組み込み機器の ネットワーク参加登録と鍵確立

八百　健嗣　　中嶋　純

近年、パソコンによって形成される情報通信ネットワークだけでなく、センサ機器やデジタル情報機器などの組み込み機器によって形成される組み込みネットワークが提案されている。組み込み機器をネットワーク化することにより、さまざまなサービスの登場が期待できる。たとえば、プレゼンス情報と連動して機器の電源を制御したり、温度センサから収集した室内の温度分布を元に冷暖房機器を制御したりする省エネ制御、各世帯の電気やガス等の検針メータ値の自動収集、および、変動する料金単価や使用料金の実時間通知、体温・脈拍・血圧などの生体情報の自動収集、および、遠隔の医師や家族への健康状態通知、家庭内の家電製品や情報機器の制御／遠隔制御などがある。以上のサービスには、双方向ではなく単に組み込み機器から情報を収集するだけのネットワークも含まれる。しかし、このようなネットワークにおいてもセキュリティを軽視できない。組み込み機器から収集したデータがプライバシ情報となる場合があるし、他の機器にとっての制御情報となる場合もある。特に、本稿で想定するような無線通信を利用して情報を交換する組み込みネットワークでは、通信データの盗聴や不正投入が容易である。パソコンによる無線ネットワークと同様に、ネットワークに参加する組み込み機器（ノード）を参加登録すると共に、必要に応じて通信データを暗号化／認証することが要求される。

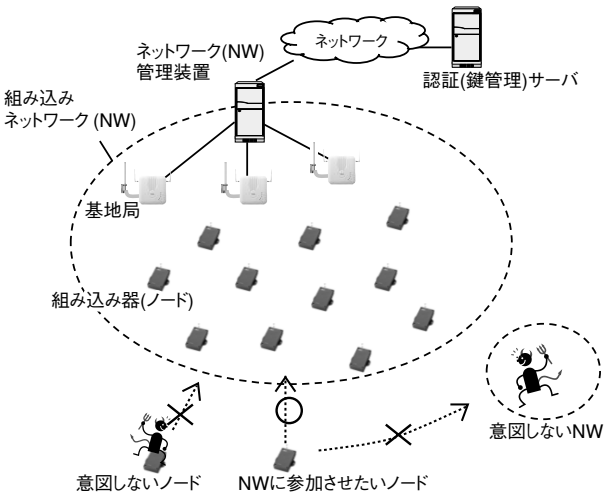

図1　組み込みネットワークのシステム構成

組み込みネットワークのシステム構成例を**図1**に示す。**図1**において、ネットワーク管理装置とは、同一の識別子を持つネットワーク全体を管理する装置であり、複数の基地局と接続しても良いし、基地局と同一の装置であっても良い。また、認証（鍵管理）サーバとは、ノード固有の情報を一括で管理するサーバである。ノードをセキュアなネットワークへ参加させるためには、以下の2つの機能を実現する必要がある。

- ノード登録機能：ネットワークに意図したノードだけを参加させる。また、ノードを意図したネットワークだけに参加させる。
- 鍵確立機能：ネットワーク内で送受信される通信データを暗号化／認証するための鍵をノードに設定する。

本稿では、ネットワークへの参加登録方法と鍵確立方法について整理し、組み込みネットワークへの適性を考察する。さらに、上述の鍵確立機能を実現する一手法として、分散配送を利用した鍵共有方式を提案する。

ネットワークへの参加登録方法と鍵確立方法の整理

ネットワークへの参加登録方法および鍵確立方法を整理した結果を**表1**に示す[1)]。

ネットワークへの参加登録方法は、登録作業実施者によるアシスト利用、識別子利用、秘密情報利用の3つに大別できる。また、ネットワークへの参加登録方法として、**表1**に記載の複数の方法を組み合わせることもできる。たとえば、登録作業実施者によるアシストの下で一定時間内に接続要求を送信したノードが、システム全体で既定される共通の秘密情報を保持していることを確認することでネットワークへの参加を許可したり、登録リストで事前に登録が許可されたノードが、そのノード固有の共通鍵を保持していることを確認することで、ネットワークへの参加を許可したりする方法が考えられる。

