TTC技術レポート
Technical Report

TR-1051

ＨＥＭＳ下位層プロトコルに対応するセキュリティ機構

Overview of security structure in HEMS lower layer protocol

2014 年 3 月 25 日制定

一般社団法人
情報通信技術委員会

THE TELECOMMUNICATION TECHNOLOGY COMMITTEE

TTC Telecommunication Technology Committee

目　次

＜参考＞

１．　国際勧告等との関連

本技術レポートに関する国際勧告はない。

２．改版の履歴

版数	制定日	改版内容
第1.0版	2014年3月25日	制定

３．参照文章

主に、本文内に記載されたドキュメントを参照した。

４．技術レポート作成部門

第１．０ 版　：　次世代ホームネットワークシステム専門委員会　（SWG3601/3602）

５．本技術レポート「ＨＥＭＳ下位層プロトコルに対応するセキュリティ機構」の制作体制

本技術レポートは、TTC次世代ホームネットワークシステム専門委員会(委員長:山崎毅文[NTT]、前委員長：伊藤昌幸[NTT])の下、物理リンク層SWG(リーダー:鹿田實[NEC])にて技術調査を行い、新世代ネットワーク推進フォーラムIPネットワークWG　レジデンシャルICT SWG(リーダー: 丹康雄[JAIST/NICT])およびその下の基盤技術タスクフォース(主幹:近藤　芳展 [NTT])と協力してまとめたものである。

１．はじめに

本技術レポートは、2012年に発行された技術レポートTR-1043「ホームネットワーク通信インタフェース実装ガイドライン」を念頭に、各通信技術で利用可能なセキュリティ技術の概要をまとめたものである。

TR-1043では、主にHEMSで利用されるホームネットワークプロトコルとしてECHONET Liteを想定し、その伝送メディアとして利用可能な各種の通信技術について、規格の参照先を明らかにするとともに、実装の際に必要となるパラメータ等の規定を記述した実装ガイドラインとなっている。本技術レポートはこのTR-1043を補完するものとなっており、各伝送技術の実装において利用可能な低位レイヤセキュリティ技術について記述している。但し、TR-1043が各伝送技術における相互接続性を実現すべく、実装に必要とされる取り決めを記述しているのに対し、本技術レポートはとりうるセキュリティ技術を列挙したものであり、実装にあたってどのようにこれらの技術を利用すべきであるかを示したガイドラインではないことには注意を必要とする。

２．ＨＥＭＳ下位層プロトコルに対応するセキュリティ機構の全体概要

通信のセキュリティを確保するための機構としては、さまざまな提案があるが、基本的な機能としては、①通信する相手の認証（ユーザ認証）、②暗号化キー（鍵）の交換、③暗号化の実施と送受信、の３つの機能が必要である。それらの機能を、どの方式、どの通信レイヤで行うかの選択が各種考えられ提案されている。

まず、現在、暗号化の方式としては、AES（Advanced Encryption Standard）の鍵長１２８bitが一般に使われている。この鍵を交換するためのプロトコルがIKE（Internet Key Exchange）で、暗号化したデータを運ぶのが、IPsec（第３層で動作） やSSL（第４層と５層の間で動作）という構造になる。 また、ユーザ認証のためにEAP（Extensible Authentication Protocol ）というプロトコルがよくつかわれているが、これはサーバ／クライアントの双方が用意したデジタル証明書を交換して認証するもので、IDやパスワードを使うのに比べて安全性が高まる。このEAPを効率的かつ安全に交換するために、PANA（Protocol for Carrying Authentication for Network. Access）といったプロトコルも適用が始まっている。

これらをまとめると、以下のように位置づけされる。なお、各技術の通信レイヤとの関係付けに関しては、プロトコルの属するレイヤなのか、守っているレイヤなのかで意見が分かれるが、本表は判りやすさのために、両者の混在版となっている点、ご容赦願いたい。

