IoT を実現する Bluetooth® low energy 技術とは何か

概要

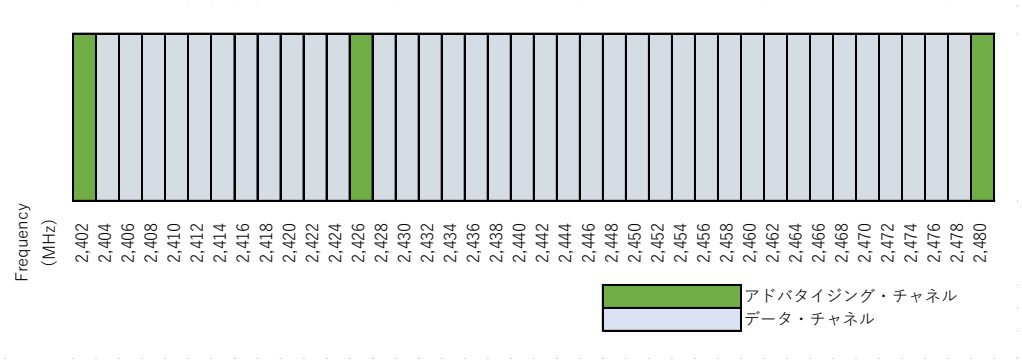
ルネサス エレクトロニクスは、低消費電力で無線通信を実現できる Bluetooth low energy マイコンをラインアップしています。コンピュータやマイコン機器といったネットワーク接続を前提にした情報通信機器だけでなく、世の中に存在するあらゆるモノがインターネットにつながり情報をやりとりする世界を目指す IoT の時代に、Bluetooth low energy は無線接続の手段として利用されています。そこで、Bluetooth low energy 技術を解説します。

はじめに

Bluetooth low energy は、WPAN(Wireless personal area networks)という近距離無線ネットワークに利用されています。近距離無線ネットワークは、数 10m の通信距離で、他の無線規格と比べて低消費電力であることが特長です。近距離無線ネットワークは、zigbee や Bluetooth を代表にする標準化無線ネットワークと、独自の通信プロトコルを利用する非標準化無線ネットワークがあります。標準化無線ネットワークの 1 つが Bluetooth low energy です。Bluetooth low energy は多くのスマートフォンに採用されています。そのため、数ある無線規格のなかで Bluetooth low energy が利用されています。

Bluetooth low energy 通信技術について解説します。従来からある音声通信に使われている Bluetooth とは Bluetooth の名前を使用しているが規格は別物です。Bluetooth low energy は、2.400 GHz から 2.480 GHz までの 80 MHz の帯域を、2MHz 幅で分割して、40 のチャネルにして利用しています。40 のチャネルは、2 種類にわかれています。