表1　ネットワークへの参加登録方法と鍵確立方法

ネットワークへのノード参加登録方法		事前に設定が必要な認証情報	懸念される主なコスト	ネットワーク参加後の鍵確立方法
登録作業実施者によるアシスト利用	登録作業実施者が許可するか否か （例）WPS（Wi-Fi Protected Setup）ボタンプッシュ方式	・なし	・NW接続時の人手による登録アシスト	・鍵配送（平文） ・公開鍵暗号を利用した鍵交換／鍵配送（公開鍵自体の認証は実施しない） ・その他、事前共通秘密情報を利用しない鍵確立（電波強度分布利用など）
識別子利用	NW識別子を知っているか否か （例）ESSID	・接続先NWの識別子	・接続先NW識別子の事前設定作業	
	登録を許可されたノードであるか否か （例）MACアドレスフィルタリング	・登録リスト （ノード識別子リスト）	・登録リストの作成と管理 ・登録リストの事前設定作業	
秘密情報利用	既定の共通秘密情報を持っているか否か （例）WEP鍵、システム全体の共通秘密鍵	・既定の共通秘密情報	・共通秘密情報の管理 ・共通秘密情報の事前設定作業	・鍵共有（共通秘密情報利用） ・鍵配送（暗号化）
	ノード固有の秘密情報（共通鍵）を持っているか否か （例）SIM	・ノード識別子 ・ノード固有の共通鍵	・ノード固有鍵の共有手段 － 人手による事前設定作業 － 鍵管理サーバの運用	・鍵共有（共通鍵利用） ・鍵配送（暗号化）
	公開鍵証明書及び端末固有の秘密情報（自身の公開鍵のペアとなる秘密鍵）を持っているか否か （例）多機能ICカード	・公開鍵証明書 ・秘密鍵 ・証明書検証用公開鍵	・証明書管理（発行・更新・無効化）	・鍵交換 ・鍵配送（暗号化）

一方、鍵確立方法は、事前に共有された秘密情報を利用して鍵確立する方法と、事前に秘密情報を共有することなしに鍵確立する方法の2つに大別できる。前者では、共通の秘密情報を利用した鍵の暗号化配送や、新たに鍵を生成する鍵共有方式がある。後者では、公開鍵暗号を利用した鍵交換がある。また、暗号技術を利用せずに、送信出力を抑えて無線平文で鍵を送るなど、ある限定された環境下でのみ有効となる方法もある。

組み込みネットワークモデルと参加登録方法の考察

組み込みネットワークにおいて、どの参加登録方法が適しているかは、その組み込みネットワークの特徴や、要求されるセキュリティレベルおよび許容されるコストに依存する。本稿では、組み込みネットワークの特徴を以下のようにモデル化した。

- ネットワーク規模（大／小）：同一ネットワークに参加するノード数が多い（数百台以上の規模）、または、少ない（数台〜数十台の規模）。
- 接続先ネットワーク（不特定多数／特定）：不特定多数のネットワークに頻繁に出入りする、または、特定のネットワークのみに参加する。

組み込みネットワークモデルとそのアプリケーション例を**表2**に示す。また、分類した4つの組み込みネットワークモデルと、ネットワークへの参加登録方法との適性を考察した結果を**表3**（次ページ）に示す。**表3**に示されるように、各組み込みネットワークモデルにおいて、適用し得る参加登録方法は複数あり、参加登録時の認証の強度も許容しなければならないコストも参加登録方法ごとにそれぞれ異なる。実際のネットワークにおいて、どの参加登録方法を採用するかは、個々のサービスで要求されるセキュリティおよび許容されるコストによって選択されることになる。

