Bluetooth® LE の多様な通信モード

$ADVB_L$ – レガシー アドバタイズ

レガシー アドバタイズ ($ADVB_L$) の理解

Bluetooth Low Energy (LE) が Bluetooth コア仕様バージョン 4.0 で初めて登場した時、通信モードは 2 種類のみでした。1 つは接続指向の LE-ACL モードで、このシリーズの別の記事でも取り上げました。もう一つは非公式にアドバタイズと呼ばれていました。

この元々のアドバタイズは、技術的には Bluetooth LE の論理伝送の一つであるアドバタイズ ブロードキャストとして定義され、ADVB をアドバタイズ ブロードキャストの略称として使います。

Bluetooth Core 仕様 (v5.0) の後期バージョンでは、ADVB が拡張アドバタイズとして知られるより高度な機能セットを追加して強化されました。この時点で、元のアドバタイズ機能は「レガシー アドバタイズ」と呼ばれるようになり、これら二つのアドバタイズを区別するようになりました。

レガシー アドバタイズと ADVB 論理伝送の新しい拡張版は、それぞれ別々に扱うべき十分なテーマであるため、本記事ではレガシー アドバタイズのみを扱い、$ADVB_L$ をレガシー アドバタイズ ブロードキャストの略称として使います。

概要

ADVB$_L$ を用いた通信は、LE-ACL 接続を使った通信とは大きく異なります。最も明白な違いは、この論理伝送が*コネクションレス(非接続型)*通信の一形態を提供することです。これは、LE-ACL の接続型通信とは異なり、デバイス間で事前の合意がなく、それぞれが独立して送信・受信を行うことを意味します。

アドバタイズは、1 台のデバイスが間隔をあけてパケットを送信し、他の 1 台以上のデバイスがスキャンによってパケットを受け取る仕組みです 。しかし、ADVB$_L$ のコミュニケーションモードはこれ以上に複雑であり、この記事の残りの部分で学びます。

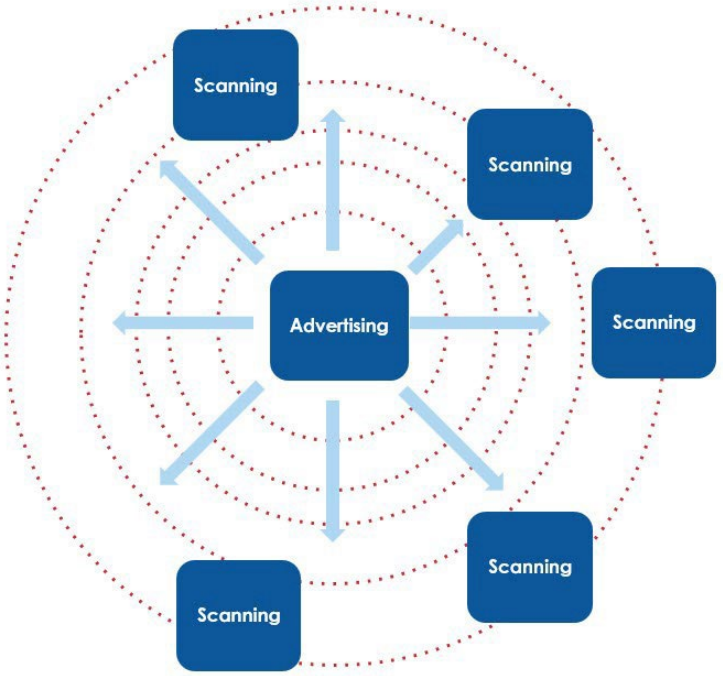

図 1 アドバタイズとスキャン

ADVB$_L$ はもともと 2 つのユースケースを念頭に置いて設計されました。*デバイス検出 (Device discovery)* がこれらのユースケースの最初の例でした。*ビーコン*は、単一のデバイスが変化しない情報を繰り返し送信するもので、2 つ目のユースケースでした。ADVB$_L$ を任意で可変なデータを扱う一般的な非接続型通信の伝送として利用することは常に可能でしたが、一般的には使われていませんでした。

レガシー アドバタイズ

デバイスがアドバタイズを出す場合、単に他のデバイスにデータを転送するだけではありません。送信されたパケットを受信したデバイスが実行できるアクションの可能性も示します。

Bluetooth コア仕様は、さまざまな種類のアドバタイズ イベントを定義しています。さまざまなイベントタイプは、異なる種類のプロトコル データユニット (PDU) の伝送を伴い、受信デバイスが独自の PDU で応答する場合もあります。

アドバタイズ イベントの種類によって、異なるいくつかの変数があります。これらの変数は表 1 のリストで説明します。

タイプ	説明
接続型 vs 非接続型 Connectable vs Non-connectable	他のデバイスからの接続要求を受け入れることができる(LE-ACL 接続を形成できる)ことを示すアドバタイズ デバイスは *接続可能なアドバタイズ*を行います。接続を行わないアドバタイズ デバイスは *非接続アドバタイズ*を行います。
スキャン可能 vs スキャン不可 Scannable vs Non-scannable	アドバタイズ デバイスは、送信するアドバタイズ パケットにスキャン要求によってより多くの情報を提供できることを通知できます。これは *スキャン可能なアドバタイズ*を行うことで実現します。デバイスが追加情報を求める場合、*アクティブスキャン*を行っていると言います。追加情報を提供しないアドバタイズ デバイスは *スキャン不可のアドバタイズを行い*、受信デバイスは *パッシブスキャン*を実行していると言います。
指向性 vs 無指向性 Directed vs Undirected	論理伝送の名前であるアドバタイズ *ブロードキャスト*(advertising broadcast) が示すように、アドバタイズ デバイスは範囲内にあるキャン中の全てのデバイスが受信することを意図したパケットを送信できます。これは *無指向性アドバタイズ*として知られています。しかし、アドバタイズ デバイスから特定のデバイスにパケットを送信するためにも使われ、これを *指向性アドバタイズ*と呼びます。

表 1 アドバタイズのイベント タイプ

ADVB$_L$ は、これらの変数を 4 通りの組み合わせで使用できます。構成できるアドバタイズ イベント タイプは以下の 4 種類です。

1. 接続型、スキャン可能、無指向性　(connectable and scannable undirected)
2. 接続型、指向性 (connectable directed)
3. 非接続型、スキャン不可、無指向性 (on-connectable and non-scannable undirected)
4. スキャン可能、無指向性 (scannable undirected)