- アドバタイジング・チャネル：3 チャネル
- データ・チャネル：37 チャネル

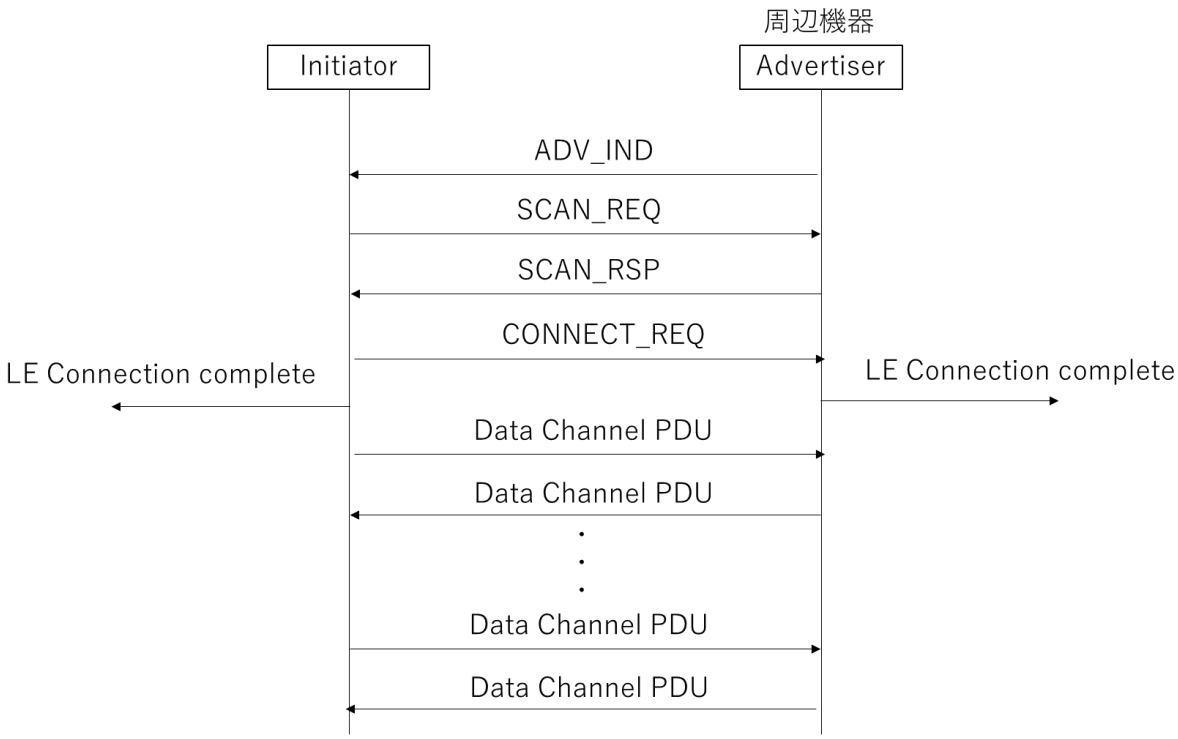


Bluetooth low energy 通信の周波数チャネル

それぞれのチャネルの使い方を説明します。

周辺機器は、アドバタイジング・チャネルでアドバタイズメント・パケットを送信します。アドバタイズメント・パケットは、自分の存在を周囲に伝えるために、アドバタイズ・インターバル毎に、3 チャネルにそれぞれブロードキャスト（送信）します。そして、デバイスの発見と接続に使います。なお、アドバタイジング・インターバル時間は、20m 秒から 10.24 秒と Bluetooth 規格で規定されています。インターバル時間は、接続の容易さ、消費電力に影響します。

データ・チャネルは、接続完了後のデバイス同士の通信で使用します。データ・チャネルは、適応型周波数ホッピング方式(AFH)と呼ばれる通信をします。チャンネルをコネクション・インターバル時間で次々にチャネルを切り替えて使用します。また適応型と言われるのは、混雑している周波数を使用しないように変更して利用できることができます。また、タイムアウト時間を持ち、例えば混信で通信できない場合でも、タイムアウト時間はホッピングをして通信をし続けます。そのため、一部のチャンネルで混信をうけても通信を断絶しない仕組みになっています。なお、コネクション・インターバル時間は 7.5m 秒から 4 秒と Bluetooth 規格で規定されています。インターバル時間は、スループット、消費電力に影響します。



Bluetooth low energy の動作フロー例

次に、Bluetooth のセキュリティについて説明します。

Bluetooth のデータ通信を暗号化ができます。暗号化通信のために、はじめに固有情報の交換（ペアリング）をします。そのペアリングにはボンディングという言葉を使用します。ボンディングは、セキュリティおよび固有の情報を交換し、格納をします。秘密鍵のためのキーのやり取りをペアリング。ペアリング後、デバイスとのペア情報を保持した状態をボンディングという言葉を使用されます。

Bluetooth low energy のセキュリティ要件は、「セキュリティモード」および「セキュリティレベル」という言葉で表現されます。各セキュリティ要件を満たすためには、ペアリングが必要になります。ペアリングには MITM(中間者攻撃)から保護される Authenticated ペアリングと、MITM(中間者攻撃）から保護されない Unauthenticated ペアリングがあります。