表1　下位層セキュリティ技術の位置づけ

	ユーザ認証 (方式)	ユーザ認証 (伝達)	鍵交換	暗号化	暗号方式の総称
セッション層					↕ SSL/TLS
トランスポート層		↕ PANA			
ネットワーク層	↕ EAP		↕ IKE		↕ IPsec
データリンク層				↕ AES-128bit	
物理層					

３．各種下位層プロトコルにおけるセキュリティ機構

３．１　Ethernet

Ethernetに関し、セキュリティ機構の概要を以下の表２に示す。

表２　　Ethernetにおけるセキュリティ機構の概要

有線LAN		
トランスポート層	TCP/UDP	■暗号化：(D)TLS
ネットワーク層	IPv6 （/ IPv4）	■暗号化：IPsec ■鍵交換：IKEv1 / IKEv2
データリンク層	IEEE 802.3 (Ethernet)	■暗号化 IEEE 802.1AE（MACsec） - GCM-AES-128（デフォルト） ■鍵交換プロトコル IEEE 802.1X - EAP-TLS
物理層		

・IEEE 802.1AE (MACsec)は、イーサネットなどのレイヤ2プロトコルで流れている「フレーム」を暗号化するための技術である。「盗聴」、「改ざん」、「なりすまし」という、ネットワーク・セキュリティの脅威に対し、より低いレベルで防衛するために非常に有効な手段といわれている。GCM-AES-128がデフォルトで規定されているほか、256ビット長を使ったGCM-AES-256もオプションとして規定されている。

・GCMとはGalois/Counter Modeの略で、認証付き暗号の一つ。データ保護とユーザ認証の双方に利用できるのが特徴。並列処理が可能であり、パフォーマンスを高められる。GCMは、IEEE 802.1AE (MACsec) イーサネットセキュリティをはじめ、ファイバーチャネル、IPsec、TLSなどでも、標準規格に採用されている。

３．２　Wi-Fi

WiFi技術に関し、セキュリティ機構の概要を以下の表３に示す。

表３　　WiFiにおけるセキュリティ機構の概要

Wi-Fi（2.4GHz帯/5GHz帯）		
トランスポート層	TCP/UDP	■暗号化：SSL
ネットワーク層	IPv6 （/ IPv4）	■暗号化：IPsec ■鍵交換：IKEv1 / IKEv2
データリンク層	IEEE 802.11 a/ac/b/g/n	■暗号化 IEEE 802.11i（WPA2） - AES 128 / 192 / 256 ■認証規格 IEEE 802.1X - 認証プロトコル ※１
物理層		
備考	RCR STD-33、 ARIB STD-T66に準拠	

※１：認証プロトコル：EAP-TLS、EAP-TTLS/MSCHAPv2、PEAPv0/EAP-MSCHAPv2、
PEAPv1/EAP-GTC、EAP-SIM、EAP-AKA、EAP-FAST

・WPA（Wi-Fi Protected Access） は Wi-Fi Allianceが策定したセキュリティプロトコルである。WPA2はWPAを改良してより強力なAES暗号を標準としている。WPA2認定は、そのセキュリティプロトコルへの準拠を示す。
このプロトコルには Enterprise と Personal の2種類がある。Enterprise は、ユーザ認証に802.1XのEAP(Extensible Authentication Protocol)を用い、認証ごとに端末とアクセスポイントに暗号化鍵を配布する方式。Personal は「事前共有鍵」を使い、アクセスする端末には全て同じパスフレーズを入力する方式。なお、IEEE 802.1X は、ネットワーク機器のポート単位でユーザのアクセス権を認証する手順を規定した標準規格。

・EAP(Extensible Authentication Protocol)の規格には様々なものが存在しており、Wi-Fi Alliance のWPA2認定プログラムには、次の規格が規定されている。

