IoTプラットフォームへのセキュア通信プロトコルの適用
Application of Secure Communications Protocol to IoT Platform

長野日本無線株式会社
中村　章　Akira Nakamura
土屋　裕　Yutaka Tsuchiya
大日方　和哉　Kazuya Obinata
松林　健一　Kenichi Matsubayashi
久保田　章裕　Akihiro Kubota

要　旨

インターネットを介してモノや機器の情報を収集するIoT（Internet of Things）システムにおいては情報セキュリティ対策が非常に重要である。産業用途においても利用が急増しているIoTシステムにおける強固なセキュリティ対策のニーズを受け，システム内の通信経路における伝送データの暗号化，デジタル証明書の受け渡しにより相互認証を行うプロトコル（EAP-TLS）を適用し，情報漏洩・データ改ざん・なりすましの脅威に対するセキュリティを高めたIoT無線端末（特定小電力無線端末）を開発した。IoT無線端末は，伝搬距離が長いSub-GHz帯（1 GHz以下の周波数帯）の電波を使用することにより広域のカバーが可能となり，公共インフラのようなネットワークにも適用できる安全なIoTシステムの基盤を確立した。

Abstract

Information security measures are very important in IoT (Internet of Things) systems that collect information about things and equipment via the Internet. In response to the need for strong security measures in IoT systems, which are rapidly utilized in industrial uses, encryption of transmitting data in the communication path in the system and protocol (EAP-TLS) that executes mutual authentication by exchanging digital certificates are applied, the IoT radio terminal (specified low power radio terminal) with enhanced security against threats of information leakage, data tampering, and spoofing has been developed. The IoT radio terminals can cover a wide area by using radio waves in the Sub-GHz band with a long propagation distance (1 GHz or less), the base of a secure IoT system that can be applied to networks such as public infrastructure has been established.

1. まえがき

公衆回線に接続しないスタンドアロンシステムや専用ネットワークで機器を監視制御するシステムに対し，モノや機器がインターネットに接続し互いに情報を交換して制御し合うIoT (Internet of Things) を利用したシステムが急速に広まってきている。インターネットやクラウドを利用するIoTでは，プラットフォーム構築において高いレベルの情報セキュリティ対策が不可欠である。IoTプラットフォームにおける情報セキュリティのポイントは，「通信経路の途中で盗み見されないか（情報漏洩を生じないか）」「通信経路の途中でデータが加工されないか（データが改ざんされていないか）」「正しい相手と接続できるか（「なりすまし」に遭わないか）」であり，これらはIoTプラットフォーム上の機器間の通信プロトコル（通信手順）において設定される。IoT無線端末（電子機器に装着され，IoTプラットフォーム上で通信を行う無線端末）には，一般的な無線端末に求められる「省電力性能」「通信エリアの広さ」「コスト」と併せて「高いレベルのセキュリティ機能」が要求される。

以上の背景を受け，当社はTLS（インターネットで安全な通信を行うHTTPSや企業向け無線LAN接続などで使用されているプロトコル）を用いて，IoTプラットフォームにおけるセキュリティ機能を向上させたので，以下に報告する。

2. IoT無線端末の概要

産業界におけるシステムは単独またはクローズドネットワークを介した運用がほとんどであり，セキュリティ対策は暗号化による情報漏洩リスクのみに対するケースが多かった。

近年，産業界においてもインターネット等のオープンネットワークへ接続するシステムが増えている。このため，図１に示すように，端末やシステムサーバを含むネットワーク全体で「情報漏洩」のみならず「データ改ざん」や「なりすまし」などのリスクも回避できる高いレベルのセキュリティを確保することが不可欠である。また，公共インフラのようなネットワークでは複数のベンダによるシステムや端末が相互に接続できることが必要である。これらの重要な社会的要求を満たすため，無線IoT端末には，標準規格に基づく通信プロトコルに準拠したハイレベルのセキュリティ機能を実装することが求められる。