ペアリング方法について説明します。ペアリング方法は、下記の 4 つの方法があります。

- Just Works：デバイス選択のみで、他に確認がないペアリング方法です。これは認証されていなく MITM(中間者攻撃)に保護がない LE Security Mode 1 Level 2 になります。

- Passkey Entry：6 桁の認証コードを入れるペアリング方法です。これは認証され MITM(中間者攻撃)に保護する LE Security Mode 1 Level 3 になります。
- Out of Band (OOB)：Bluetooth 以外の通信（有線 や NFC など）で行うペアリング方法です。これも認証され MITM(中間者攻撃)に保護する LE Security Mode 1 Level 3 になります。
- Numeric Comparison：6 桁の認証コードを表示しての一致確認をするペアリング方法です。これは Bluetooth 4.2 に追加された LE Secure Connections のみで使用できます。

セキュリティモード	セキュリティレベル	概要	備考
LE Security Mode 1	1	セキュリティ無し(認証なし、暗号化なし)	
	2	Unauthenticated ペアリングによる暗号化	Just Works でペアリング
	3	Authenticated ペアリングによる暗号化	Passkey, OOB でペアリング
	4	Authenticated LE Secure Connections ペアリングによる暗号化	RL78/G1D は未サポート
LE Security Mode 2	1	Unauthenticated ペアリングによるデータ署名	
	2	Authenticated ペアリングによるデータ署名	

LE セキュリティモードとセキュリティレベル

LE セキュリティモード 1 のレベル 3 は、LE セキュリティモード 2 のセキュリティ要件を満たします。

LE セキュリティモード 2 のデータ署名(Data Signing)は、高速の接続・切断・転送を目的にするもので、通常は暗号化無しの状態で使う目的のものになります。データ署名を行うために、暗号化・認証とは別に CSRK (Connection Signature Resolving Key) 鍵を使用します。

デバイスの構成により、ペアリング方法の鍵生成方法がきまります。MITM(中間者攻撃)に保護して使用するには、デバイス構成に OOB(Out of Band)での鍵交換方式を持ってい

る場合では、OOB(Out of Band)を使用できます。

その他に、6 桁の数値を入れる Passkey Entry の使用方法があります。**Passkey entry の場合は、6 桁の数値を使用する。その結果、MITM(中間者攻撃)の成功確率は、1/1,000,000 の確率になります。MITM(中間者攻撃)からの危険度は非常に小さいものとなります。また、Bluetooth low energy の通信距離は短いため、近くにいないと盗聴できません。そのため、ペアリング中の盗聴の可能性は低く、屋内では盗聴から保護はされると考えています。それ以降の接続は、暗号化によりセキュリティが確保されますので、安心して使えます。**

さらに、MITM(中間者攻撃)から守る方法の提案、ペアリングモードに入っていないとペアリングをしない様に実装して、隔離されているところでペアリングすることで、MITM(中間者攻撃)から避けることが可能です。モード設定は、物理的な設定や、通信上の設定が考えられます。

RL78/G1D は、Bluetooth 4.2 のオプションで追加された LE Secure connections には、サポートしていません。これは、Numeric Comparison でのペアリングのみで使用可能で、機器に表示機能がないと実装できません。製品によっては、実装面積などによる表示機能が実装できないアプリケーションは、実装検討前から使用できません。

デバイス構成により、実装できるペアリング方法が決まり、デバイス構成(IO Capability)のマッピングのようにまとめられます。

	発信デバイス				
応答デバイス	Display Only	Display Yes No	Keyboard Only	No Input No Output	Keyboard Display
Display Only	Just Works	Just Works	Passkey Entry	Just Works	Passkey Entry
Display Yes No	Just Works	Just Works	Passkey Entry	Just Works	Passkey Entry:
		Numeric Comparison (For LE Secure connections)			Numeric Comparison (For LE Secure Connections)
Keyboard Only	Passkey Entry	Passkey Entry	Passkey Entry	Just Works	Passkey Entry
No Input No Output	Just Works	Just Works	Just Works	Just Works	Just Works
Keyboard Display	Passkey Entry	Passkey Entry	Passkey Entry	Just Works	Passkey Entry
		Numeric Comparison (For LE Secure connections)			Numeric Comparison (For LE Secure connections)