EAP-TLS／EAP-TTLS/MSCHAPv2／PEAPv0/EAP-MSCHAPv2／PEAPv1/EAP-GTC／
EAP-SIM／EAP-AKA／EAP-FAST

３．３　Bluetooth

Bluetoothに関し、セキュリティ機構の概要を以下の表４に示す。

表４　　Bluetoothにおけるセキュリティ機構の概要

Bluetooth	Bluetooth 2.0 + EDR PAN profile
トランスポート層	TCP/UDP
ネットワーク層	IPv6 （/ IPv4）
データリンク層	BNEP L2CAP セキュリティ機能 1. 接続認証（誤接続防止） ペアリング 2. 暗号化（盗聴防止）
物理層	Baseband 2.4GHz ISM Band
備考	

※PAN profile : Personal Area Network プロファイル

※BNEP:Bluetooth Network Encapsulation Protocol : 上位ネットワーク層をカプセル化するプロトコル

Bluetoothのセキュリティに関しては、その安全性を疑問視する意見もあるが、以下のような対応が考えられている。

① 鍵管理

高位レイヤのソフトウェアにおいて複数の異なる鍵を使用することが可能。

② デバイス認証

Bluetoothデバイスのアドホックネットワーク間に信頼ドメインを構成（ペアリング）する方法。その認証はPIN（ASCII最大16文字の認証番号）を使用して、2つのデバイス間接続のセキュリティを保証するチャレンジ/レスポンス方式を採用。デバイスの認証に失敗した場合、新たな認証処理は一定時間が経過した後でなければ実行できない。

③ 暗号化

認証が成功するとリンクキーが生成される。リンクキーと128ビット長の暗号キー（乱数）を使用して暗号化通信が行われる。　Bluetoothパケットのデータ・ペイロードは暗号化されるが、Bluetoothのアクセスコードとパケット・ヘッダは暗号化されない。

④ 物理層でのデータ・セキュリティ

Bluetoothの通信に採用されている周波数ホッピング方式（周波数ホッピング・スペクトル拡散方式）は、盗聴を困難にするメカニズムとして働く。北米や欧州では、2.402～2.480GHzまでの周波数帯域を、1MHz幅の79のサブチャンネルに分けて使用している。　また周波数ホッピング方式では、１600回/秒のホッピング・シーケンスをおこなっている。

３．４　JJ-300.10方式A

JJ-300.10方式Aに関し、セキュリティ機構の概要を以下の表５に示す。

表５　　JJ-300.10方式Aにおけるセキュリティ機構の概要

920MHz帯 特小無線	Wi-SUN
トランスポート層	TCP/UDP　■認証：PANA
ネットワーク層	IPv6
データリンク層	6LoWPAN IEEE 802.15.4 + 802.15.4e　■暗号化 AES-128
物理層	IEEE 802.15.4g
備考	ARIB STD-T 108に準拠

・920MHz帯の低電力無線をPAN(personal area network)として利用するための規格がIEEE 802.15.4であるが、伝送速度こそ40～250Kbpsと無線LANやBluetoothよりも遅いものの、1つのネットワークに多くのデバイスが参加できたり、煩雑な設定なしで機器の接続、切断が行えるアドホックネットワークとしての高いメリットがある。

・ただし、ここにIPv6を通すのは容易なことではない。IPv6の最小MTUが1280バイトであるのに対し、IEEE 802.15.4のL2ペイロードは81バイト。フラグメンテーションやヘッダ圧縮が必須である。したがって、IPv6のデバイスがそのまま通常のIPv6ネットワークにつながるわけではなく、中間的なレイヤとして6LoWPANが定義された。

・無線系は盗聴などセキュリティ上の課題を克服するために、いろいろな方式が適用されている。デジタル証明もその一つだが、多様なデータリンク層の下で、認証メッセージを運ぶに適したPANAが導入されている点にも特徴がある。