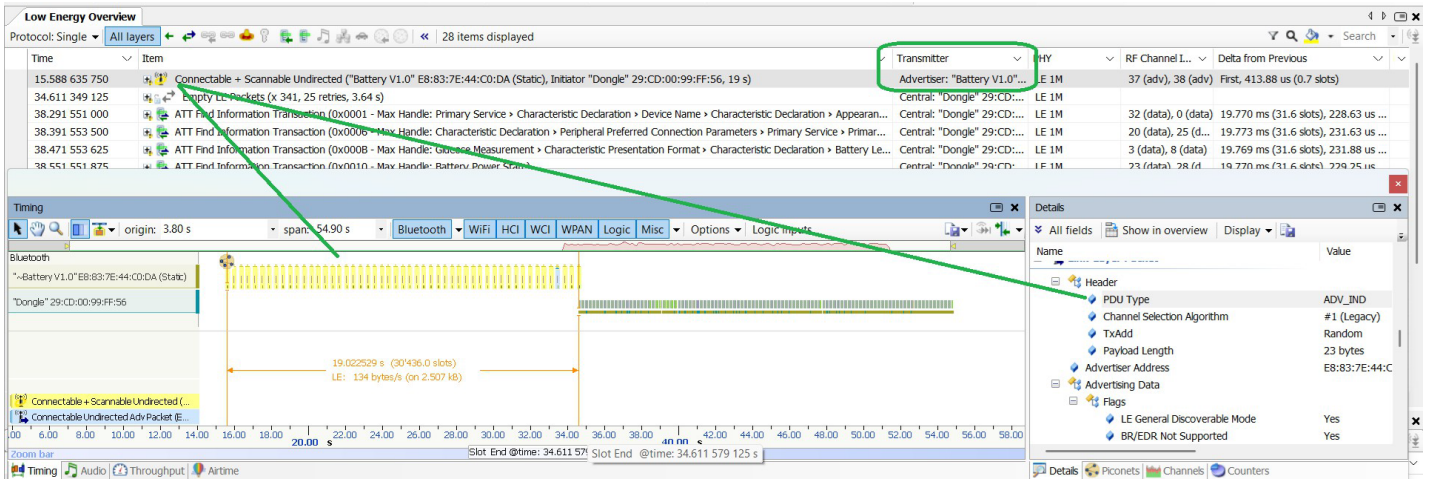

図 2 バッテリー デバイスが "接続型、スキャン可能、無指向性" のアドバタイズを送信している様子 (Ellisys Bluetooth 解析ソフトウェア)

アドバタイズ デバイスにはもう一つの特性があり、それは *検出可能*かどうかというものです。これは Bluetooth コア仕様の Generic Access Profile (GAP) として定義されています。GAP には、他のデバイスの検出や自分を他のデバイスに検出させるといった目的でリンク層の機能を使用するためのルールが含まれています。

*検出可能*は誤解されがちな概念です。

正しいチャネルでスキャンしているデバイスは、範囲内にある他のデバイスが送信したパケットを受信できます。その意味では、すべてのデバイスが検出可能と言えるでしょう。しかし、Bluetooth コア仕様と GAP の文脈では、検出可能はより微妙な定義と目的を持ちます。デバイスが検出可能モード(2 つあります)のいずれかにある場合、それは単に検出されることを意図していることを意味します。これにより、受信側デバイスは、検出されることを意図していないデバイスを、グラフィカルユーザーインターフェース(GUI)の表示といった後処理から除外できます。検出不可能なデバイスは、*見えない*デバイスではないことを理解することが重要です。つまり、これはセキュリティ機能ではありません。

デバイス ロール(役割)

GAP はアドバタイズとスキャンに関連する 4 つのデバイスの役割を定義しています。

- **ブロードキャスター** - このロールでは、デバイスはパケットを送信しますが受信しません。そのため、ブロードキャスターに接続することはできません。
- **オブザーバー** - オブザーバーはブロードキャスターに対応するデバイスです。アドバタイズ パケットを受け取り、追加情報を求めるために応答することは可能ですが、ブロードキャスターと接続することはできません。
- **ペリフェラル** - GAP ペリフェラルはアドバタイズ パケットを送信し、使用中のアドバタイズ イベントの種類に応じて接続要求やスキャン要求などのパケットを受け取ることができます。
- **セントラル** - GAP セントラルは GAP ペリフェラルに対応するデバイスです。アドバタイズ パケットはスキャンによって受信し、使用されるアドバタイズ イベントの種類に応じて送信された接続要求やスキャン要求に応答することができます。

リンク層でも、ペリフェラル と セントラル という用語が使われていることに注意してください。これらの用語の意味は 2 層間で一致せず、リンク層ではデバイスが接続されている場合にのみ適用されます。しかし、GAP ペリフェラルは接続時にリンク層ペリフェラルの役割を担い、GAP セントラルは GAP ペリフェラルと接続を確立した後にリンク層セントラルの役割を担います。

パケットと PDU

リンク層は一般的なアドバタイズ パケットのフォーマットを定義します。アドバタイズ パケットのペイロードには複数の異なる PDU が送信でき、アドバタイズ イベント タイプごとに異なる PDU タイプ、アクティブ スキャンのリクエスト PDU やレスポンス PDU、接続確立のための PDU も存在します。

送信可能な PDU の種類は、表 2 にまとめられているように、アドバタイズ イベントの種類とデバイス ロールによって異なります。

PDU	送信時	送信者
ADV_IND	接続型、スキャン可能、無指向性	ブロードキャスターまたは ペリフェラル
ADV_DIRECT_IND	接続型、指向性	ブロードキャスターまたは ペリフェラル
ADV_NONCONN_IND	非接続型、スキャン不可、無指向性	ブロードキャスターまたは ペリフェラル
ADV_SCAN_IND	スキャン可能、無指向性	ブロードキャスターまたは ペリフェラル
SCAN_REQ	ADV_IND または ADV_SCAN_IND への応答	オブザーバーまたは セントラル
SCAN_RSP	SCAN_REQ への応答	ブロードキャスターまたは ペリフェラル
CONNECT_IND	ADV_IND または ADV_DIRECT_IND への応答	セントラル

表 2 アドバタイズ PDU

スケジュール

他の Bluetooth 通信モードと同様に、ADVB$_L$ には無線の使用時間に関するルールが含まれています。これらのルールは、ブロードキャスターまたはペリフェラルとしてアドバタイズを送信するデバイスと、スキャン要求を送信するデバイス（オブザーバーとセントラル）または接続要求を送信するデバイス（セントラルのみ）の両方に適用されます。

アドバタイズ

従来のアドバタイズ送信は *アドバタイズ イベント* 内で行われます。アドバタイズ イベントは、デバイスがリンク層のアドバタイズ状態に入ったときに始まります。次のアドバタイズ イベント開始は、アドバタイズ インターバル (advertising interval) と呼ばれるタイミング パラメータと、ランダムに生成される値であるアドバタイズ ディレー (*advDelay*) から計算されます。アドバタイズの間隔は 20ms から 10.24s の範囲で、アプリケーションの要求に応じて設定されます。advDelay の値は、アドバタイズ イベントの開始時にランダムに新たに選ばれ、0～10ms の範囲です。

*アドバタイズ イベント*が始まると、ブロードキャスターやペリフェラルは同じパケットのコピーを 3 つの異なる無線チャネルに 1 つずつ 10ms 以内の間隔を空けて送信します。従来のアドバタイズパケットは短く、送信に必要な時間は 400µs 未満なので、10 ミリ秒で十分で、場合によってはそれ以上の送信でも可能です。