デバイス構成(IO Capability)のマッピング

暗号に使用する鍵交換方法について説明します。鍵交換については下記フェーズで行われます。

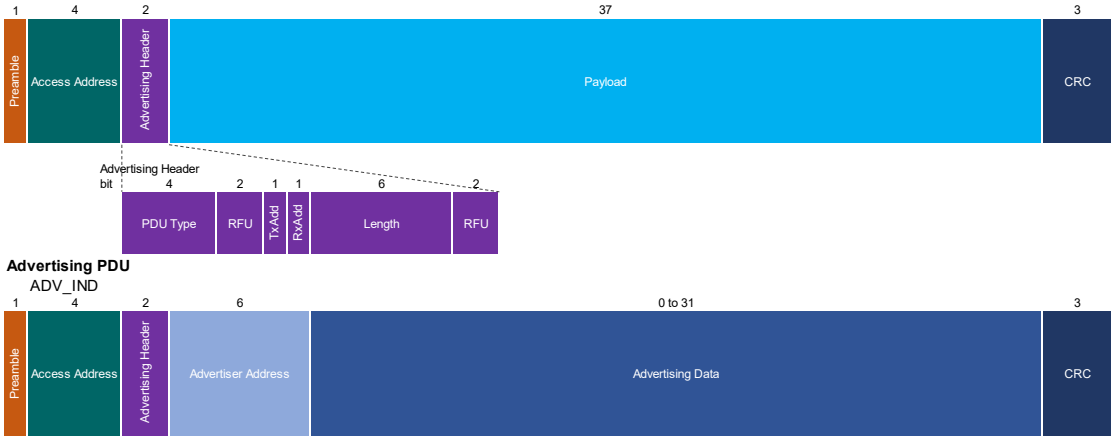
フェーズ 1：ペアリング・フィーチャーの交換（デバイス構成(IO Capability)、認証要件等）
フェーズ 2：STK の生成。STK 生成方法はフェーズ 1 にて交換した情報に基づきます。
フェーズ 3：生成されたキーの配布。フェーズ 2 で生成したキーを使用し暗号化されたリンクで行われます。

ペアリング、暗号化、プライベートアドレス解決およびデータ署名などで扱われる鍵は下記になります。この鍵は、各フェーズによって使用されます。

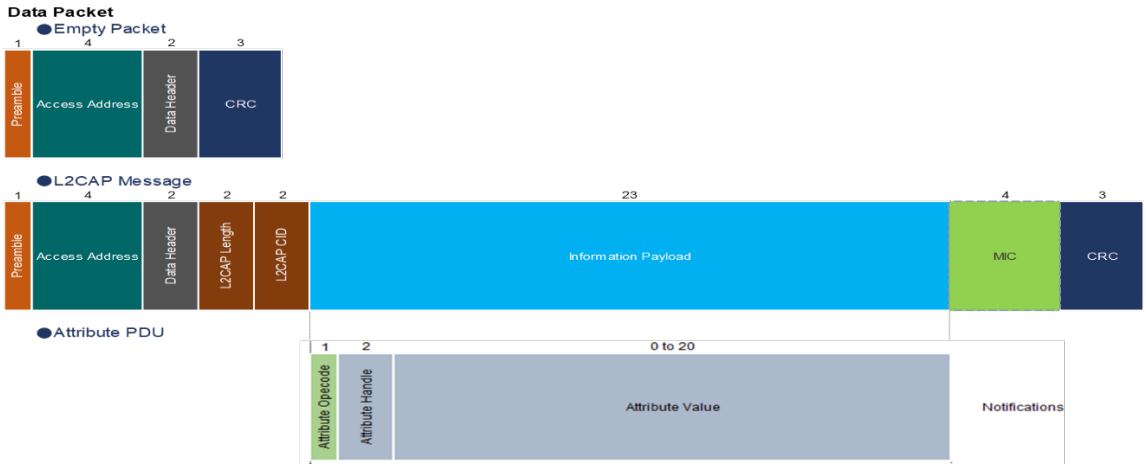
鍵タイプ	概要	生成
TK (Temporary Key)	128bit STK 生成のためにペアリングフェーズ 2 で使用される	アプリケーションで生成する
STK (Short Term Key)	128bit TK を使用しペアリングフェーズ 2 にて生成される。フェーズ 2 後のリンクの暗号化に使用される	BLE ソフトウェアで生成する
LTK (Long Term Key)	128bit（同意されたキーサイズに応じて部分的に使用） 暗号化のためのセッションキーを生成する為に使用される	アプリケーションで生成する
EDIV (Encrypted Diversifier)	16bit LTK を識別するために使用される。LTK が配布されるたびに EDIV は生成される	アプリケーションで生成する
Rand (Random Number)	64bit LTK を識別するために使用される。LTK が配布されるたびに Rand は生成される	アプリケーションで生成する
IRK (Identity Resolving Key)	128bit ランダムアドレスの生成・解決に使用される	アプリケーションで生成する
CSRK (Connection Signature Resolving Key)	128bit 署名の作成および、受信データの署名の確認に使用される	アプリケーションで生成する