３．５　JJ-300.10方式B

JJ-300.10方式Bに関し、セキュリティ機構の概要を以下の表６に示す。

表６　　JJ-300.10方式Bにおけるセキュリティ機構の概要

920MHz帯 特小無線	ZigBee IP
トランスポート層	TCP/UDP　■認証： PANA ■暗号化：(D)TLS, TLS-PSK
ネットワーク層	IPv6 + RPL
データリンク層	6LoWPAN IEEE 802.15.4　■認証： EAP ■暗号化：AES-128
物理層	IEEE 802.15.4g
備考	ARIB STD-T 108に準拠

JJ-300.10Bのセキュリティは次の通りである。

①　鍵管理

デバイスごとに異なる認証鍵を設定することができる。

暗号鍵は、PAN（ZigBeeIPマルチホップネットワーク）に共通の鍵を利用し、PAA(ZigBeeIPコーディネータ)からの配送により設定・更新される。PAAから鍵が送付されるためには②におけるネットワーク参加認証によって認証される必要がある。

②　ネットワーク参加認証

ZigBeeIPマルチホップネットワークへの参加認証を実施する。認証方式として、EAP-TLSを利用し、事前共有鍵を利用する方式(TLS-PSK)とデジタル証明書を利用する方式(TLS-ECC)の２つを用意する。マルチホップネットワーク上で認証メッセージを中継配送するためにPANA Relay機能が導入される。

③　暗号化

128ビット長のAES暗号を利用し、メッセージの暗号化と認証を実施する。暗号化に使われる鍵は①における暗号鍵を元に生成される。

３．６　JJ-300.10方式C

JJ-300.10方式Cに関し、セキュリティ機構の概要を以下の表６に示す。

表７　　JJ-300.10方式Cにおけるセキュリティ機構の概要

920MHz帯 特小無線	Wi-SUN
データリンク層	IEEE 802.15.4 + 802.15.4e　■暗号化 AES-128
物理層	IEEE 802.15.4g
備考	ARIB STD-T 108に準拠

・通常のIPネットワークと同じ考え方、同じ方法論をもって方式の拡張性を確保しようとしたのが6LowPAN制定の考えであるが、逆に、IPにとらわれずに低消費電力PANに最適なものを選択しようとするのが300.10Cを制定した目的。　したがって、この方式では第3層以上のセキュリティは個別方式となっている。

３．７　高速PLC

高速PLCに関し、セキュリティ機構の概要を以下の表７に示す。

表８　　高速PLCにおけるセキュリティ機構の概要

高速PLC	ITU-T G.hn	IEEE 1901 (HD-PLC)	HD-PLC inside (JJ-300..21)	IEEE 1901 (HomePlug)	HomePlug GP
トランスポート層	TCP/UDP	TCP/UDP	TCP/UDP	TCP/UDP	TCP/UDP
ネットワーク層	IPv6 (/ IPv4)	IPv6 (/ IPv4)	IPv6 (/ IPv4)	IPv6 (/ IPv4)	IPv6 (/ IPv4)
データリンク層	G.9961 （Ether向けAPC規定含む） 暗号化（盗聴防止） AES-128bit	IEEE 1901 -Wavelet OFDM （MAC規定のみ） 暗号化（盗聴防止） AES-128bit	IEEE 1901 - Wavelet OFDM （機能限定 *1） 暗号化（盗聴防止） AES-128bit	IEEE 1901 -FFT OFDM （MAC規定のみ） 暗号化（盗聴防止） AES-128bit	-
物理層	G.9960 G.9964	IEEE 1901 - Wavelet OFDM	IEEE 1901 - Wavelet OFDM （機能限定 *1）	IEEE 1901 - FFT OFDM	-
備考	ITU（G.9972）及びIEEE（ISP機能）により、これら4つの標準方式の間には共存機能あり（但し、HD-PLC間以外では相互接続機能なし）。				HomePlugアライアンスによる独自仕様
	電波法施行規則　第44条、第46条、第46条の2、第46条の3 「広帯域電力線搬送通信設備」に準拠。				