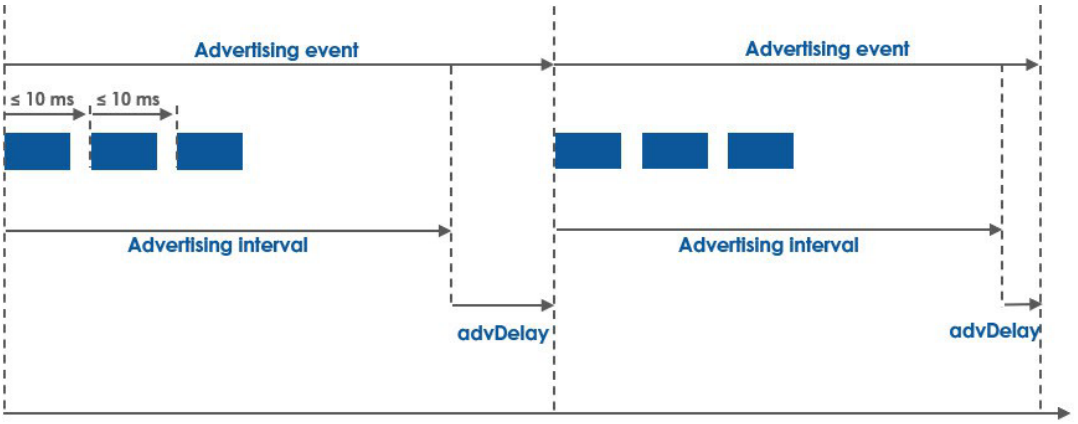

図 3 アドバタイズの送信タイミング (Interval, advDelay, event)

注：このルールには例外があります。本文書の *“ご存じですか？”* のセクションに、高デューティサイクルと低デューティサイクルのアドバタイズメントに関する興味深い記述があります。

ランダムに生成される advDelay 変数をアドバタイズ イベントのスケジュールに含めると、アドバタイズの時間的変動が生じます。言い換えれば、従来のアドバタイズは LE-ACL 接続におけるイベントを制御する規則的なタイミング パターンであるのに対し、不規則なタイミング スケジュールに従うことになります。

パケットの衝突は、2 台以上の異なるデバイスが同じ無線チャネル上に同じ時間にパケットを送信した場合に発生します。衝突が発生すると、パケットが破損します。アドバタイズ スケジュールをランダム化することで、異なるデバイス間で継続的に繰り返し衝突が発生する確率を大幅に低減することができます。

スキャン

単一チャネルのスキャンは、*スキャン インターバル* と呼ばれるタイミング パラメータに従って定期的に実行されます。デバイスが選択されたチャネルをスキャンする時間は、*スキャンウィンドウ*と呼ばれるパラメータによって制御されます。

アクティブスキャンを使用する場合、オブザーバーまたはセントラル デバイスは、ADV_IND PDU や ADV_SCAN_IND PDU への応答として、SCAN_REQ PDU を同じ無線チャネル上に送信することにより、追加の情報を要求できます。アドバタイズ デバイスは同じ無線チャネルで SCAN_REQ PDU を受信すると、SCAN_RSP PDU で追加データを送信します。

SCAN_REQ PDU および SCAN_RSP PDU を送信する前には、フレーム間スペース (IFS: Inter Frame Space) に等しい間隔を空ける必要があり、連続する ADV_IND PDU または ADV_SCAN_IND PDU の開始間隔は 10ms を超えてはなりません。これを図 4 に示します。

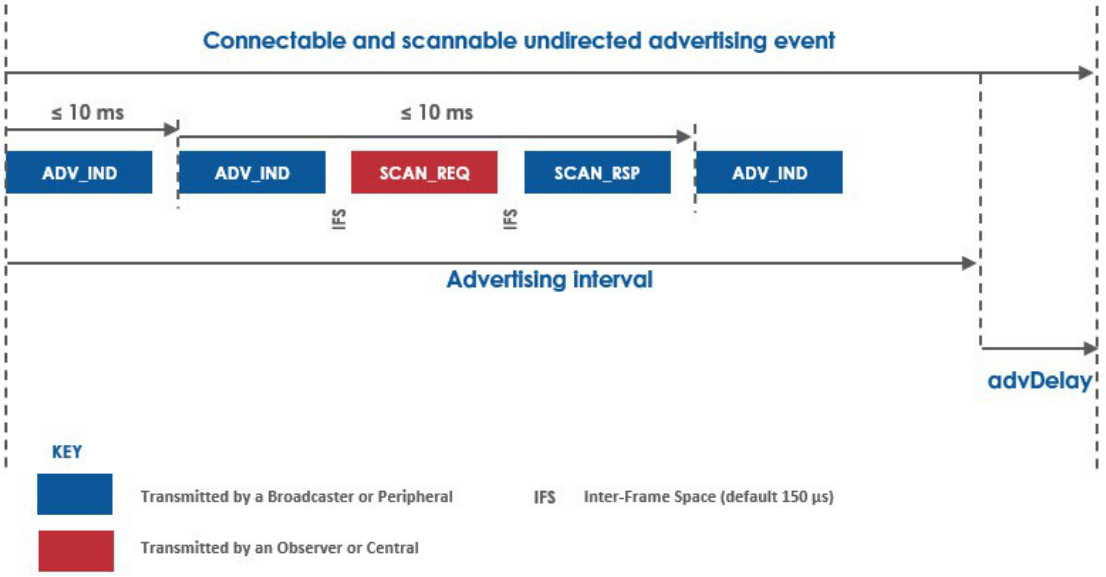

図 4 SCAN_REQ および SCAN_RSP PDU のスケジューリング

接続の開始 (Initiating)

接続を要求するデバイスはリンク層の開始状態 (Initiating state) にあります。

接続可能なアドバタイズ イベントでアドバタイズ パケットをスキャンしているデバイスは、ADV_IND PDU や ADV_DIRECT_IND PDU に対して CONNECT_IND PDU で応答できます。これは、スキャンしているデバイス(セントラル)がアドバタイズ デバイス(ペリフェラル)に接続を要求することです。