Bluetooth low energy の鍵タイプ

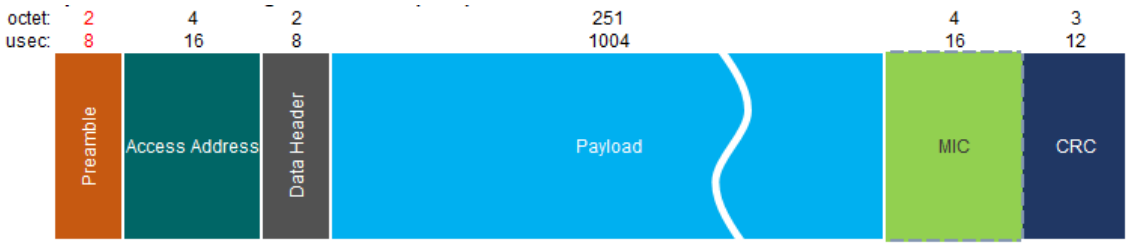
次に通信パケットについて紹介します。Bluetooth 4.0(Low Energy)規格で制定されたアドバタイジング・パケットは下記の構成となります。31 バイトをアドバタイジング・データとして使用できます。Bluetooth の新しい使い方であるビーコン機器は、このパケットを一定間隔でブロードキャスト（送信）として、それを受信してアプリケーションを実現しています。ビーコン機器の応用例については、後ほど紹介します。



データ・チャネルを利用してデバイス同士の通信に使用するパケットは、下記の構成で 20 バイトをデータ通信に利用できます。20 バイトに収まらない場合は、20 バイト単位にデータを分割して使用します。

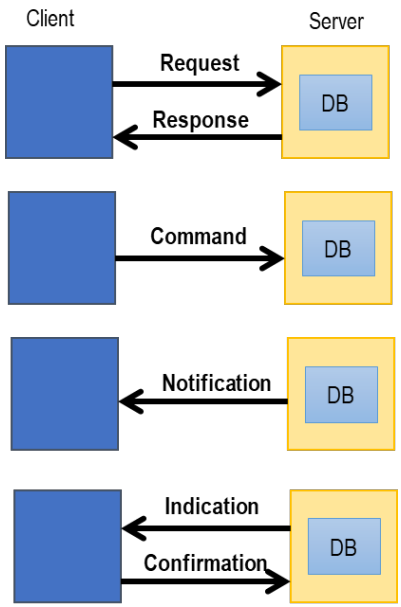


Bluetooth 4.2 で LE Data extension が追加され、下記のように通信パケットが拡張されました。この LE Data extension は、オプション仕様で、RL78/G1D ではサポートしていません。