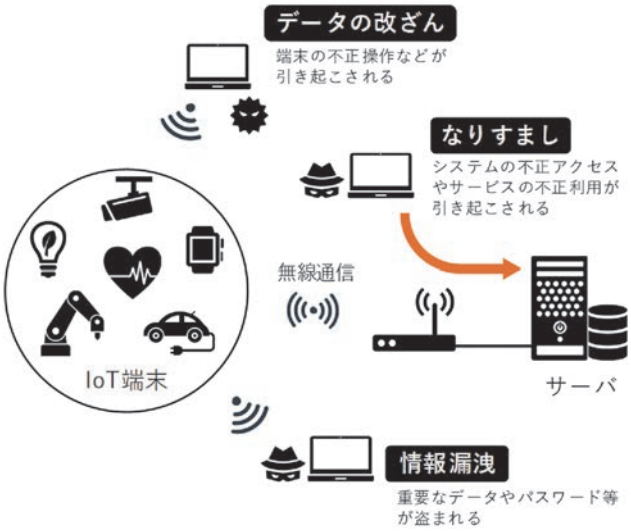

図1　セキュリティ脅威の概念
Fig.1　Concept of security threat

3. セキュリティを高めたIoT無線端末の開発

既述の社会的要求を受け，情報セキュリティのリスク（情報漏洩，データ改ざん，なりすまし）を回避する能力が高い通信プロトコルを適用したIoT無線端末を開発した。

開発のポイントは，通信プロトコルの「物理層」「MAC層」に国際標準規格であるIEEE 802.15.4g/eを，また「ネットワーク層」にIPv6/6LoWPANを適用し，通信経路の暗号化およびデジタル証明書によるサーバとの相互認証により，ハイレベルのセキュリティ対策を講じている点である。このようなセキュリティ対策を，通信相手の認証方式として国際標準を採用する無線通信規格である「Wi-SUN FAN」を実装することにより実現した。Wi-SUN FANは，異なるシステム間における相互運用を可能とするサービスとセキュリティで保護された無線ネットワークの実現を目指す団体である「Wi-SUNアライアンス」が制定する規格である。Wi-SUN FANについての詳細は後述する。

表1　長野日本無線製の標準規格対応無線モジュール
Table 1　Radio module made in Nagano Japan Radio Co., Ltd. complying with the standard

用途	ホームエネルギーマネージメントシステム（HEMS）	ホームエリアネットワーク（HAN）
型名	NHM-10246	NHM-10264
適合規格	ARIB STD-T108	
プロトコル	Wi-SUN Profile for Echonet Route B	Wi-SUN Profile for Echonet Single-Hop HAN
ネットワーク構成	1:1通信	1:N通信
セキュリティ	暗号化：AES-128 認証：PANA	
アンテナ	内蔵／外部	
周波数	922.5 ～ 927.7 MHz	
データ伝送速度	100 kbps	
送信出力	20 mW	
電源電圧	DC 2.7～3.6 V	
消費電流	送信時：45 mA，受信時：25 mA	
外形寸法	40 (W)×4.1 (H)×23 (D) mm	

本開発には，従来のWi-SUNアライアンス認定製品（表1）やガス検針用の標準規格（Uバスエア）に対応した製品の開発を通じて当社が得た経験と技術が活かされている。当社が従来開発した製品の活用領域は家庭内およびその周辺ネットワークに限定されていたが，本開発は，次世代スマートメータやインフラストラクチャ，高度道路情報システムなど，極めてハイレベルの情報セキュリティが要求される大規模なアプリケーションに適用するIoTプラットフォームである。

開発機は，複数種類の機器に対する利用の共通化を図るためモジュール構造としている。その外観を図2に，また仕様を表2に示す。

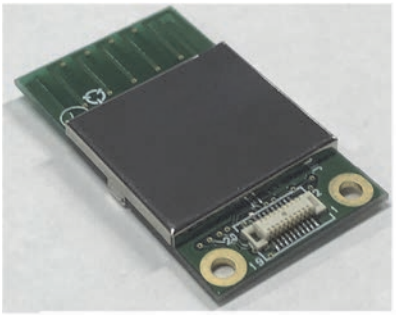

図2　開発したWi-SUN FAN対応無線モジュール（試作機）
Fig.2　Developed radio module for Wi-SUN FAN (prototype)