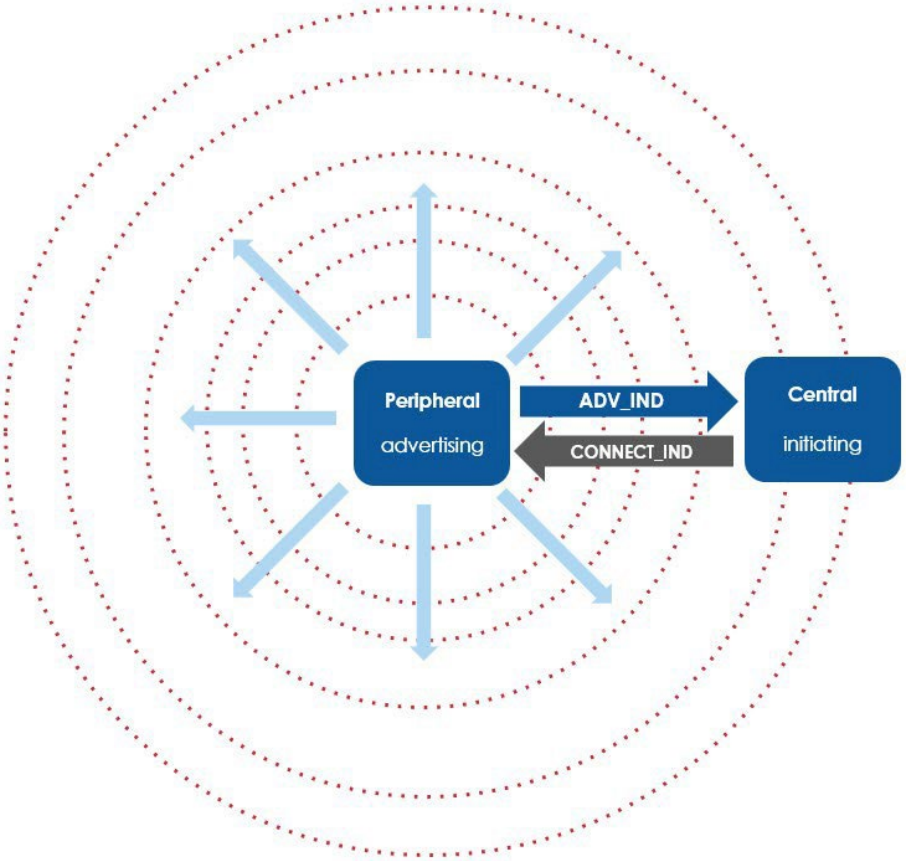

図 5 ADV_IND PDU に CONNECT_IND PDU で応答するセントラル デバイス

アドレス指定

すべてのレガシー アドバタイズ PDU には、アドバタイズ デバイス自身の Bluetooth デバイス アドレスを含むフィールドが含まれています。このフィールド名は AdvA です。

ADV_IND、ADV_NONCONN_IND、ADV_SCAN_IND PDU は、アドバタイズ デバイスが無指向性アドバタイズイベントで送信し、ターゲットの Bluetooth デバイス アドレスは含みません。これらの PDU は定義上、特定のデバイスを対象としていません。ただし、AdvData というフィールドがあり、このフィールドにアプリケーション データを格納できます。

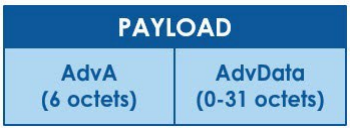

図 6 ADV_IND、ADV_NONCONN_IND、ADV_SCAN_IND PDU のフィールド

ADV_DIRECT_IND PDU は接続型で指向性のアドバタイズ イベントで送信され、特定のデバイスを対象としています。この PDU にはターゲットデバイスの Bluetooth デバイスアドレスを含む TargetA というフィールドが含まれていますが、AdvData フィールドが存在しないことに注意してください。

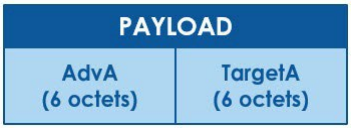

図 7 ADV_DIRECT_IND PDU のフィールド

SCAN_REQ PDU と CONNECT_IND PDU は、送信元、スキャン デバイスのアドレスとアドバタイズ デバイスのリモートアドレスの両方が含まれています。

SCAN_RSP PDU は受信した SCAN_REQ PDU に応答するアドバタイズ デバイスのアドレスが含まれますが、ターゲットデバイスのアドレスは含まれていません。

無線チャネル

ADVB$_L$ は 2.4 GHz 帯を 2 MHz の幅の 40 チャネルに分割し、そのうちの 3 つの特定チャネルをアドバタイズに使用します。これらの チャネルはプイライマリ アドバタイズ チャネルと呼ばれます。

プライマリ アドバタイズ チャネルは、Wi-Fi 通信の影響を受けないように、また少なくとも 1 つが正常に機能する可能性を最大化するために、チャネル同士が十分な間隔を保つよう慎重に選ばれました。

プライマリ アドバタイズ チャネルのチャネル インデックス番号は 37、38、39 です。

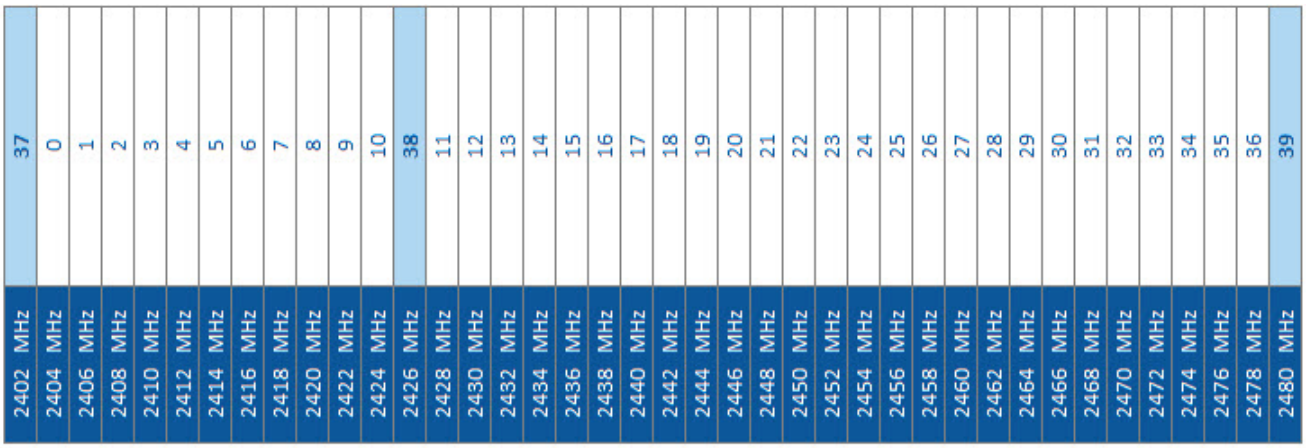

図 8 プライマリ アドバタイズチャネル (薄青色で表示)

アプリケーションはプライマリ アドバタイズ チャネルのうち 1 つ、2 つ、または 3 つすべてを使用するよう選択でき、これはアドバタイズ チャネル マップと呼ばれるデータ構造で示されます。

各アドバタイズ イベントでは、リンク層はアドバタイズ チャネル マップに従い使用中の各チャネルに同じアドバタイズ パケットのコピーを送信します。チャネルの順序は、各アドバタイズ イベントでランダムに選ばれます。