ここでは、通信パケットのやり取りについて紹介します。通信確認の応答のある通信と、通信確認の応答のない通信があります。通信処理の組み合わせは下記になります。

Bluetooth low energy の応答がある通信は、次のインターバル動作での応答（Response/Confirmation）をするようになります。すなわち、1 秒インターバルで動作する場合、1 秒後に応答通信になり、通信の送信／応答を完結するには 2 回のインターバル時間を必要となります。高速でデータ通信をするならば、通信確認の応答がない通信の利用を行い、アプリケーション側で正しく送信されたことを確認するように実装したのが、高速化ができます。



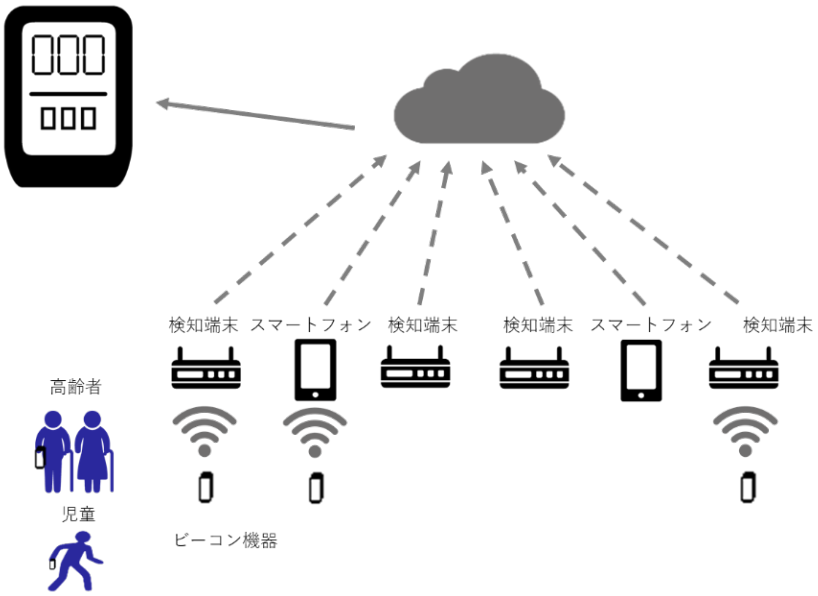
Bluetooth low energy の通信規格について説明をしましたが、従来の Bluetooth low energy のコンセプトは、名前の通り低消費電力で動作をすることを目的にしています。そのため、少量のデータを通信することに適しています。そして、数年間バッテリーを交換なしで長時間使用可能にします。低消費電力の電子機器や電池アプリケーションを、Bluetooth で接続をして、その後、データをインターネットに接続を可能にする目的でした。

昨今の Bluetooth 規格の Bluetooth low energy は、Bluetooth 4.0 で制定された規格をベースに改訂されました。規格は、大きな容量、高速通信、長距離通信が追加されました。Bluetooth 5 は、これらの機能がオプションとして 2016 年にリリースされています。

今後も、**Bluetooth low energy の基本規格(Bluetooth4.0 で制定された規格)は必須の機能となります。そして、Bluetooth low energy のどの製品でもサポートしています。この基本規格を使用することで、確実に繋がることできます。そして、今後も多くの機器で使用されます。そして、接続性の問題が起こり難いものと考えています。**

それでは、Bluetooth low energy が使用されているアプリケーション例を紹介します。まずは、従来の Bluetooth ではなかったアドバタイジング・パケットのブロードキャストを利用してアプリケーションを実現しているビーコン機器の応用例を紹介します。

高齢者や児童等にビーコン機器を所持して利用します。そのビーコン機器の電波を受信するために、施設に検知端末を設置します。検知端末の設置例としては、児童向けには学校、高齢者向けには公民館に設置、そして家や公共の場所に設置をします。その他に、地域のボランティアによる特別なアプリケーションがインストールしたスマートフォン保有します。スマートフォンは、ビーコン機器の電波を受信します。そして、検知端末やスマートフォンが受信をしたビーコン情報を、それぞれの検知端末やスマートフォンの位置情報と共に、クラウドに蓄積されます。クラウドに蓄積されたデータは、ビーコン機器に関連する保護者のみに、スマートフォンの地図にビーコンの位置情報を示すことができます。そのため、ビーコン機器を所持している人を把握できて、見守り端末に応用されています。