表2　開発した無線モジュールの仕様
Table 2　Specifications of the developed radio module

用途	フィールドエリアネットワーク（FAN）
型名	NHM-10283
適合規格	ARIB STD-T108
プロトコル	Wi-SUN FAN
ネットワーク構成	メッシュネットワーク
セキュリティ	暗号化：AES-128 認証：IEEE 802.1X/EAP-TLS
アンテナ	内蔵／外部
周波数	922.4 ～ 928 MHz
データ伝送速度	50 kbps / 150 kbps
送信出力	20 mW
電源電圧	DC 3.3 V
消費電流	送信時：45 mA，受信時：20 mA
外形寸法	35(W)×4.1(H)×20(D) mm

以下，本開発に適用した技術について述べる。

(1)　Wi-SUN FAN

Wi-SUN FANは，IEEE 802.15.4gの仕様に基づき，様々なシステムや組織を連携させた相互運用を可能とし，多種多様なサービスに適応する安全なIPv6無線メッシュネットワークを提供する技術であり，大規模ネットワークに適した国際標準無線通信規格である。

情報セキュリティのリスクである「データ改ざん」「なりすまし」からデータを保護する仕組みを支えるものが「認証」という技術である。Wi-SUN FANは，認証技術の標準規格として多数の実績がある「IEEE 802.1X/EAP-TLS」を採用する。Wi-SUN FANのデータ構造を表3に示す[1]。

表3　Wi-SUN FANのデータ構造
Table 3　Data structure of Wi-SUN FAN

<table>
<tr><td>アプリケーション層</td><td colspan="2" rowspan="3">アプリケーションソフトウェア</td></tr>
<tr><td>プレゼンテーション層</td></tr>
<tr><td>セッション層</td></tr>
<tr><td>トランスポート層</td><td rowspan="3">IEEE 802.1X
EAP-TLS
IEEE 802.11i</td><td>UDP/TCP</td></tr>
<tr><td>ネットワーク層</td><td>IPv6/ICMPv6/
RPL/6LoWPAN</td></tr>
<tr><td>データリンク層</td><td>IEEE 802.15.4e</td></tr>
<tr><td>物理層</td><td colspan="2">IEEE 802.15.4g</td></tr>
</table>

(2)　IEEE 802.1Xの認証システム

IEEE 802.1Xによる認証システムは，サプリカント（ネットワークに接続する無線端末），認証サーバ，およびこれら二者間の認証プロセスを相互に中継するオーセンティケータ（認証装置）で構成される。IEEE 802.1Xにおける認証プロトコルであるEAPには，表4に示す複数の方式があり，認証方式によりセキュリティの強度が異なる。本開発において採用したEAP方式は，この中で最もセキュリティの強度が高い「TLS」である。

表4 IEEE 802.1X 認証プロトコル比較
Table 4　IEEE 802.1X authentication protocol comparison

方式	サーバ認証	クライアント認証	セキュリティ強度
EAP-TLS	デジタル証明書	デジタル証明書	高
EAP-TTLS	デジタル証明書	ユーザ名，パスワード	中
PEAP	デジタル証明書	ユーザ名，パスワード	中
EAP-MD5	なし	チャレンジレスポンス	低

(3)　TLS

TLSは，通信相手を認証する際にIDやパスワードではなく「デジタル証明書」を使用する。デジタル証明書は「認証局（信頼された第三者機関）」が発行するもので，これを使用することにより「なりすまし」を防ぎ，セキュリティの強度を高めることができる。TLSは，「通信相手の認証」「通信内容の暗号化」「改ざんの検出機能」をもち，暗号化通信技術である「PKI」を採用する。PKIは，「公開鍵」と「秘密鍵」がペアとなる「公開鍵暗号方式」によって情報のやりとりを行うもので，セキュリティの強度が非常に高い。