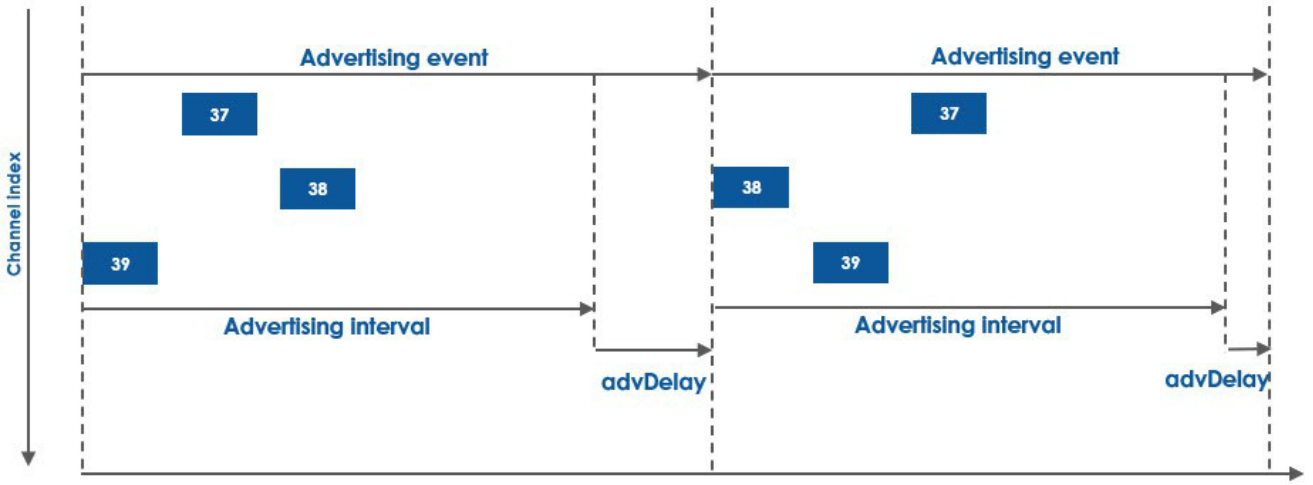

図 9 ランダムに選ばれたプライマリ アドバタイズ チャネルでのアドバタイズ

物理層

従来のアドバタイズ PDU、すなわち ADV_IND、ADV_DIRECT_IND、ADV_NONCONN_IND、ADV_SCAN_IND、SCAN_REQ、SCAN_RSP、CONNECT_IND は LE 1M PHY のみが使用可能なので、100 万シンボル/秒のシンボル レートで送信されます。

アプリケーション上の懸念

アプリケーションには独自の要件や優先順位があります。このセクションでは、Bluetooth ADVB$_L$ 非接続型通信の利用に関するアプリケーション上の問題をいくつか検討します。

コンフィグレーション

アプリケーションは、レガシー アドバタイズの機能に影響を与える複数のパラメータを指定または提案することができます。ホスト コントローラー インターフェース (HCI) コマンド *"LE Set Advertising Parameters"* を使用することで、アプリケーションは例えば以下のことが行えます。

- アドバタイズ間隔の最小値と最大値の指定
- アドバタイズ種類の指定
- ピア (リモート) デバイスのアドレス指定
- 使用する 3 つのプライマリ アドバタイズ チャネルの指定

アドバタイズ間隔は製品のスケジューリング アルゴリズムによって選択されますが、これは Bluetooth コア仕様で完全に規定されておらず、実装上の問題です。アプリケーションの要求範囲内の値を取得できない場合、コントローラーは HCI イベントでアプリケーションにエラーを返します。

アドバタイズ タイプの設定パラメータは、リンク層が使用するアドバタイズ イベント タイプと関連する PDU を決定します。

ピア アドレスは、指向性アドバタイズを行う場合にのみ意味があります。

アドバタイズ チャネル マップは、連続した 3 ビットで、アドバタイズ パケットの送信に使用するプライマリ アドバタイズ チャネルを指定します。

HCI はレガシー アドバタイズを設定するためのコマンドとパラメータを定義していますが、アプリケーション開発者はプラットフォームの API を通じてすべてのパラメータにアクセスできるとは限らないことに注意してください。特定のプラットフォーム向けに開発されるアプリケーションの機能や制約を確認するために、必ず API ドキュメントを参照してください。

アプリケーションデータ

4 つのレガシー アドバタイズ PDU のうちの 3 つには AdvData というフィールドが含まれています。このフィールドには、アプリケーションが他のデバイスと通信したいデータが入っています。

前述の図 6 で示したように、可変長の AdvData フィールドには最大 31 バイトを格納できますが、実際にはその全てがアプリケーション データというわけではありません。これは、アプリケーションが AdvData フィールドに一連のデータ項目を設定することができ、各項目は AD タイプと呼ばれるデータ構造内にエンコードされる必要があるためです。

すべての AD タイプは同じ 3 つのフィールド構造を持っています。

- **Length**（長さ）- 他の 2 つのフィールドが占めるバイト数を示す 1 バイト
- **Type**（タイプ）- 最後のフィールドに含まれるデータ タイプを示す識別子の 1 バイト
- **Value**（値）- アプリケーション データ自体を構成する可変長バイト（長さは Length – 1）

図 10 は、接続型、スキャン可能な無指向性イベントで送信されたアドバタイズ パケットです。ペイロードは 16 進形式で提示され、合計 11 バイトの長さです。これが AdvData フィールドです。

図 10 アドバタイズパケットの Ellisys Bluetooth アナライザによる表示

注： *心拍数モニターのアドバタイズ パケットは、Nordic Semiconductor nRF54L15DK 開発キットで生成されました。*

AD タイプの Length/Type/Value 構造による分類:

Length	Type	Value (HEX)
02	01	06
07	03	0D18 0F18 0A18

表 3 アドバタイズ PDU の AdvData フィールド内の AD タイプ

該当する仕様書でタイプや構造を調べることができますが、Ellisys の Bluetooth アナライザを使えばデータは自動的に解析されるので、その必要はありません。図 11 のように、アドバタイズ パケットに ADV_IND PDU が含まれ、AdvData に含まれるフィールドはデコードされて値と意味を表示しているのが解ります。

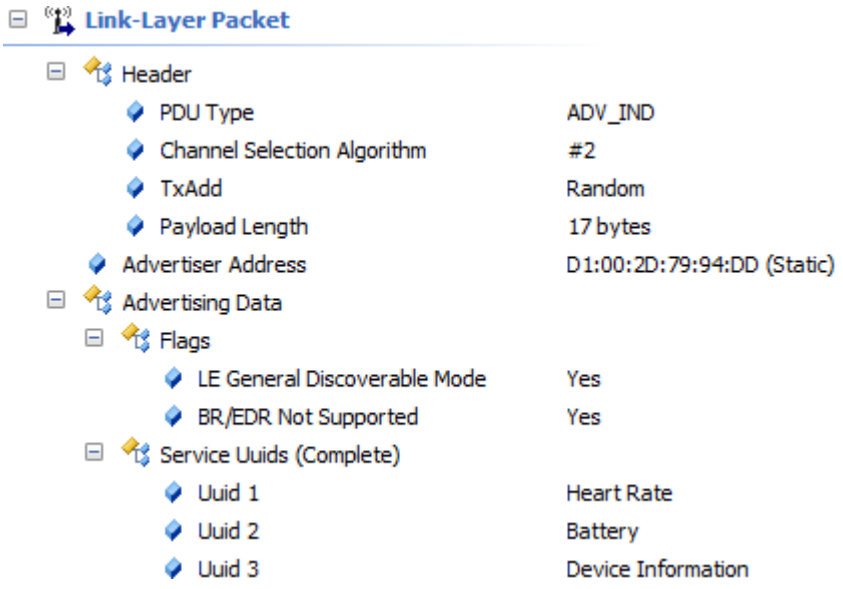

図 11 AdvData フィールドのデコードされた内容

Flags フィールドは、このデバイスが 2 つの検出可能なモードのいずれかにあることを示しています。

Bluetooth LE の汎用属性プロファイル (GATT: Generic Attribute Profile) は、デバイス内に実装された機能（**サービス**）とデータ（*特性と記述子*）を識別するために、UUID (Universally Unique Identifier を用います。このアドバタイズ パケット内のサービス UUID は、アドバタイズ デバイスが心拍数、バッテリー残量や一般的なデバイス情報を提供する GATT サービスをサポートしていることを示します。アプリケーションに関連する他のデバイスを検出したいスキャン デバイスにとって、この情報は有用です。少しの知識があれば、Ellisys プロトコルアナライザが提供した情報から、検出されたデバイスが Bluetooth 心拍数プロファイルに対応していることが一目でわかります。