見守り端末の応用例

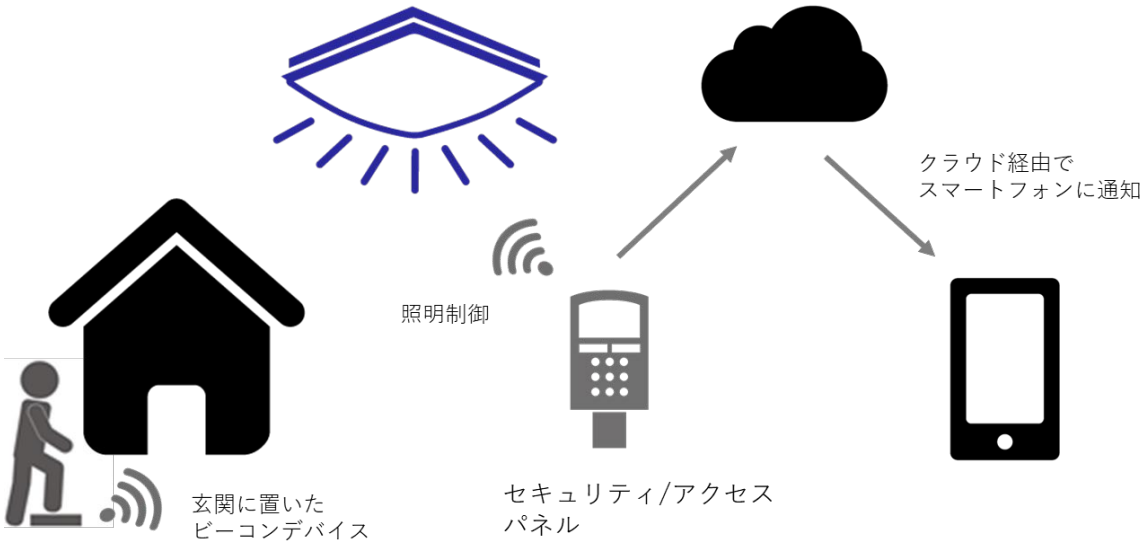
この事例は、下記ホームページでも紹介をしています。ご参照ください。

IoT 技術を活用した見守りサービス「otta」を進化させた BLE ソリューション
https://www.renesas.com/promotions/cases/bluetooth-low-energy-1.html

アドバタイジング・パケットのブロードキャストを利用したアプリケーションを、もう一つ紹介します。Bluetooth low energy をセンシングに使う使用例です。

玄関に置いたビーコンデバイスにより、防犯用途や家電を制御するためのスイッチやセンサとして利用できます。これにより、リモコンが不要となり、人の手を介在しないホームオートメーションを実現できます。

Bluetooth low energy は低消費電力の規格です。そのため、機器はエナジーハーベストの少ないエネルギーで、アドバタイジング・パケットを送信できます。下記の場合、マット型の足で踏んだエネルギーでビーコン（アドバタイズ・パケット）を送信できます。このデバイスは、電池交換不要で半永久的に動作をすることができるメリットがあります。ビーコン電波をセキュリティ/アクセス・パネルが受信をします。そこから照明制御、クラウド経由で、家族に通知をすることができます。防犯や高齢者の見守りにも使用できます。



センシングデバイスへの応用例

このように、アドバタイジング・パケットのブロードキャストを利用してアプリケーションを実現しているビーコン機器向けに、Bluetooth low energy のすべての機能を使用しない、ビーコン機器に使用するアドバタイジング・パケットのブロードキャスト(送信)と、その受信（スキャン）に特化したビーコンスタックを用意しています。