表2　組み込みNWモデルとアプリケーション例

組み込みNWモデル		アプリケーション例
NW規模	接続先NW	
大	不特定多数	携帯電話
大	特定	省エネ制御、検針
小	不特定多数	携帯ゲーム機
小	特定	健康見守り、家庭内機器制御、車両内機器制御

認証情報の設定の考察

ノード登録機能を実現するには、ノードおよびノードを認証する装置に事前に認証情報を設定しておく必要がある。（ただし、登録作業実施者がアシストすることで参加登録する方法を除く。）組み込み機器の装置構成は、センサが無線通信機能を持っただけの低機能な装置から、ユーザーフレンドリーなGUIを有する携帯電話まで多様である。一般に組み込み機器は、認証情報を設定するための利用しやすいインタフェースを搭載しているとは限らない。このような組み込み機器への認証情報の設定は、課題となり得る。

認証情報の設定場所とその特徴を整理した結果を**表4**（次ページ）に示す。認証情報はノード製造時に自動的に設定できることが好ましい。一方で、たとえば、認証情報として鍵などの秘密情報を設定する場合には、製造業者における秘密情報の管理が負担となる可能性もある。また、接続先ネットワークの識別子やネットワーク個別の秘密情報など、ノードの参加登録に必要な認証情報が製造時には特定できない場合もある。このような場合には、サービス事業者や、セキュリティの専門知識のないユー

表3 組み込みNWモデルと参加登録方法との適性

認証情報	ノードを認証する装置	NW規模:大		NW規模:小	
		接続先NW:不特定多数	接続先NW:特定	接続先NW:不特定多数	接続先NW:特定
なし（登録作業実施者がアシスト）	NW内の他のノード	×〜△ ノードの参加登録ごとに人手によるアシストが要る。また、接続先NW変更の度に人手によるアシストが要る。	△ ノードの参加登録ごとに人手によるアシストが要る。	×〜△ 接続先NW変更の度に人手によるアシストが要る。	○
	NW管理装置	△ 接続先NW変更の度に人手によるアシストが要る。	○	△ 接続先NW変更の度に人手によるアシストが要る。	○
接続先NW識別子	NW内の他のノード	×〜△ NW識別子を不正利用された場合に影響が大きい。また、接続先NW変更の度にNW識別子の設定変更が要る。	△〜○ NW識別子を不正利用された場合に影響が大きい。	△ 接続先NW変更の度にNW識別子の設定変更が要る。	○
	NW管理装置				
登録リスト（ノード識別子）	NW内の他のノード	× ノードを認証する各ノードに登録リストを事前設定する必要がある。また、接続先NW変更の度に登録リストの設定変更が要る。	× ノードを認証する各ノードに登録リストを事前設定する必要がある。	× ノードを認証する各ノードに登録リストを事前設定する必要がある。また、接続先NW変更の度に登録リストの設定変更が要る。	△ ノードを認証する各ノードに登録リストを事前設定する必要がある。
	NW管理装置	× 接続先NW変更の度に登録リストの設定変更が要る。	○	×〜△ 接続先NW変更の度に登録リストの設定変更が要る。	○
	認証（鍵管理）サーバ	○	○	○	○
既定の共通秘密情報	NW内の他のノード	△〜○（システム共通の鍵） ×〜△（NW個別の鍵） 共通秘密情報を不正利用された場合に影響が大きい。また、接続先NW変更の度に共通秘密情報の設定変更が要る。	△〜○ 共通秘密情報を不正利用された場合に影響が大きい。	○（システム共通の鍵） △（NW個別の鍵） 接続先NW変更の度に共通秘密情報の設定変更が要る。	○
	NW管理装置				
ノード固有鍵	NW内の他のノード	× ノードを認証する各ノードと固有鍵を事前に共有させる必要がある。また、接続先NW変更の度に固有鍵を共有させる必要がある。	× ノードを認証する各ノードと固有鍵を事前に共有させる必要がある。	× ノードを認証する各ノードと固有鍵を事前に共有させる必要がある。また、接続先NW変更の度に固有鍵を共有させる必要がある。	△ ノードを認証する各ノードと固有鍵を事前に共有させる必要がある。
	NW管理装置	× 接続先NW変更の度に固有鍵を共有させる必要がある。	○	×〜△ 接続先NW変更の度に固有鍵を共有させる必要がある。	○
	認証（鍵管理）サーバ	○	○	○	○
公開鍵証明書	NW内の他のノード	○（システム共通の認証局） △（NW個別のローカル認証局） 接続先NW変更の度に証明書検証用の公開鍵（ローカル認証局の公開鍵）を把握する必要がある。	○	○（システム共通の認証局） △（NW個別のローカル認証局） 接続先NW変更の度に証明書検証用の公開鍵（ローカル認証局の公開鍵）を把握する必要がある。	○
	NW管理装置				