※APC: Application Protocol Convergenceレイヤ
注)　＊1　IEEE1901仕様の一部機能に限定される

・高速PLC(ITU-T/G.hn、IEEE1901/HD-PLC、HD-PLCinseide、IEEE1901/HomePlug)においては、
データリンク層のMAC規定をそのまま、あるいはカプセル化（APC）して適用している。
基本的には家やオフィスに閉じた有線の小ネットワークなので、利用効率は悪くなるが必要とあれば
3.1 Eternetの項に示された上位レイヤのセキュリティ技術を重ねて適用することもできる。

３．８　低速PLC

低速PLCに関し、セキュリティ機構の概要を以下の表８に示す。

表９　　低速PLCにおけるセキュリティ機構の概要

低速PLC	G3-PLC	PRIME	ITU-T G.hnem	IEEE 1901.2
トランスポート層	TCP/UDP	TCP/UDP	TCP/UDP	TCP/UDP
ネットワーク層	IPv6	IPv6（/IPv4）	IPv6（/IPv4）	IP
データリンク層	G.9903 - APCとして、6LoWPAN及びMesh Routing (LOADng)を規定 - 802.15.4準拠	G.9904 -APCとして、IPv4/IPv6向け規定含む - IPv6向けAPCは、ITU-Tにおいて検討中	G.9902 -IPv6 APC規定を含む（6LoWPAN含む複数のヘッダ圧縮方式、及びRFC4861 (Neighbor Discovery)を規定）	低速PLC共通 暗号化（盗聴防止） AES-128bit
物理層	G.9903 -CENELEC Aバンド -CENELEC Bバンド -FCC拡張バンド -ARIBバンド	G.9904 - CENELEC Aバンド	G.9902 -本文に規定 -CENELEC Bバンド -CENELEC CDバンド -FCC拡張バンド -ARIBバンド	
備考	G.9903の上位層としてJJ-300.11を規定			標準化作業中。 G3-PLC或いはPRIMEと相互接続可能モードあり
	- IEEE 1901.2、G.hnem、G3-PLC、PRIME間での共存を可能とする仕様を検討中 - ARIB STD-T84に準拠すること			

※HEMSおよびスマートメータへの利用については、屋外利用が制限されていない点が低速PLCのメリットである

•データリンク層の規定が、いずれも高速系の規定からAPCとしてカプセル化して適用することを想定している。したがって、AES-128がMAC層で適用可能。高速PLCの場合と同様に、利用効率は悪くなるが必要とあれば 3.1 Ethernet の項に示された上位レイヤのセキュリティ技術を重ねて適用することもできる。

４．まとめ

HEMS下位層プロトコルのセキュリティ機構に関して概観した。 HEMSやスマートメータの使用においては、家庭内の生活用機器が外部のネットワークと接続されるのであるが、セキュリティに関する知識を持ちえない一般の人が相手である以上、悪意を持った外部の人が故意に機器にアクセスして操作できるようなことは決してあってはならない。セキュリティに関しては、攻める側と守る側のイタチごっことよく言われるが、より安全性が高く、しかも扱い易いセキュリティ機構への発展がますます期待される。

今後とも、技術の動向を見定めるとともに、実装レベルの課題等の発生に注意してゆく必要がある。

付録　セキュリティ機構に関する共通技術の簡単な説明

・暗号化

暗号化に関わる基本的な用語の定義を以下のとおりとする。 送信側の元の文章を「平文」、暗号文に変換することを「暗号化」、 受信側で暗号文を元の平文に戻すことを「復号化」と言う。 暗号化や復号化の手順を「アルゴリズム」、暗号化に用いるパラメータのことを「鍵（キー）」と呼ぶ。

・鍵（キー）

鍵の使い方には、共通鍵暗号と公開鍵暗号という２つの方式がある。送信側と受信側が同じ鍵を使う方式を「共通鍵暗号方式」と呼ぶ。対象ごとに鍵が異なるので、管理が煩雑だが、暗号化操作を高速化できる。一方、暗号化に使用する鍵と復号に使用する鍵とがそれぞれ違う鍵を使う方式で、片方の鍵を相手に公開する方式を「公開鍵暗号」と呼ぶ。通常、暗号化する鍵が公開されている。公開しない方の鍵を自分の秘密鍵として管理すればよいので、鍵の管理が楽である。ただし、アルゴリズムが複雑なので、高速化が難しくなる。