AD タイプは、Bluetooth core Specification Supplement（コア仕様補足文書）で定義され、タイプ識別子は Bluetooth SIG Assigned Numbers（Bluetooth SIG 割当て番号文書）で定義されていることに注意してください。

一般的なデータ通信

$ADVB_L$ は非接続型通信の一般的な通信として利用できます。AdvData フィールドと、すべてのデータ項目のパッケージング構造として AD タイプを用いるため、アドバタイズ PDU で送信できるデータ量は非常に少ないものの、多くのユースケースで有効活用できます。

ADVB$_L$ が一般的な通信手段として選ばれる主な理由:

- **シンプル** - 事前に接続を確立する必要がなく、デバイス検出を行う必要もない
- **スケーラビリティ** - デバイスは同時接続数が限られているため、接続を用いた場合には同時に通信できるデバイス数は限られます。一方、ADVB$_L$ は送信された各パケットを任意の数のデバイスで受信できます。

次の例を考えてみましょう。新しい電力モニター製品は、一度に 1 つの接続しかサポートできない制約のあるマイクロコントローラーをベースにする必要がありました。しかし、この製品の要件には、複数のスマートフォンやデータ ロギング サーバーなど複数のデバイスにリアルタイムの電力消費データを同時に通信することが含まれていました。そこで転送方法として ADVB$_L$ が選ばれ、マイクロコントローラーは電力値をブロードキャストするようにしました。これにより、関連するスマートフォン アプリや Linux データ ロギング サーバーで同時に受信できるようになります。Linux データ ロギング サーバーにはすべての測定値が保存され、過去の電力消費分析が可能になります。

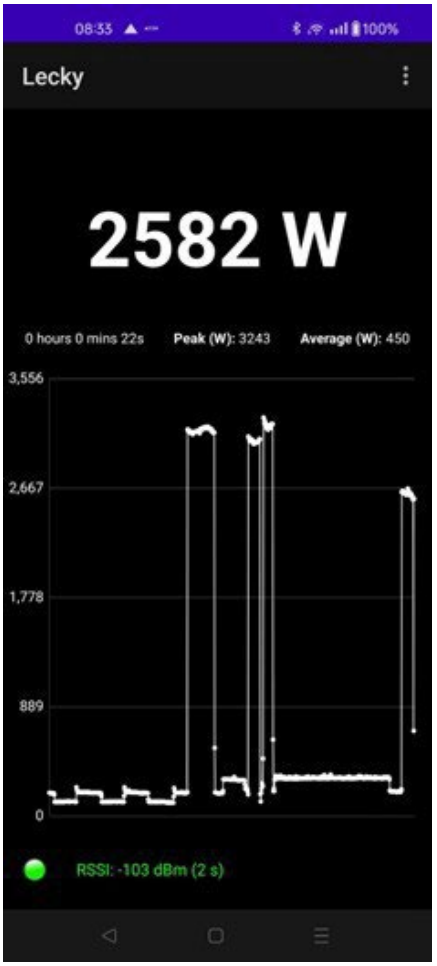

図 12 スマートフォン アプリで受信、使用される ADVB$_L$ ブロードキャスト データの様子

Ellisys プロトコル アナライザ ソフトウェアを使えば、このデバイスからのブロードキャストと、テスト中に記録されたサンプル パケットを検証できます。(図 13 参照)

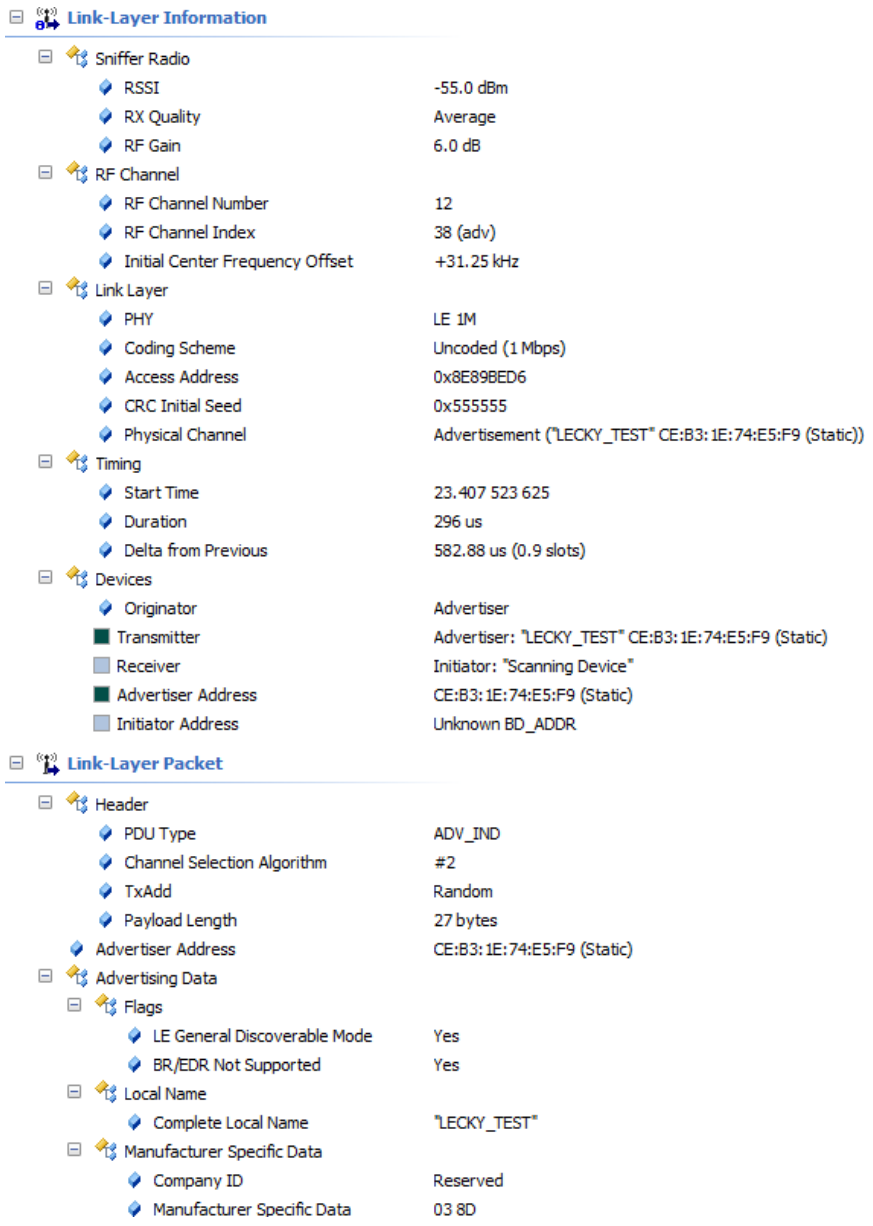

図 13 電力モニターのペリフェラル デバイスが送信した ADV_IND パケット

注：電力モニターのアドバタイズパケットは、Nordic Semiconductor nRF52833 搭載の BBC microbit V2 で生成されました。

図 13 には多くの有用な情報が示されています。

- パケットはプライマリ アドバタイズ チャネル 38 で送信
- アドバタイズ デバイスのアドレスは CE:B3:1E:74:E5:F9
- アドバタイズ イベントタイプは接続方、スキャン可能、無指向性で、PDU タイプは ADV_IND
- デバイスは検出可能
- AdvData フィールドに、"LECKY_TEST" の値を持つ Complete Local Name と、2 つのサブフィールドを持つ Manifactuurer Specific Data（メーカー固有データ）が存在