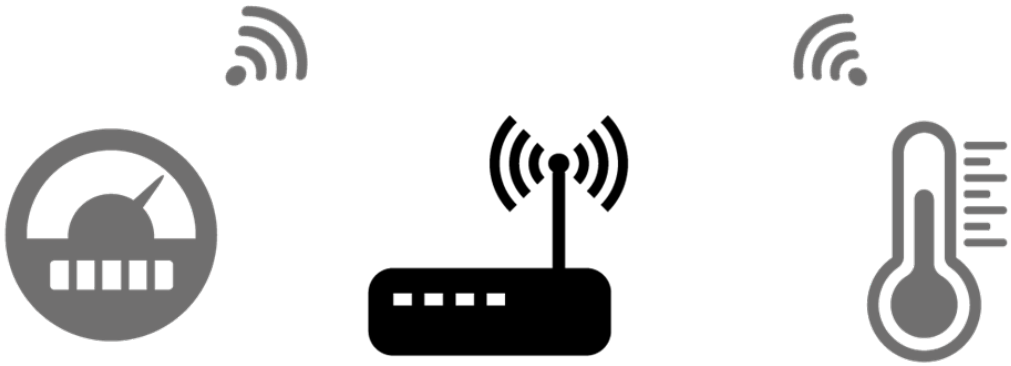
ビーコンスタックは、機能を限定しているため、プログラム構造はシンプルで、プログラムサイズは小さいです。そのため、プログラムのコンパイルは評価版でビルトができます。また、低消費電力で起動をして、動作することができます。

次に、Bluetooth low energy の機器を接続してデータ通信をして使用するアプリケーション例を紹介します。Bluetooth low energy 規格はスマートフォンにサポートされています。Bluetooth low energy は、容易にデータを収集ができる低消費電力無線インタフェースとして利用されています。そのため、ヘルスケア機器は、スマートフォンと接続をして多くの機器が利用されています。下記は例となりますが、心拍計、血圧計、体重計から、あらゆる計測機やセンサデバイスに利用されています。

スマートフォンと接続しての使用例

その他、Bluetooth low energy 機器を接続してデータ通信の使用は、機器間のデータ通信に利用されています。その例について紹介します。

Bluetooth low energy センサデバイスが、クラウドにデータ蓄積のため Bluetooth low energy と LTE/3G 等のゲートウェイ(ブリッジ)と接続して利用することがあります。ゲートウェイ(ブリッジ)は LTE/3G 等を経由してクラウドにアップされます。このように利用されるのは、Bluetooth low energy が低消費電力であるところにあります。センサ・エンドデバイスのデータ通信に、Bluetooth low energy が採用されています。そして、ゲートウェイ(ブリッジ)先としては、長距離通信ができる無線規格が採用されています。

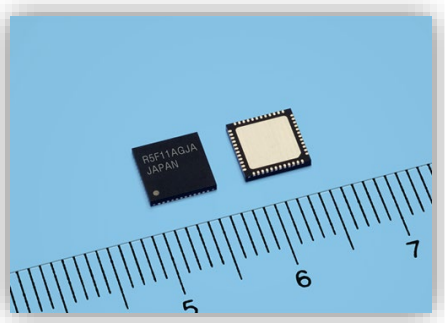


機器と接続しての使用例

アプリケーション例のように、アプリケーションの使い方としては、アドバタイジング・パケットのブロードキャストを利用するアプリケーションと Bluetooth low energy の機器

と接続してデータ通信をして使用するアプリケーションの 2 つに分けることができます。そこでルネサスでは、ソフトウェアスタックは、Bluetooth low energy プロトコルスタックと、ビーコンスタックの二つを用意しています。目的に合わせて選ぶことができます。

また、ルネサス製品には、Bluetooth 4.2 Certification の IC 製品とモジュール製品があります。量産規模、開発期間、RF 技術の有無に応じて、IC 製品、モジュール製品の選択できます。



RL78/G1D(R5F11A)

RL78/G1D モジュール（RY0711）

ルネサス エレクトロニクスの Bluetooth® low energy ソリューションはこちらから：
https://www.renesas.com/solutions/bluetooth