4.　評価結果

Wi-SUN FANを実装したIoT無線モジュールのセキュリティ機能について，動作を評価した。評価システムの構成を図3に示す。評価試験は「正規のデジタル証明書を実装する無線端末」と「不正なデジタル証明書を実装する無線端末」を用意し，サーバにおいて認証されるか否かを検証したものである。この結果，「正規のデジタル証明書を実装する無線端末」は認証サーバにおいて認証され，端末から送出されるデータ（パケット）はデータサーバに到達したが，「不正なデジタル証明書を実装する無線端末」はネットワークへの接続が拒否され，認証サーバにおいて認証されず，端末から送出されるデータ（パケット）はデータサーバに到達しなかった。以上の評価により，IEEE 802.1X認証によるセキュリティ機能により，「データ改ざん」や「なりすまし」からデータが保護されることを確認した。

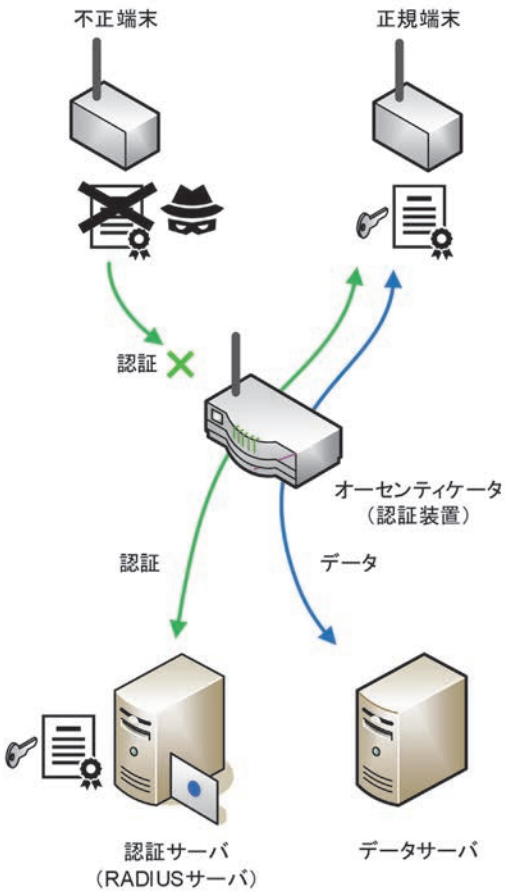

図3 評価システムの構成
Fig.3 Composition of the evaluation system

5. あとがき

公共の通信インフラに求められる要件として，「設置の容易性」「柔軟な拡張性」「高い信頼性」に加え「ハイレベルの情報セキュリティ」「高い相互接続性」があるが，これら全ての要件を満たし，情報セキュリティにおいて安全性が高いIoTプラットフォームを実現した。また伝搬距離が長いSub-GHz帯の電波を使用することにより，広域エリアをカバーする必要がある公共インフラのようなネットワークに適し，かつセキュリティの面で安全なシステムの提供が可能になる。

IoTプラットフォームの端末ではバッテリー駆動時間を延長するため，消費電力の更なる低減が求められる。

Wi-SUN FANの将来的な規格として超低消費電力化および無線通信速度の高速化の仕様が検討されており，これらの導入による機能改良を引き続き進めてゆく。

用 語 一 覧

EAP: Extensible Authentication Protocol
FAN: Field Area Network
HAN: Home Area Network
HEMS: Home Energy Management System
HTTPS: Hypertext Transfer Protocol Secure
IoT: Internet of Things
IPv6: Internet Protocol Version 6
PANA: Protocol for carrying Authentication for Network Access
PKI: Public Key Infrastructure
RADIUS: Remote Authentication Dial In User Service
SUN: Smart Utility Network
TLS: Transport Layer Security
IEEE std 802.1X-2020: Port-Based Network Access Control
（LAN接続時に使用する認証規格）
IEEE std 802.11i-2004: Wireless LAN Medium Access Control and Physical Layer specifications
（無線LAN接続時に使用するセキュリティ規格）
IETF RFC 3579：RADIUS Support For Extensible Authentication Protocol（拡張認証プロトコルのRADIUSサポート規格）
IETF RFC 5216：The EAP-TLS Authentication Protocol
（EAP-TLS認証プロトコル規格）

参考文献

(1) Phil. B, "Wi-SUNテクノロジーと認証", 総務省MRA国際ワークショップ2018