ザーを含む登録作業実施者が、手動で認証情報を設定する必要がある。サービス事業者や登録作業実施者による認証情報の設定作業をサポートするための手段として、作業を簡易化／効率化できるような設定用のツールを開発したり、無線通信を利用して複数のノードに認証情報を一括して設定してくれるような設定用のネットワークを構築したりすることも有効だと考える。

分散配送を利用した鍵共有方式の提案

テレビ、ハードディスクレコーダ、リモコンなど、家庭における情報機器の制御を用途とする組み込みネットワークは、規模が小さく、接続するネットワークも固定である。表3に示すように、このような組み込みネットワークにはさまざまなノードの参加登録方法を適用できる。ただし、認証情報の設定は課題となる。ノードの接続先ネットワークは、家庭内にあるため、ネットワーク接続時にしかわからない。すなわち、ネットワークへの登録作業は最終段階で誰かが実施する必要があり、その実施者は、セキュリティの専門知識がない家人である可能性

表4　認証情報の設定場所と特徴

認証情報の設定	特徴
製造業者がノード製造時に設定	【利点】 ・自動で設定できるため、出荷後の手動での設定作業をなくせる。 ・設定したノード識別子やノード固有鍵のリストを自動で作成できるため、出荷後の手動でのリスト作成作業をなくせる。
	【欠点】 ・秘密情報を設定する場合には、設定する秘密情報が不正に漏洩しないための管理、配送手段が必要になる。 ・NW識別子や既定の共通秘密情報を設定するためには、接続先NWを事前に知る必要がある。
サービス事業者が事前に設定	【利点】 ・登録作業実施者による手動での設定作業をなくせる。 ・サービス提供業者の管理下で、接続先NWやNWへの参加を許可する機器を事前に選択できる。
	【欠点】 ・手動での設定が必要になる。 ・現地にて接続先NWの変更や、NWへ参加させる機器に変更が生じた場合に、再設定が必要になる。
登録作業実施者がNW接続時に設定	【利点】 ・ノードをどのNWに接続するか、どのノードをNWに参加させるかを最終段階で決定できる。 ・既定の共通秘密情報やノード固有鍵をローカルNW内に閉じて管理できる。
	【欠点】 ・手動での設定が必要になる。 ・登録作業実施者に設定作業の負担がかかる。（専門知識がない場合に正しく設定できない可能性がある。） ・現地において、ノードを認証する装置に、識別子リストやノード固有鍵を設定する手段が必要になる。

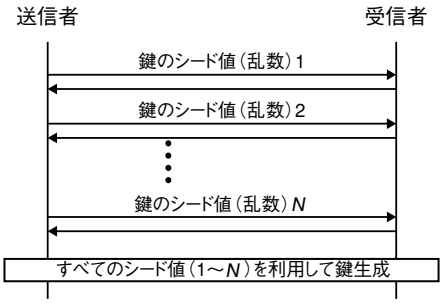

図2　分散配送を利用した鍵共有方式

が高い。また、通信データの暗号化や認証も必要である。ネットワーク外部からの家庭内機器の不正操作や、制御情報が盗聴されることによるプライバシ侵害が脅威となる。一方、これらの脅威は、金銭的な被害が膨大であったり、生命にかかわる危険を被ったりするものではないため、要求されるセキュリティレベルは高くないと考えることができる。