メーカー固有データの AD タイプは特に注目に値します。標準 AD タイプが定義されていない任意のデータをこのフィールドに入れることができます。使用上のルールは、メーカーの Company ID（Bluetooth SIG が発行）をメーカー固有データのサブフィールドでアプリケーション データの前に配置することです。これにより、受信したデバイスは、その会社の仕様に基づいてデータをデコードできます。図 13 の例では、このフィールドにワット単位の電力値が配置されており、16 進数 0x038D をビッグエンディアン値としてデコードすると、電力モニターが 909 ワットの電力使用量を報告していることがわかります。

しかし、$ADVB_L$ が一般的なデータ伝送手段として使われている最良の例は Bluetooth Mesh ネットワークでしょう。Bluetooth Mesh は、ネットワークを横断するメッシュ メッセージの伝送手段として $ADVB_L$ を使用し、センサー データの活用や照明の制御などを可能にしています。これは $ADVB_L$ が一般的な非接続型通信をサポートする能力を持っているという強力な根拠となります。Bluetooth Mesh プロトコル仕様では、$ADVB_L$ の使用が伝送手段として定義されていることに注意してください。

エネルギー効率

アドバタイズ デバイスの場合、小さなパケットの伝送はエネルギーコストが低いので、考慮すべき唯一の変数は送信パケット数です。これはアドバタイズ間隔の値と使用チャネル数によって制御できます。ただし、アドバタイズ間隔が長いとスキャン アプリケーションの応答性に影響があり、利用可能なアドバタイズ チャネルを 3 つ未満にすると通信の信頼性低下の可能性があります。しかし、エネルギー効率が最優先であれば、これらの変数を考慮すべきです。

スキャン デバイスの場合、エネルギー効率はより深刻な問題となります。$ADVB_L$ 通信は非接続型なので、スキャンデバイスはアドバタイズがいつ行われるかを予測できず、ランダムなアドバタイズ スケジュールもあまり役に立ちません。したがって、スキャンの頻度（スキャン間隔）と期間（スキャン ウィンドウ）は、エネルギーコストを増大させるほど長時間のスキャンをすることなく、十分な信頼性でデータを受信できるように慎重に考慮する必要があります。

信頼性

アドバタイズ パケットには巡回冗長検査 (CRC: Cyclic Redundancy Check) フィールドが含まれており、これにより送信中のデータ破損を検出できます。

$ADVB_L$ を用いた非接続型通信で信頼性が重要な場合、アプリケーション層で特定の手順を踏む必要があります。信頼性が重要でない場合もあると言うのは奇妙に思えるかもしれませんが、実際はそうです。例えば、ショッピングモールのビーコンから送信される同じ URL などは必ずしもスマートフォン アプリに受信される必要はないでしょう。

考慮すべき問題は、ブロードキャスターやペリフェラルのアドバタイズ スケジュールは、オブザーバーやセントラルのスキャンスケジュールとはいかなる形でも調整されていないという事実です。さらに、パケットは一度に 1 つのチャネルでしか送信できず、スキャンも一度に 1 つのチャネルでしか受信できません。パケットを受信するためには、3 つのチャネルのうち適切なチャネルで適切なタイミングかつ十分な期間スキャンする必要があります。ADVB$_L$ はデータ伝送として成功と失敗が混在するということです。下図 14 はその例です。

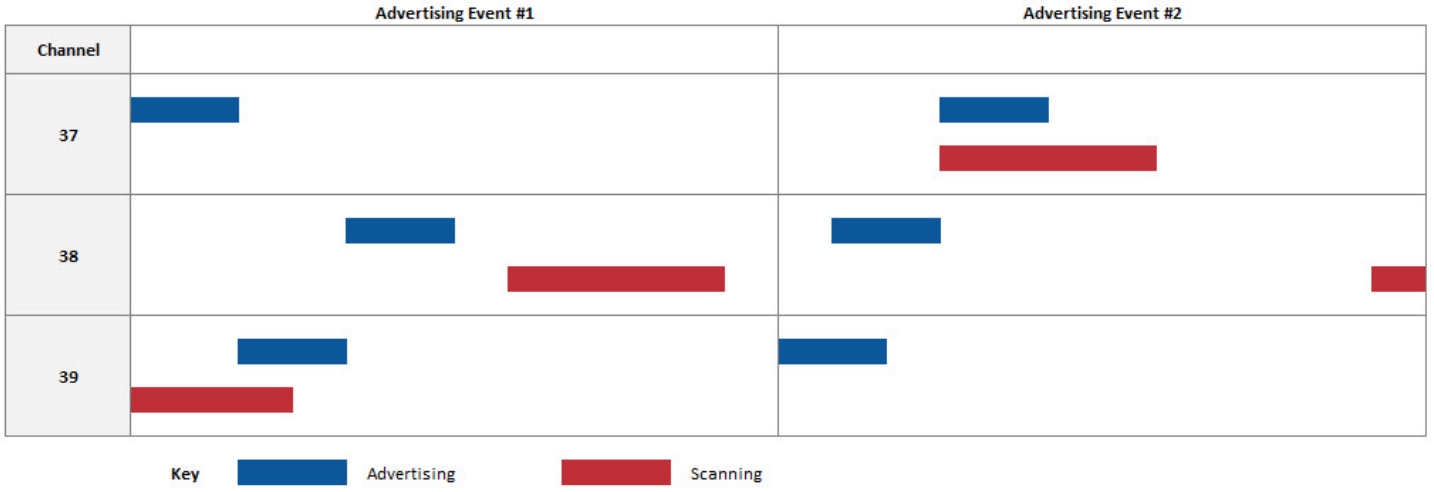

図 14 調整されていないスキャンとアドバタイズのスケジュール

ここでは、最初のアドバタイズ イベントで、最初にスキャンがチャネル 39 で行われ、送信されたアドバタイズパケットの最初の部分だけが重複していることがわかります。パケットが送信されていない時に、チャネル 38 でスキャンが行われます。2 回目のアドバタイズ イベントで、チャネル 37 でのスキャンがパケットの送信と完全に重複するため、今回は受信されます。

Bluetooth Mesh は、ADVB$_L$ をメッシュメッセージの伝送手段として信頼性を高めるための特別な技術を用いています。通常、メッセージは アドバタイズパケットとして複数回、高速バーストで送信されます。各メッセージを繰り返し送信することで受信される確率が劇的に高まり、一般的な非接続型通信に効果的です。

セキュリティ

データの機密性

Bluetooth Core Specification v5.4 のリリースまでは、アドバタイズ パケットで送信されるアプリケーション データの機密性を保護する標準的な仕組みは存在せず、そのようなセキュリティ要件はアプリケーション自身で対応しなければなりませんでした。

Bluetooth コア仕様 v5.4 では、暗号化アドバタイズ データという新機能が導入されました。アドバタイズ デバイスが AdvData に含めるデータを暗号化し、信頼できるデバイスと暗号鍵パラメータを共有するための標準化された仕組みを提供するということが重要です。