・AES　（Advanced Encryption Standard）

米国商務省標準技術局(NIST)によって制定された新世代標準暗号化方式。かつて標準暗号として用いられていたDES（Data Encryption Standard）が制定されたのは1977年であり、その後のコンピュータの高性能化、暗号理論の発展に伴い、鍵長が５６ビットのDESでは、その信頼性が年々低下していた。そこで、NISTはDESに代わる次世代の暗号標準として、AES候補となる暗号方式を全世界から公募した。世界中から集まった15の方式が審査を受けていたが、2000年10月に、ベルギーの暗号開発者Joan Daemen氏とVincent Rijmen氏が開発した「Rijndael」という方式が選ばれた。

ブロック長は128ビットで、鍵長は128、192、256ビットのいずれかを選ぶことができる。 現在AES-１２８ビットが多く用いられている。

・SSL （Secure Sockets Layer）、TLS（Transport Layer Security）

インターネット上で情報を暗号化して送受信するプロトコルのこと。Netscape Communications社が開発。インターネットで広く使われているWWWやFTPなどのデータを暗号化し、プライバシーに関わる情報やクレジットカード番号、企業秘密などを安全に送受信することを目指したもの。

SSLは公開鍵暗号や秘密鍵暗号、デジタル証明書、ハッシュ関数などのセキュリティ技術を組み合わせ、データの盗聴や改ざん、なりすましを防ぐことができる。OSI参照モデルではセッション層(第5層)とトランスポート層(第4層)の境界で動作し、HTTPやFTPなどの上位のプロトコルを利用するアプリケーションソフトからは、特に意識することなく透過的に利用することができる。

なお、SSL 3.0をもとに若干の改良が加えられたTLS1.0がRFC2246としてIETFで標準化されている。SSL-TLSとか、EAP-TLSとかの言い方、使われ方をしている。

・IPsec

インターネットで暗号通信を行うための規格。IETF(Internet Engineering Task Force)において標準化された。OSI参照モデルではネットワーク層（第３層）となるIPのパケットを暗号化して送受信するもので、TCPやUDPなど上位のプロトコルを利用するアプリケーションソフトはIPsecが使われていることを意識する必要はない。IPsecは、認

証や暗号のプロトコル、鍵交換プロトコル、ヘッダ構造など、複数の機能を総称するもの。 IPv4ではオプションとして使用ができる。IPv6では標準で実装されている。

・IKEv1 / IKEv2　（Internet Key Exchange verion1,2）

IPsecにおける鍵交換のためのプロトコル。通信相手との間でSA(Security Association)と呼ばれるセキュアな通信路を作るために、IKEの通信相手の本人性の確認、認証・暗号化用の秘密鍵の交換を行うもの。同じくIETFにおいて標準化された。

・EAP-TLS　（Extensible Authentication Protocol Transport Layer Security）

認証にTLS(Transport Layer Security)を利用する方式。TLSの暗号スイート (認証・鍵交換・暗号化・MAC等 のアルゴリズムの一式) に応じて、公開鍵暗号や共通鍵暗号、デジタル証明書、ハッシュ関数などを認証方式として利用することができる。 IEEE802.11bなどの無線LANにおいては、サーバ／クライアントの双方が用意したデジタル証明書を交換して相互に認証することでセキュリティを強化している。」

・PANA　（Protocol for Carrying Authentication for Network. Access）

トランスポート層（第４層）のUDP/IP上で、EAP-TLS認証メッセージを運ぶためのクライアント／サーバ型のプロトコル。　IETFにおいて標準化されている。データリンク層やネットワーク層の多様な方式に対応できることがポイント。