は、ZigBee Alliance の登録商標です。

をもたせている。ただし、盗聴機器の受信感度が高い場合には、PSKが復号化されてしまう可能性がある。

機器ペアリング法③は、無線LANの簡易接続方式であるWPS (Wi-Fi Protected SetupTM)[*3] に代表される方法である[4]。関連付け操作は、方法②と同じボタンプッシュであり[*4]、鍵共有には公開鍵暗号技術であるDiffie-Hellman鍵共有方式を利用する。本鍵共有方式は、暗号学的安全性（計算量的安全）が理論的に評価されており、PSKを盗聴したり推測したりすることは困難である。ただしメモリ容量と計算時間（消費電力）の観点から、計算リソースが乏しい機器には実装が困難なケースが考えられる[*5]。

上述したように、既存方式では、安全性・簡便性・低リソース性を両立することは難しい。そこで本稿では、スマートフォンと、PSKを配信するサーバーを組み合わせた新しい機器ペアリング方式を提案する。

提案機器ペアリング方式

提案機器ペアリング方式では、関連付け操作は、スマートフォンのカメラで機器のQRコードを読み取ることで完結し、また鍵共有では、各機器のPSKをPSK配信サーバーが保管し、親機へ安全に配送することで、機器に計算等させることなく、安全に鍵共有することができる。

以下、**図 4**を参照しながら提案する機器ペアリング作業の流れを説明をする。**図 4**において、HGW（ホームゲートウェイ）は家庭におけるM2Mネットワークの親機であり、既存のIP網にも接続する機器である。

PSK配信サーバーは、ユーザーデータベースと、機器の鍵管理データベースをもっている。

また機器には、製造時に機器個別のPSKがインストールされており、機器のIDとPSKのコピーがPSK配信サーバーにおける機器の鍵管理データベースに登録されている。尚、PSK配信サーバーとスマートフォン間（またはHGW間）は、それぞれSSL暗号方式により、通信路上の盗聴・改ざんに対して安全になっている。

（1）事前設定ステップ

AさんがHGWを購入したとき、PSK配信サーバーのユーザーデータベースに、Aさんが当該HGWを所有することが登録され、AさんにはPSK配信サーバーにログインするためのQRコード（ユーザーID、パスワード）が印刷されたカードが発行される。

（2）機器ペアリングステップ

いま、Aさんは、無線温度センサー（参加機器）を購入してきたとする。

①Aさんはまず、スマートフォンを用いて（1）で発行されたログイン用QRコードを読み取り、PSK配信サー

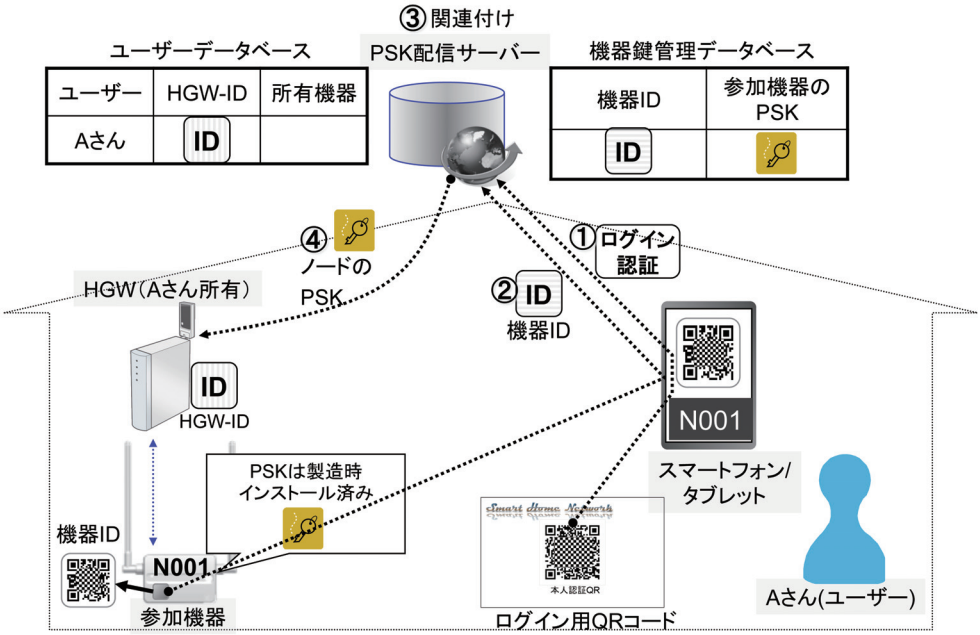

図 4　提案機器ペアリング方式

*3）Wi-Fi、WPS は Wi-Fi Alliance の商標または登録商標です。　*4）機器にランダムな数字（PIN）を一時的に表示させ、これを親機に入力する方法もある。
*5）例えば 8bit、8MHz のマイコンと TinyOS を搭載した機器で ECDH を実装した場合、ROM が 8KB、RAM が 150Byte、実行時間が 31 秒程かかることが報告されている[3]。