アドバタイズ デバイスが暗号化アドバタイズ データ機能を使用するには、ペリフェラル ロールを適用し、接続を受け入れる必要があります。これは、暗号鍵パラメータの共有は暗号化された LE-ACL 接続上で行われるので、デバイス同士がペアリングされている必要があるからです。

アドバタイズ デバイスは盗聴から守りたいデータ フィールドを単一の AD タイプの複合シーケンスとして暗号化し、その結果得られた暗号文を暗号化データ (Encrypted Data) と呼ばれる AD タイプに配置します。信頼され、暗号化キーパラメータを取得したスキャン デバイスのみがこの AdvData フィールドの部分を復号化できます。

プライバシー

アドバタイズ、スキャン、その他の目的で使用されるリンク層 PDU には、送信機器のアドレスを格納するフィールドが含まれることがよくあります（例：アドバタイズ用 PDU の AdvA）。デバイス アドレスの格納は必須の場合もオプションの場合もあります。デバイスアドレスは識別子であり、その役割を果たすためには静的である必要があります。

静的で変わらないデータを繰り返し送信するデバイスは追跡される危険性が高いと言えます。セキュリティの分野では、これは *プライバシーの問題* と分類されます。

この問題を軽減するために、Bluetooth デバイス アドレスに適用する *プライベート アドレス* と呼ばれる特別なアドレスが仕様書に定義されています。プライベート アドレスは一定の間隔で自動的に変更されます。変更頻度は実装によって異なりますが、コア仕様では約 15 分間隔を推奨しています。

デバイスのプライバシーを保護し、信頼できるデバイスによって確実に識別できるようにする必要がある場合 、特殊なタイプのプライベート アドレスである *解決可能なプライベートアドレス (RPA: resolvable private address)* が定義されています。RPA を使用する場合、デバイスには信頼性が高く不変の識別子として機能する隠*れた識別アドレス (identity address)* も持ちます。RPA と併用した場合、識別アドレスは公開されませんが、2 台のデバイスがペアリングされている場合に限り、デバイスは RPA を識別アドレスに変換または解決できます。

プライベート アドレスが変更されるたびに、暗号化されたアドバタイズ データ暗号化手順（上記 “データの機密性” 参照）の入力の一つである *nonce* も変化し、それに伴い暗号化データの価値も変化します。これもデバイスのプライバシー保護に役立ちます。

通信モードのプロパティ

このシリーズの最初の記事「Bluetooth LE の多様な通信モード」では、通信モードを比較するのに役立つ一連のプロパティを紹介しました。表 4 がレガシー アドバタイズ (ADVB$_L$) のプロパティです。

プロパティ	コメント
トポロジー	無指向性:1対多 (1:m) または 指向性:1 対 1 (1:1)
送信と受信	アドバタイズイベントの種類、デバイスロールによって異なる *上記 "デバイスロール" のセクション参照*
アプリケーションデータの方向	一方通行。アプリケーション データはアドバタイズ デバイスからスキャン デバイスへのみ送信可能
接続型/接続型	非接続型
データと時間	非同期
レシーバの同時受信	無指向性のアドバタイズ パケットを同時に受け取るデバイスの数は無制限 指向性アドバタイズとは、送信されたパケットが 1 つのスキャン デバイスにのみ関連することを意味します。
無線チャネル	プライマリ アドバタイズ チャネルを最大 3 つ使用可能 使用するチャネルはアプリケーションによって決定され、チャンルの順序はランダムに決定
スケーラビリティ	無指向性アドバタイズは、理論上のデバイスの数に制限がないので、ADVB$_L$ は非常にスケーラブル ADVB$_L$ によるデータ転送は、AdvData のペイロードサイズが小さく、許可されるアドバタイズ間隔の制限を受けるので、スループットは比較的低速
PHY の選択	LE 1M のみ

表 4 ADVB$_L$ のプロパティ

ご存じですか？

この記事の終わりにあたり、レガシーアドバタイズに関する興味深く有用な追加ポイントをいくつか紹介して締めくくります。

コントローラーにはいくつかのフィルタ ポリシーが実装されていることをご存知ですか？

アプリケーションは、スキャン状態や接続開始状態にコントローラーのフィルタを適用するように設定できます。例えば、*スキャン フィルタ ポリシー*は、各デバイスから受信した最初のアドバタイズ パケットのみがホストに渡るように設定できます。そのため、すでに検出されたデバイスからの重複したアドバタイズ パケットは破棄されます。同様に、*イニシエータ フィルタ ポリシー*は接続可能なアドバタイズ パケットを様々な方法でフィルタリングします。フィルタ ポリシーは、コントローラーから無関係または既に受信したデータを送信しないため、ホストによる処理効率を高めます。

Bluetooth Core Specification v6.0 で Monitoring Advertisers という新機能が導入されたことをご存知ですか？

コントローラーのフィルタ ポリシーは効率性を向上させる可能性がありますが、潜在的な欠点もあります。コントローラーによってパケット フィルタリングが適用されない場合、ホストは対象デバイスの存在や、そのデバイスが通信範囲内に入ったり出たりしたタイミングを推測できます。

これは非常に貴重な情報ですが、重複パケットを処理する必要があるという代償を払うことになります。

Monitoring Advertisers 機能により、ホストはコントローラーの設定を行い、関心のあるデバイスが範囲内に出入りする際に、コントローラーから送信される HCI イベントでホストは通知を受け取ることができます。これにより、アプリケーションはコントローラーに重複パケットのフィルタを依頼し、受信したアドバタイズ パケットの処理にかかるオーバーヘッドを抑えつつ、デバイスの有無を把握できるようになります。

検出可能なモードが 2 種類あることをご存知ですか？

Generic Access Profile (GAP) は、限定検出可能モードと一般検出可能モードを定義しています。デバイスが限定検出可能モードに留まれるのは 180 秒以内です。デバイスが一般検出可能モードに留まれる時間に制限はありません。

デバイスがどちらのモードなのかは、アドバタイズ PDU の Flags のビットで示されます。

この 2 つのモードが存在する理由は、限定検出可能モードのデバイスを一般検出可能モードのデバイスよりも優先させるためです。

接続で使われるフレーム間時空間パラメータを変更できる可能性があることをご存知ですか？

指向性アドバタイズの用途の一つは、ターゲット デバイスの接続を陣族に行うことです。そのため、接続型指向性のアドバタイズは *高デューティサイクルモード* または *低デューティサイクルモード* のいずれかで実行可能です。高デューティサイクルモードでは、同じアドバタイズチャネルで送信される連続した 2 つの ADV_DIRECT_IND PDU の開始間隔は 3.75ms を超えてはなりません。低デューティサイクルモードでは、任意のチャネルで送信される隣接する PDU 間隔は 10ms を超えてはなりません。高デューティサイクル指向性アドバタイズは消費電力の点でコストが高くなることに注意してください。

シリーズの次回

この記事では、Bluetooth LE の $ADVB_L$ 通信モードについて探ってきました。

このシリーズの次回の記事では、拡張アドバタイズ($ADVB_E$)コミュニケーションモードについて詳しく見ていきます。