以上のような状況下では、事前に認証情報の設定が必要なく、家人でも簡単に（半自動的に）設定できるノードの参加登録方法および鍵確立方法が望まれる。要求されるセキュリティレベルは決して高くないため、コストの抑制が重視される。すなわち、ノードの処理能力やメモリ容量が小さくても動作する方法であることも重要である。登録作業実施者は、ボタン押下などの認証情報の事前設定が必要ない参加登録方法で、機器をネットワークに参加させ、その後、事前共有秘密情報を利用せずに鍵確立する。家庭内のような閉じた環境下で、事前共有秘密情報を利用せずに鍵確立する方式の一例として、我々が提案している分散配送を利用した鍵共有方式がある[2) 3)]。提案方式の概要を**図2**に示す。提案方式では、送信者と受信者との間で、鍵のシード値となる乱数情報を共有し、共有したすべての乱数情報から鍵を生成する。ここで、乱数情報を1ビットでも誤って受信した盗聴者は、正しい鍵を生成できない。家庭内機器の不正操作や制御情報の盗聴を企む攻撃者は、近傍には存在せず、隣家や屋外に存在すると考える。送信者は出力を抑えて情報を送信することで、近傍に存在する受信者とのみ、正しい乱数情報を共有する確率が高くなる。提案方式では、送信出力を抑えて乱数情報を配送するため、正当な受信者においても受信誤りが発生する可能性を考慮している。正当な受信者と盗聴者における鍵のシード値の受信ケースを**図3**に示す。受信者は誤り検出符号により受信誤りを検出し、正しく受信した場合にのみ受信応答を返す。このような配送規則にすることで、正当な受信者が乱数情報を誤って

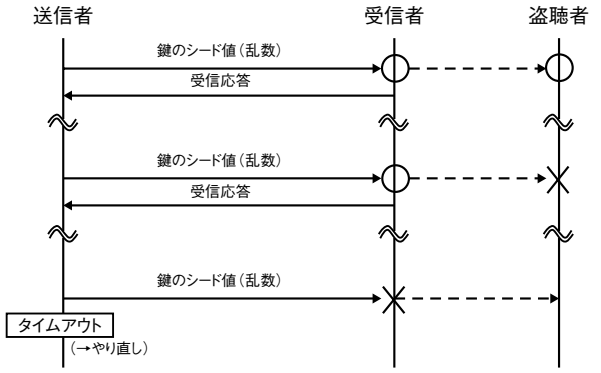

図3　鍵のシード値の受信ケース

受信した場合には、送信者が乱数情報の配送をやり直す一方で、盗聴者のみが乱数情報を誤って受信した場合には、乱数情報の再送を要求することが困難になる。

ま と め

本稿では、組み込み機器のネットワークへの参加登録方法と鍵確立方法について整理し、組み込みネットワークへの適性を考察した。さらに、事前に秘密情報を共有することなしに鍵確立する方法として、分散配送を利用した鍵共有方式を説明した。今後は、ネットワークへの参加登録だけでなく、運用や廃棄も含めた組み込みネットワークのライフサイクル全体を考慮した管理システムを提案する予定である。 ◆◆

■参考文献

1）服部，藤岡：改訂版ワイヤレスブロードバンド教科書ー高速IPワイヤレス編ー，インプレスR&D，2006年
2）山口：より安全なZigBee網を作る鍵配布と認証の技術，NETWORK WORLD，2008年2月号， IDGジャパン，pp.120–122
3）日本国特許庁 公開特許公報　特開2007-235516

●筆者紹介

八百健嗣：Taketsugu Yao. 研究開発センタ ユビキタスシステムラボラトリ
中嶋純：Jun Nakashima. 研究開発センタ ユビキタスシステムラボラトリ