バーにログインする。

②続いて、ログインしたスマートフォンを用いて、温度センサーに貼り付けられている機器ID（QRコード）を読み取り、PSK配信サーバーに送る。 **図 5**は機器ID読み取りの参考イメージ図である。

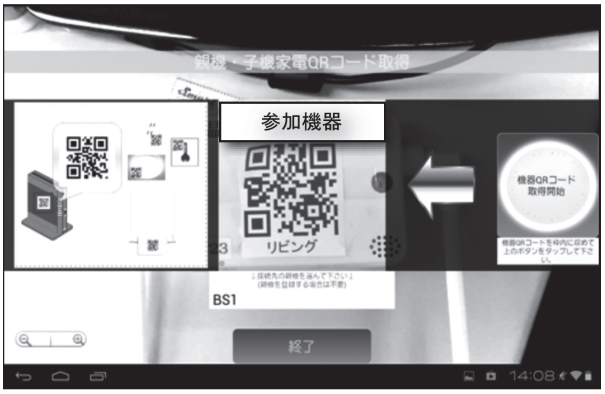

図 5　機器 ID の読み取り画面

③PSK配信サーバーでは、当該温度センサーがAさんの所有物になったことをユーザーデータベースに登録し、登録が完了したことをAさんにメールで通知する。

④Aさんが温度センサーの電源を入れ、温度センサーがHGWに仮接続を行うと、HGWはPSK配信サーバーに温度センサーのPSKを問い合わせる。PSK配信サーバーは、HGWがAさんのHGWであることを確認すると[*6]、温度センサーのPSKをHGWに配信する。

以上によりPSKがHGWと機器の間で共有される。この後温度センサーは、認証に成功する親機を探し、このHGWのネットワークに参加する。

筆者らは、提案方式を実際に実装し、機器1台の登録作業（読み取りからサーバ登録完了まで）が通常3秒程かかることを確認した。

特徴の考察

既存のボタンにより関連付ける方式では、関連付けたい機器同士のボタンを押すだけなので、ユーザーに直感的な操作性を与えることができる。一方、機器には押しボタン以外にも機器ペアリングの成否確認のためのLEDなどの装置も必要であり、これらが搭載困難な機器には適用できない。

一方提案法では、確認や修正といった操作も、スマートフォンのタッチ画面を通して行うことができる。

またPSK配信サーバーを利用する利点として、誤接続を防止できるだけでなく、自分の機器が他人のネットワークに勝手に参加させられた場合には、前述のペアリングステップの③でユーザーにメールで通知するなどの方法で警告することが可能である。

今後について

QRコードの読み取り作業では、光の反射等で読み取りが失敗する場合があり、ユーザーはこの間、スマートフォンを静止させる必要がある。この点を含めてユーザビリティの更なる向上が課題であると考えている。

上記に加えて、PSK配信サーバーの運用コストや、機器ベンダとの連携方法など、実運用面も含めたソリューションモデルを、今後検討する必要がある。◆◆

■参考文献

1）橋爪洋 他：920MHz 帯無線マルチホップネットワークシステム、OKIテクニカルレビュー221号、Vol.80 No.1、pp.18-23、2013年5月

2）T. Yao, etc., “Initial Common Secret Key Sharing using Random Plaintexts for Short-range Wireless Communication，” IEEE TRANSACTIONS ON CONSUMER ELECTRONICS，Vol.55 No.4，pp.2025-2033， Nov. 2009

3）A. Liu and P. Ning, “TinyECC: A configurable library for elliptic curve cryptography in wireless sensor networks,” Technical Report TR-2007-36, North Carolina State University, Department of Computer Science, 2007

4）Wi-Fi Alliance , “Wi-Fi Protected Setup Specification Version 1.0h,” December 2006

5）Buffalo Technology(USA), Inc. : AirStation One-Touch Secure System(AOSSTM), http://www.buffal otech.com/content/files/resource_center/AOSS_Whitepaper.pdf, October 2004.

●筆者紹介

中嶋純：Jun Nakashima. 研究開発センタ スマート社会ビジネスイノベーション推進部

八百健嗣：Taketsugu Yao. 研究開発センタ スマート社会ビジネスイノベーション推進部

福井潔：Kiyoshi Fukui. 研究開発センタ スマート社会ビジネスイノベーション推進部

*3）HGW を機器認証する方法としては、例えば EAP-TLS 等の機器認証プロトコルを利用することができる。